CRANFIELD UNIVERSITY

MIKE HUMPHREY

IDENTIFYING THE CRITICAL SUCCESS FACTORS TO IMPROVE INFORMATION SECURITY INCIDENT REPORTING

CRANFIELD DEFENCE AND SECURITY
PhD

Academic Year: 2010-2017

Supervisor: Dr Ruth Massie
August 2017

CRANFIELD UNIVERSITY

CRANFIELD DEFENCE AND SECURITY
PhD

Academic Year 2010-2017

MIKE HUMPHREY

Identifying the Critical Success Factors to Improve Information Security Incident Reporting

Supervisor: Dr Ruth Massie
August 2017

ABSTRACT

There is a perception amongst security professionals that the true scale of information security incidents is unknown due to under reporting. This potentially leads to an absence of sufficient empirical incident report data to enable informed risk assessment and risk management judgements. As a result, there is a real possibility that decisions related to resourcing and expenditure may be focussed only on what is believed to be occurring based on those incidents that are reported. There is also an apparent shortage of research into the subject of information security incident reporting.

This research examines whether this assumption is valid and the potential reasons for such under reporting. It also examines the viability of re-using research into incident reporting conducted elsewhere, for example in the healthcare sector. Following a review of what security related incident reporting research existed together with incident reporting in general a scoping study, using a group of information security professionals from a range of business sectors, was undertaken. This identified a strong belief that security incidents were significantly under-reported and that research from other sectors did have the potential to be applied across sectors. A concept framework was developed upon which a proposal that incident reporting could be improved through the identification of Critical Success Factors (CSF's). A Delphi study was conducted across two rounds to seek consensus from information security professionals on those CSF's.

The thesis confirms the concerns that there is under reporting and identifies through a Delphi study of information security professionals a set of CSF's required to improve security incident reporting. An Incident Reporting Maturity Model was subsequently designed as a method for assisting organisations in judging their position against these factors and tested using the same Delphi participants as well as a control group. The thesis demonstrates a contribution to research through the rigorous testing of the applicability of incident reporting research from other sectors to support the identification of solutions to improve reporting in the information security sector. It also provides a practical novel approach to make use of a combination of CSF's and an IRMM that allows organisations to judge where their level of maturity is set against each of the four CSF's and make changes to strategy and process accordingly.

ACKNOWLEDGEMENTS

Special thanks go to my wife Julie for her continuing support and understanding throughout the whole length of time taken to research and write this up.

Thanks my supervisors Dr Ruth Massie, Prof. Debi Ashenden and Dr Annie Maddison-Warren

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF APPENDICES

(Separate Document)

LIST OF ABBREVIATIONS

A&E	Accident and Emergency
ALE	Annual Loss Expectancy
ASAP	Aviation Safety Action Platform (US)
ASRS	Aviation Safety Reporting System (US)
AUSCERT	Australian Computer Emergency Response Team
Bcc	Blind Carbon Copy
BCP	Business Continuity Plan
BSI	British Standards Institute
BYOD	Bring Your Own Device
CARO	Computer Antivirus Research Organisation
CIA	Confidentiality, Integrity and Availability
CCP	CESG Certified Practitioner
CD	Compact Disc
CERT	Computer Emergency Response Team
CERT Australia	Computer Emergency Response Team Australia
CERTNL	Computer Emergency Response Team Netherlands
CESG	Communications Electronic Security Group (UK)
CHIRP	Confidential Human Factors Incident Reporting System
CIPPIC	Canadian Internet Policy and Public Interest Clinic (CAN)
CINRAS	Communications security Incident Notification Reporting and Alerting Scheme
CISO	Chief Information Security Officer
CiSP	The Cyber-security information Sharing Partnership
GovCERTNL	Government Computer Emergency Response Team Netherlands

CPNI	Centre for the Protection of National Infrastructure
CROP	Common Relevant Operating Picture
CoI	Community of Interest
CSF	Critical Success Factors
DoS	Denial of Service
DDOS	Distributed Denial of Service
DHS	Department for Homeland Security (US)
DNS	Domain Name System
ENISA	European Network and Information Security Agency
FCA	Financial Conduct Authority
GIAC	General Information Assurance Certificate (US)
GovCERT	Government Computer Emergency Response Team
GovCERTNL	Government Computer Emergency Response Team Netherlands
GovCERTUK	Government Computer Emergency Response Team UK
GSI	Government Secure Intranet (UK)
HIPAA	Health Insurance Portability and Accountability Act (US)
HMRC	Her Majesty’s Revenue and Customs (UK)
HoMER	Holistic Management of Employee Risk
HR	Human Resources
HSE	Health and Safety Executive (UK)
IAAC	Information Assurance Advisory Council
IAAF	Information Assurance Assessment Framework
IAMM	Information Assurance Maturity Model
ICO	Information Commissioner’s Office (UK)
ICT	Information Communication and Technology
ID	Identity Document

IDS	Intrusion Detection System
IISP	Institute of Information Security Professionals
IRMM	Incident Reporting Maturity Model
IS1	Information Security Standard 1 (UK)
ISAC's	Information Sharing and Analysis Centres (US)
ISO	Information Security Officer
MOD	Ministry of Defence (UK)
NASA	National Aeronautics and Space Administration
NCA	National Crime Agency
NISC	National Information Security Conference
NISCC	National Infrastructure Security Coordination Centre (replaced by CPNI)
NIST	National Institute for Standards and Technology
NHS	National Health Service (UK)
NorCERT	Norwegian Computer Emergency Response Team
NPSA	National Patient Safety Agency
NRLS	National Reporting and Learning System
PCIDSS	Payment Card Industry Data Security Standards
PCR	Perceived Composite Risk
PHIPA	Personal Health Information Protection Act (Canada)
PNN	Police National Network
PWC	Price Waterhouse Cooper
RCA	Root Cause Analysis
RIDDOR	Reporting of Injuries Diseases and Dangerous Occurrences
ROI	Return on Investment
RSSB	Rail Standards and Safety Board

SCADA	Supervisory Control and Data Acquisition
SIAF	Scottish Information Assurance Forum
SPF	Security Policy Framework (UK)
SRA	Structured Risk Analysis
SRA-IS	Structured Risk Analysis-Information Security
TCO	Total Cost of Ownership
US-CERT	United States- Computer Emergency Response Team
WARP	Warning Advice and Reporting Point

Chapter 1 The Real World Problem – From Cyberspace to Security Incident Reporting

1.1 Introduction

In the field of Information Security there is a common perception amongst practitioners and academics, (Baker, Rees and Tippett, 2007; Gordon, Loeb et al, 2003; Hagen, J, 2009; Parker, 2010) that the true number and type of information security incidents is unknown, the perception is that this is largely due to under reporting. Without an accurate empirical knowledge of incident numbers, the true likelihood of a particular type, or group of, incidents occurring is unlikely to be known, therefore adversely affecting any risk calculation, irrespective of the methods used. This results in the potential for accuracy and value of risk assessments to be put into question. This in turn could result in resources and the associated hard to come by budgets, being directed at mitigating the wrong risks.

> "It is important an organisation has the best possible information on risks in order to decide whether or not to invest (scarce) resources in countermeasures and if so how much." (Birch and McEvoy, 1992, p.44).

Parker (2010) describes the problem with risk assessments as they cannot be measured accurately due to unknown threats and vulnerabilities. Is this a problem peculiar to the information security industry or does the same under reporting issue appear elsewhere? This chapter will introduce the background to the perceived problems regarding the reporting of incidents and the potential impact on information sharing and risk analysis associated with a lack of empirical incident data.

1.2 The Value of Information in Today's Society

In today's world information is ubiquitous and, increasingly for individuals, organisations and nations, seen as an asset which has value (Horne, 1995; Moody and Walsh, 1999; Keohane and Nye, 1998). This could be monetary, intellectual property, customer information, personal information and many others forms. It may be the case that information has always been considered of value, as evidenced by the need to protect it through early iterations of cyphers and encryption in Egyptian times, as well as Caesar cyphers and biblical cyphers (Singh, 1999). Such widespread information availability has inevitably resulted in those who are not entitled to access it trying to do so. Whether they are competitors, criminals or nation states the value of such information to those not entitled to see it becomes an attraction. The need to protect it is clear.

The main difference between then and today is the sheer volume of information available and the numerous methods and devices that access that information. An ever increasing proportion of that information is now stored, processed and accessed via technology and users increasing acceptance of these methods of accessing it (Venkatesh et al, 2012). The reliance upon that technology, and the skills to support it, has become commonplace (Lockridge, Brandon and Barnett, 2011) but not necessarily providing the necessary skills, user friendly instructions and support for its users who have to interact with it (Parasuraman, 2000).

Terms such as “the cloud” (NIST, 2011) “bring your own device – BYOD” (Caldwell, Zeltmann and Griffin, 2012) and ‘smart phone’ (Power, 2013) are part of everyday language.   A collective noun ‘Cyberspace’ (Pollitt, 1998) commonly describes the widespread use and reliance upon computer networks. It is possible to consider cyberspace as an increasing element of a new engine of economic growth and, to some extent, a contributory factor to the modern industrial revolution as described by Jenson, (1993).   By default, other derivatives of cyber such as cybercrime and cyber security have now become everyday terms. Cyber is now of great interest, and concern, to governments and nation states, many having introduced cyber strategies. ENISA (2012) has published a list of countries that now have a strategy which includes the UK, US, Germany, France, Estonia and many others.

There is a potential overlap in the use of the term cyber and the focus of this research, which is information security incidents. For example; cybercrime incidents relate to reported crimes. To commit a cybercrime may involve the exploitation of a security vulnerability to achieve a criminal gain. The use of such a vulnerability may be an information security incident, but the cybercrimes that result are not. In a similar vein cyber threats can include attacks on digitally-controlled physical systems with no resultant access to or risk to information. These cyber risks are outside the scope of this thesis in relation to information security risk management and assessment.

The real or perceived threat to nations, critical infrastructures, organisations and citizens from cyber-attacks, cybercrime and concerns about the prospect of cyber warfare has led to calls for greater collaboration amongst nations to tackle the problem. This has resulted in the growth in Computer Emergency Response Teams (CERTS) in a number of countries and initiatives which aim to encourage real time sharing of Cyber threats such as in the UK - CiSP - the Cyber-security information Sharing Partnership. To counter the threats to information in cyberspace, and to exploit the benefits the internet can bring, requires a greater understanding of the threats and risks. Unfortunately, with the growth of technology there are those who seek to exploit that information for financial gain and organised crime,

> “If there is a single cross-cutting issue that has changed the landscape for serious and organised crime and our response against it, it is the growth in scale and speed of internet communication technologies.” Great Britain, National Crime Agency *(2014)*

It is of note that in recent years there has been an increase in regulation and legislation intending to tackle the protection of information and in some cases the mandation of reporting incidents, where Room (2009) suggests that the current cycle of development of security law began in 2003 with mandatory reporting in the state of California. He later suggests,

> “one of the inevitable consequences of the regulatory bear market will be greater instances of conflict between the regulators and the regulated.” (Room, 2009, p.376).

This puts pressure on organisations to try to undertake business activity against a changing regulatory landscape. There is a need therefore, for companies and organisations, to know what is happening to their data assets and the possible security incidents that could lead to breaches. Although high-profile events involving cyberspace are reported in the media, for example: TK Maxx in 2007 “Hackers target TK Maxx customers” (BBC, 2007); Sony in 2014 “Sony Pictures computer system hacked in online attack” (Taylor, 2014); in 2015 Talk Talk, “TalkTalk customer data at risk after cyber-attack on company website” (Johnston, 2015) , and major data losses such as the UK HMRC data loss in 2008; it is strongly suspected many others are not.

Regulatory oversight requires information to assure the governance of managing risk, leading to the need for more precise metrics and risk management models (Davenport and Harris, 2010). This regulatory oversight is set to be increased with the soon to be introduced General Data Protection Regulation (Regulation (EU) 2016/679) which relates to personal data incidents, the mandated reporting of incidents within certain timeframes and a considerable uplift in fines.

Due to the uncertain nature of the true scale of information security incidents through under reporting, there is a subsequent lack of sufficient empirical data to make reasoned judgements for risk assessment and risk management. In the face of the increasingly recognised cyber threat, nations wishing to collaborate and or share incident information are potentially being hampered by this lack of data.

This chapter begins with a description of the research problem – the apparent lack of research in the area of information security incident reporting and the issue that there is no recognised definition of a security incident. It continues by suggesting how that gap may be addressed by re-using research elsewhere to the benefit of information security which in turn demonstrates the contribution to knowledge. It outlines the scope of the research, the aims and goals together with a selection of the existing literature that highlights the problem. It concludes with the research approach and structure of the thesis.

1.3 The Research Problem

There is a perception that the true scale of information security incidents is unknown due to under reporting. This potentially leads to an absence of sufficient empirical data to enable informed risk assessment and risk management judgements. There is also an apparent shortage of research in the area of information security incident reporting. To test the validity of these concerns a confidential scoping study was undertaken in 2011 and this is set out in detail in Chapter 4. This scoping study examined the perceptions and experiences of a number of information security professionals from a range of sectors. The results identified a firm belief amongst them that security incidents were significantly under-reported, thereby potentially denying the opportunity for analysis of a wider pool of information on the causes, vulnerabilities and human factors which led to these incidents.

A particular problem is that of understanding what a security incident is. Identifying that a security incident has occurred has to happen before it can be reported. It could be argued that not all incidents can be of direct use to an overall cyber security strategy, but few attacks are totally technical. Many require elements of social engineering and the targeting of key employees can ensure an easier method of breaching the defences of an IT system. Security incidents involving the loss of an ID or door entry pass, the misplacing of a relevant technical document or inappropriate actions of disgruntled employee, if not reported, can provide the elements of a combination of factors that could lead to a successful cyber security attack.

One of the challenges is there is no nationally or internationally recognised incident classification criterion. Even the recognised ISO standard for managing security incidents, BS ISO/IEC 27035 (2011) does not include a definition of an incident. Within the standard it states;

> "Organisations should ensure that information security incidents are documented in a consistent manner, using appropriate standards for incident categorisation and classification, and sharing, so that metrics are created from aggregated data over a period of time. This provides valuable information to aid the strategic decision making process when investing in information security controls." (British Standards Institute 2011, p.4)

On further examination of this statement phrases such as "incidents documented in a consistent manner" may be acceptable if only collated and used locally but do not add value when any sharing of incident information is required. The scoping study in Chapter 4 identified the existence of a number of locally used incident definitions. This is likely to cause difficulty when these local reports are used for wider incident data sharing. Likewise, where the standard continues in the same vein regarding categorisation and classification it really exposes the standard as a unilateral one.

This is not to criticise the current focus of the standard but there needs to be more consistency and common classification if the wish for wider industry sectors and governments to be able to truly understand the information risks they are facing. This "strategic decision making process" (British Standards Institute 2011, p.4) will remain aspirational until there is some consensus, whether voluntary or regulatory, on incident categorisation and classification.

The recent issue of BS ISO/IEC 27035-1:2016 gives a high level definition of a security incident as

> "one or multiple related and identified information security events (referring to their definition of an event – occurrence indicating a possible breach of information security or failure of controls) that can harm an organisations assets or compromise its operations." (British Standards Institution, 2016, p.2)

As a result of differing definitions the ability to compare and contrast incident data may be flawed from the outset. Chapter 2 examines the issue of a lack of a common security incident definition in more detail as well as offering a new definition and one that was used in the Delphi and Validation Studies described in chapter 5 and 6. This provided participants with a common definition upon which to base their interpretation of an incident when completing their questionnaires.

If the real, or near real, picture of the likelihood of certain types of information security incident is not known, there is the danger that those which are reported are given higher prominence simply because that is the only information upon which to work on. For example, electronically gathered incident reports from audit logs or Intrusion Detection Systems (IDS) are automatically generated and therefore more readily visible. These incident logs, because they are tangible, can be used to justify risk based decisions. The absence of a wider perspective of the true nature of the type and volume of incidents, and near misses, may give undue prominence to the electronic log indicators and may mask the real threat. Information security incidents that rely upon staff to report are equally important in assessing risk.

Early research into information security risk and the relationship between managing information risk and applying countermeasures was reported by Birch and McEvoy (1992). They recognised that the value of information stored on the information systems exceeds that of the value of the technology used to store and process it. In a similar vein Willcocks and Margetts (1993) conducted studies into risk assessment and information systems but there was little in their research relating to security incidents. One of the earliest papers on the subject of information security incidents was by Blakely, McDermott and Geer (2002), they refer to the lack of information regarding security incidents and made the comparison that information security is now somewhat in the same position as the healthcare industry was 100 years ago. In medicine about 100 years ago some basic medical facts were known, certain treatments and medicines worked but many did not and there was no real data collection but over time the situation improved. However, despite having such a head start over information security, papers, such as “An Organisation with a Memory” (Great Britain, Department of Health, 2000) show that incident reporting in the healthcare sector is not all it should be with many barriers to reporting adverse patient incidents being identified. It was these barriers that were used in the scoping study in Chapter 4 to ascertain if there was any potential for them to be recognised as relevant to the information security sector.

One of the earliest theses that made reference to information security, the links to security culture and the relationship with individuals was Dhillon (1995) who suggested that within organisations, the formal and informal systems are often not appreciated in the analysis and design of information systems. Dhillon (1995) identified that users often interpret the formal work requirements in a local way and then play out the processes to suit the informal element of their environment. This can lead to the centre of an organisation falsely believing that corporate policies are adhered to across the whole organisation. For example a policy may be in place that states staff must report incidents but not followed for those same local reasons. In reality, the adoption of local practices to support a colloquial view win through, often putting central policy at risk (Lipsky, 1980).

Other research refers to the issue of there being a need for information on security incidents but true analysis is hampered by lack of data. Parker (2009) proposes that security risk assessments should in fact come with a health warning that they are likely to be “incomplete and subjective”. (2009, p.33). The situation has obviously not improved in his perception as previously Parker (2006) in his paper “Making the case for balancing risk based security” referred to the problem of there not being enough valid data to make risk assessment a straightforward and successful method. He argues that although there should be efforts made to improve incident reporting, he does not suggest how and expresses doubts this will be achieved;   this thesis aims to propose a method that can do this. Soderburg, Grankvist, Brulin and Wallin (2009) observed that despite it being mandatory to report all incidents that relate to patient safety, as required by the National Board of Health and Welfare in Sweden, this did not occur.   A number of reasons were given by respondents for not reporting including;

> "lack of time, a complicated reporting procedure, no one else reports incidents and the belief that the reporting of an incident would not make any difference."
> Soderburg, Grankvist, Brulin and Wallin (2009, p.733)

Dalkey (1969, p.2) refers to there being a spectrum of inputs; ranging from speculation through to knowledge. In between lies opinion which he believes is the flattering name for the collective "products of judgement, wisdom, insight and similar intellectual processes". In this Spectrum of Inputs, the lower the probability of truth could relate to the number of security incidents where the view of this research is this could result in more speculation as opposed to true knowledge. Using Dalkey's model (Figure 1-1), the perceived lack of empirical evidence on security incidents would suggest that risk assessments and risk management judgements on countermeasures may be more based on speculation and opinion rather than evidenced knowledge. This leads to the possibility that the probability of truth as outlined in Dalkey's model could be considered as low.

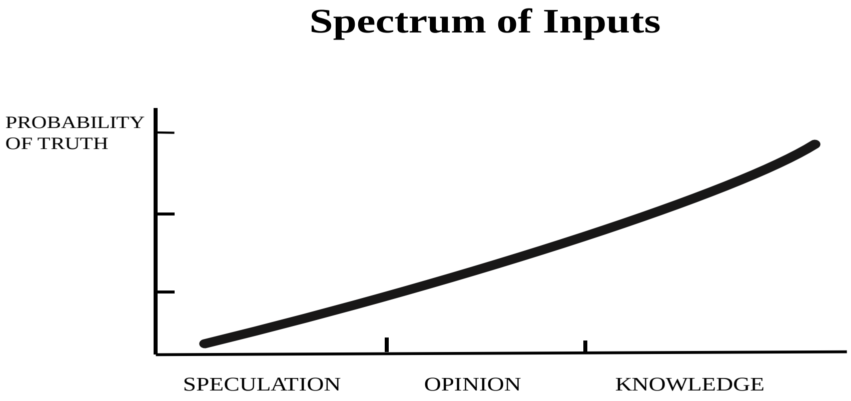


Figure 1-1 Based on Dalkey, N (1969, p.3) Spectrum of Inputs

The process of risk analysis based on a lack of information is commented on by Baskerville (1991) who describes it as professional interpretivistic knowledge. He outlines his position on the weaknesses of the positivist philosophical use of risk analysis as opposed to his view of the more important element of interpretive use to which risk analysis can be deployed. In particular where it takes into account the professional and contextual understanding of a particular information system and its controls. He examines the potential for risk analysis not to be considered in the same vein as other analysis methods that have empirical statistics available but places it in an interpretive position. Baskerville (1991) proposes that a professional security practitioner has values and also 'a priori' knowledge that can interfere with empirical observations. A situation also identified by Hubbard and Evans (2010) where they refer to people judging risks often ignoring facts and basing their judgement on memories. When this inference is in play it could be argued the risk analysis is interpretive. He strongly argues that there is a place for risk analysis, despite the lack of empirical figures to populate any method of calculation, and that the professional experience of those charged with risk analysis should be recognised more.

He suggests that improving the volume of evidence related to reported incidents could damage the 'priori knowledge' element of risk analysis.

> "Improving the positivist scientific accuracy of the statistical representation simultaneously reduces the interpretive scientific accuracy." (Baskerville, 1991, p.756)

However, he also recognises that the lack of empirical evidence makes the findings of many risk analysis processes difficult to prove or disprove. This perceived lack of data could put at risk the increasing push to share incident and threat information between communities of interest potentially resulting in an interpretative approach to decision making but without sufficient data to have real confidence in the validity of the outcome. Those incidents that are reported, although providing some basis for risk assessment and management, may contain unknown biases that could affect any such assessments.

1.4 Research Approach - A Conceptual Framework

The proposed research will use a conceptual framework (Figure 1-2) to articulate the various components relating to information, information risk and risk management. It will be used to illustrate the suggested relationship between possessing information, the requirement to use or exploit that information, the understanding of information risk, risk management, the potential consequences of a loss or compromise (an incident) and sanctions (regulatory, legislative, reputational) against which an organisation's "risk appetite" (Drew, 2007) is formed and finally the main focus of this research - incident reporting.

When things go wrong and data is lost, stolen or compromised the occurrence of such a security incident should trigger a review of the event, thereby enabling a valuable input into the benefit versus sanction element within the conceptual framework. This is important as such a review should enable the organisation to learn and understand the real causes of the incident. If that review is superficial it may be difficult to identify the true cause. However, an end to end root cause analysis (O'Connor (NASA) 2005, p.5; see Glossary), in the form of 'double loop learning' (Argyris, p.116, 1997) is more likely to discover the true cause(s). Lukic, Margaryan and Littlejohn (2010) refer to double loop learning as important due to its ability to "surface latent and systemic causes that might be contributing to incidents at a later stage". (2010, p.431)

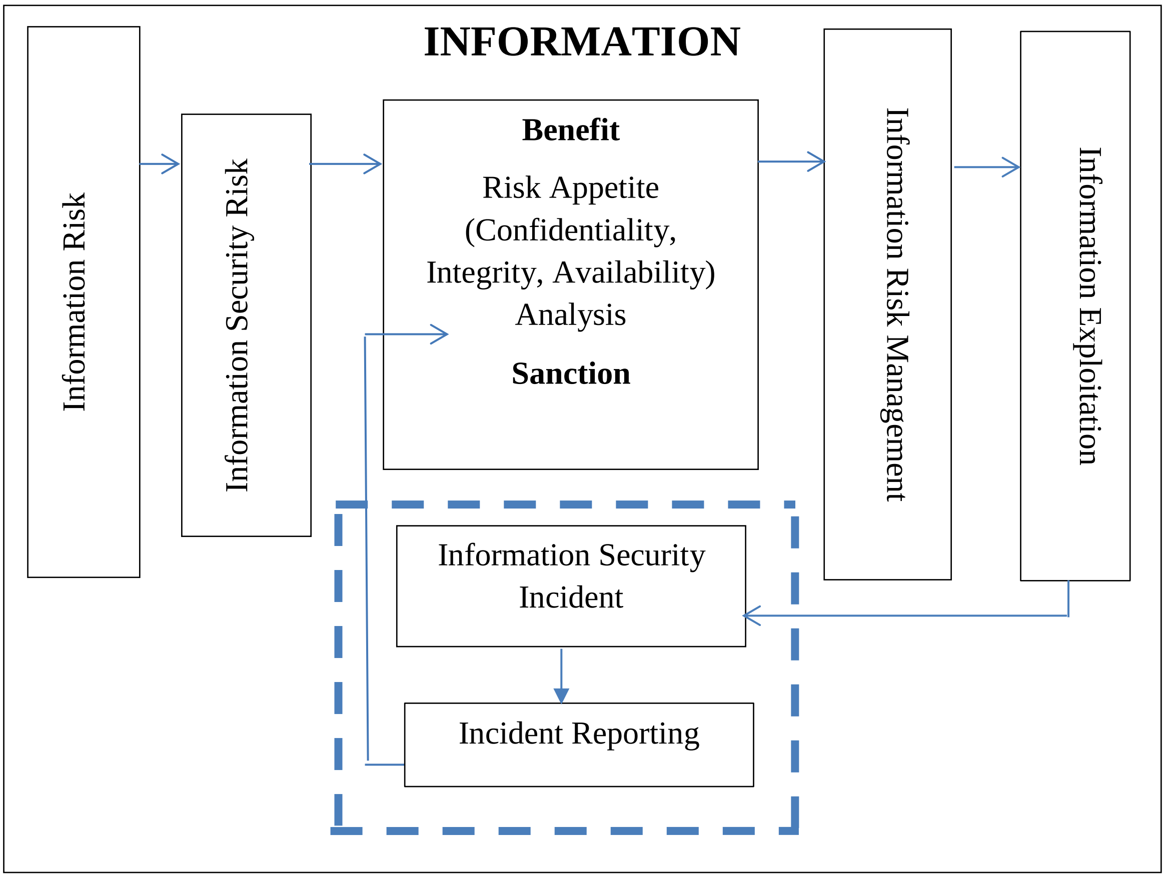


Figure 1-2 Information Conceptual Framework (area of focus within dotted lines)

This thesis will suggest the process set out in the framework is hampered by barriers to reporting. In public enquiry reports into previous disasters for example; the Bradford Football Club fire in 1995 (Popplewell, 1985), the sinking of Herald of Free Enterprise 1987 (Sheen, 1988) and the Kings Cross Underground fire 1987 (Fennell, 1988), the cause(s) of the particular disaster was the culmination of a number of smaller events, design and or management deficiencies which, if individually had been identified reported and tackled, the disaster(s) may either never had occurred or at least had less severe consequences.

Many of these minor incidents, although different in nature, were often not reported. Toft and Reynolds (1999) propose that disasters are incidents created by people operating within complex systems and where the causes are not acted upon, similar accidents can and do occur. In the case of the Bradford fire Mr Justice Popplewell in his enquiry report highlighted that many of the safety related recommendation were in fact identified in previous reports into other football related disaster but had not been put in place.

> “I too shall argue for these and related measures. It is to be hoped they will be more vigorously pursued by the appropriate bodies than in the past.” (Popplewell, 1985, p.17)

This is similar to the ‘Swiss Cheese’ model as proposed by Reason (1990) where safeguards may be by-passed or fail due to the coming together of a number of factors which, when combined, lead to a break in a safety mechanism.

The next major incident may not be a fire or a shipping disaster but a failure of one or more elements of Critical National Infrastructure facilities resulting in civil unrest and or harm. It is possible to postulate that the inevitable subsequent enquiry may highlight a lack of incident reporting as a cause? The question is not if, but when, a major disaster will occur involving a failing of a system or systems as a result of an unreported singular or series of information security incidents. As technology appears destined to continue to be integrated in our everyday lives, for example the proposed advent of smart cities (Smartcities Council, 2015: see Glossary), this is potentially more likely.

1.5 The Research Contributions

It is apparent from the literature review in Chapter 2 that the amount of research into the reporting of security incidents is limited. Critical to managing risk is to understand and have confidence in the level of protection against known vulnerabilities and accurate data relating to the types of adverse security incidents that have occurred and are still occurring. Knowledge of trends and emerging threats is key to this. However, without sufficient trusted data, such decisions can never be truly fully informed. There is also a real concern over the ability to identify and classify incidents to provide a true analysis of the number of type of incidents actually occurring. Examination of the literature relevant to incident reporting so far has identified there are gaps in research in the area of security incident reporting, though this will be further examined in chapter two. It has also identified a lack of standard taxonomies for security incidents and information security risk.

This research aims to add value to academic knowledge by investigating the subject of security incident reporting which appears not to have been studied in depth. It will examine the potential re-use of research on the subject conducted elsewhere such as in healthcare studies into patient safety and the adverse incidents that can lead to harm as well as aviation and other safety industries. These research findings aim to be of relevance to the information security field and, to test this, it is proposed to study the applicability of this research by data collection from information security professionals. A method to improve incident reporting will be proposed through the identification of the Critical Success Factors involved and set these in a Maturity Model that can be applied by organisations in an iterative, non-prescriptive and contextual manner that may improve the level reporting of security incidents.

Thereby increasing the pool of data to enable improved analysis and lead to better informed risk based decisions. It will examine the relationship and importance of information security incident reporting to the ability of organisations and nations to share information in their quest to improve overall cyber security.

Through the use of a scoping study, followed by a full scale Delphi study and subsequent validation study the research will aim to identify a range of Critical Success Factors believed necessary to improve the reporting of security incidents. It will also outline the apparent lack of consistency of information risk, incident definitions and classification including the subsequent challenges this places upon professionals tasked with implementing the growing number of information sharing initiatives. Although not a key part of the research an information security risk and security incident definition has been proposed. The incident definition was created to ensure consistency in understanding of the term for the purposes of the Delphi and Validation studies.

Figure 1-3 suggests where the Critical Success Factors and an Incident Reporting Maturity Model could fit into the conceptual framework. The aim is to enable organisations to adopt the Maturity Model as part of their information handling and incident management process. The outcome may potentially improve security incident reporting. This improvement in the volume of incident data may in turn enable better informed analysis for future risk assessment and management.

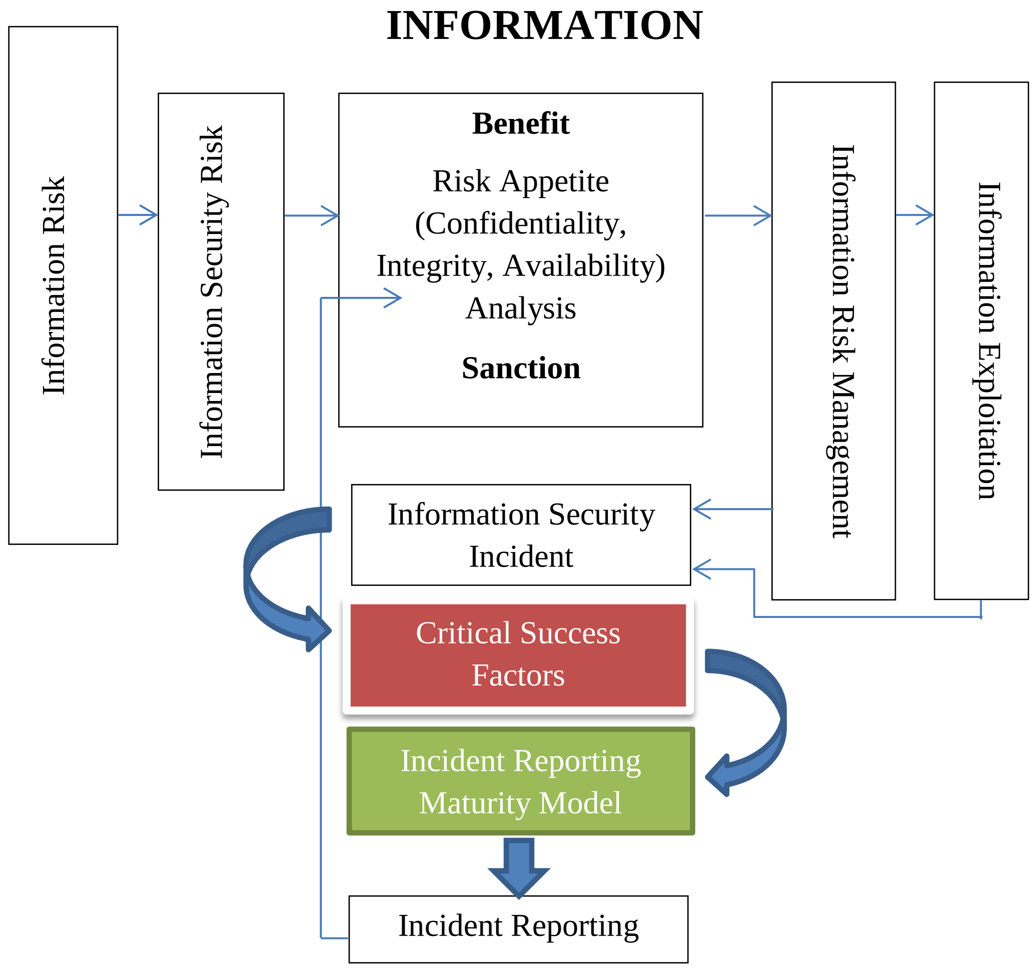


Figure 1-3 Showing the Conceptual Framework Incorporating Critical Success Factors and Security Incident Maturity Model

1.6 Research Scope and Goals

The subject of information security, incidents, analysis, risk assessment, risk management is wide and becoming more complex as the world is increasingly becoming a digital one, relying upon digital communications, and data storage in every aspect of life. There is a danger that this research could try and examine many of the above aspects which would not be manageable.

Instead it focusses on the reporting of incidents, the purpose of reporting, and will try to identify what information security incident reporting Critical Success Factors are required to be in place to bring about a change in incident reporting that ultimately benefits the need to share. It will refer to information sharing, but not in depth, as there is more research and activity in this space. The reason for this light touch reference is to demonstrate the inextricable relationship between accurate reporting and the sharing of the product of such reports.

The research goals are:

> (1) To test whether the assumption that not all information security incidents are being reported is correct.
>
> (2) To examine whether research on incident reporting conducted in other sectors, such as healthcare, can be applied to the information security sector.
>
> (3) To identify the Critical Success Factors that may be applicable to information security incident reporting.
>
> (4) To propose an information security Incident Reporting Maturity Model that could be applied by organisations and may improve the flow of incidents that are reported.

The potential outcome of these goals being to increase the levels of reporting leading to sufficient incident data that could facilitate more accurate analysis of the likelihood and causes of those incidents. This in turn may encourage more grass root reporting that ultimately would feed through the local processes into the regional/sector and ultimately assist in improving national information sharing initiatives.

The above lead to the thesis title.

> ‘Identifying the Critical Success Factors to improve Information Security Incident Reporting’:

The research sub questions to support the overall research question and provide a valuable contribution to the furtherance of research in information security incident reporting are:

> *(1) Is the perception that not all information security incidents are reported a correct one?*

This is a key element to the research and, if confirmed, what follows is to identify the possible reasons for this under reporting. Assuming this is a correct assumption this leads to question 2;

> *(2) Are the reasons for low reporting similar to those identified in other research such as the healthcare and safety industries?*

This will identify research already conducted elsewhere and examine whether any findings can be applicable to information security. The results can then be tested by conducting surveys through questionnaires on representatives of the information security profession. This in turn will enable the information security profession to make use of such findings to improve reporting in their sector.

> *(3) Is it possible to identify the Critical Success Factors required to improve information security incident reporting?*

The identification of Critical Success Factors should enable a greater degree of focus on what is important and more likely to achieve results thereby improving the identification of methods to deploy to enable better reporting.

> *(4) Can a security Incident Reporting Maturity Model be developed that would enable an iterative approach to its deployment whilst taking account of any methods already in place?*

This will give information security professional a greater degree of knowledge in what activities and reporting mechanisms to deploy that may improve the level of reporting.

It is recognised that within the scope of this research there is not sufficient time to identify if the adoption of a Maturity Model has any significant effects. The result is focussed on the question of reusing previous research to identify the CSF's required to produce such a Maturity Model.

1.7 Research Limitations due to the Sensitivity of the Subject

The research subject focusses on sensitive issues and in engaging with security professionals, asking for their honest opinions regarding the true situation in respect of their organisations incident reporting systems and effectiveness may result in a reduction in participants or less than candid responses, a situation recognised by Kotulic and Clark (2004) and Flores, Antonsen and Ekstedt (2014). The identification of a company or organisation that has suffered from a security breach or information loss or where their processes for identifying the same are weak or inadequate would be a serious concern for those charged with their security. Any research undertaken needs to be cognisant of this and provide assurances to participants that any information provided will be handled appropriately to ensure strict confidentiality for those providing responses to any surveys, interviews or other forms of research. A fuller discussion of this can be found in the Chapter 3 methodology ethics section.

1.8 Research Design and Thesis Structure

The research will be set out in seven stages

Stage 1. To understand if the perceived problem of a lack of reporting of information security incidents is supported by literature.

The literature reviewed in the introductory chapter already provided evidence that it was of concern to a number of authors and researchers studying information security, but no specific research on why could be identified.

Stage 2. Identify the appropriate research methodology.

Due to the apparent lack of qualitative empirical evidence the conceptual framework (as illustrated in figure 1-3) research paradigm of this thesis will encompass interpretative methods and also utilise qualitative data primarily through the use of questionnaires. However, that will not prevent the acquisition of quantitative data as a result of studies undertaken.

This included the use of qualitative and quantitative research using a scoping study questionnaire and a Delphi study to identify the opinions of information security professionals.

> *Stage3. A scoping study of a number of information security professionals was undertaken to test the initial assumption that there was indeed a problem with security incident reporting.*

The scoping study questionnaire used a mix of interpretative and some qualitative analysis of the questionnaire text responses. Its main aims were to identify the understanding of a number of information security professionals their perception and experience of incident reporting. The opportunity was also taken to test whether initial findings from research in the healthcare sector could be considered as valid to be used by those professionals and the sector as a whole. The scoping study achieved its aims in confirming the belief there was under reporting and that findings from healthcare relating to adverse patient reporting were relevant and could be considered for re use.

> *Stage 4. Subsequent to the analysis of the scoping study the results were socialised in a series of presentations to information security professionals at security seminars and conferences.*

The purpose was to examine the responses of information security professionals in both the public and private sector to identify if any adverse reaction or comment to those results was made. There was considerable support for the research, a firm belief the findings were truly reflective of incident reporting concerns.

Even as recently as July 2017 at a CISO conference in Barcelona the findings were presented to the audience and during the presentation they had the opportunity to anonymously provide an answer to the question “how confident are you that your staff know how to report strange activity or a potential security incident?” the choices being very confident, fairly confident or low confidence. Using an in-conference confidential on line poll the result was 22% very confident, 50% fairly confident and 28% low confidence (see appendix 18). This indicates that amongst security professionals there are still concerns regarding the reporting of incidents.

> *Stage 5. Identify the critical success Factors to improve the reporting of security incidents through the use of a Delphi study*

Having socialised the research findings so far the next stage was to propose a method that could identify which of the findings would be of the most use to organisations to improve the reporting of incidents. It is often the case that when a report publishes its findings, whether it is the result of a disaster or significant event or one commissioned to resolve a problem, the valuable content is not always taken up in practice as organisational cultures are resistant to change (Perrow, 2007; Schein, 1992). The elements identified in the research that could influence and potentially improve incident reporting may be able to form the basis of a series of Critical Success Factors (CSF's). These Critical Success Factors could be considered to be a vehicle to identify what was essential for an organisation to focus on should it wish to improve the reporting of incidents.

To gain consensus from a wide community of information security professionals a Delphi study was considered an appropriate method. The study would set out the potential CSF's identified from healthcare and other research and, using a Likert scale, the iterative Delphi process would gain consensus to what elements were considered as critical to improving incident reporting. A wide range of information security professionals will be invited to participate ranging from those belonging to the main professional body, the Institute of Information Security Professionals – the IISP, Information Asset Owner's in government, members of CiSP and other recognised communities of interest. Respondents were given the opportunity to add other factors if they felt warranted inclusion and consideration by the wider Delphi group.

> *Stage 6. Consideration will be given to conducting a validation survey to test the findings of Delphi study*

This enables the testing of the Delphi findings amongst the original participants to ensure any potential researcher bias has not influenced the outcome of the analysis of the Delphi results. It also tested the potential use of the identified CSF's within an Incident Reporting Maturity Model that could be applied by organisations to improve their information security incident reporting. It is intended that the Maturity Model is offered as a potential tool to assist in improving incident volume reporting using a non-proscriptive, iterative, contextual approach.

The use of a control group not previously involved in the studies provided an additional check that the findings are not at odds with security professionals who did not participate in the original Delphi study.

Stage 7. Review the outcome of Critical Success Factors and proposed Incident Reporting Maturity Model.

The analysis of the outcome of the validation study will identify if it is a realistic option for organisations to use to improve security incident reporting.

The research design is summarised in Figure 1-4.

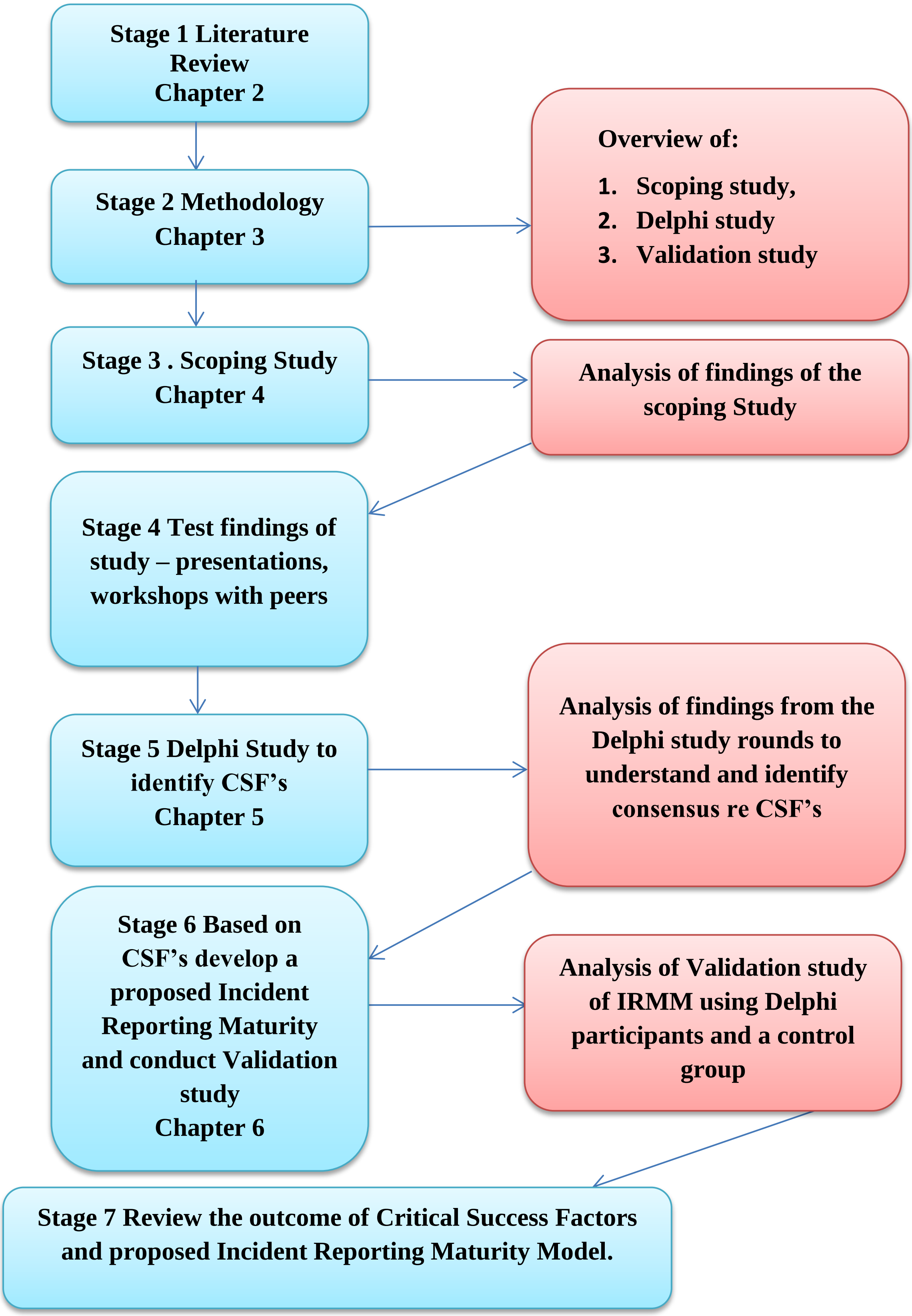

Stage 1 Literature Review
Chapter 2
Stage 2 Methodology
Chapter 3
Overview of:
1. Scoping study,
2. Delphi study
3. Validation study
Stage 3 . Scoping Study
Chapter 4
Analysis of findings of the scoping Study
Stage 4 Test findings of study – presentations, workshops with peers
Stage 5 Delphi Study to identify CSF's
Chapter 5
Analysis of findings from the Delphi study rounds to understand and identify consensus re CSF's
Stage 6 Based on CSF's develop a proposed Incident Reporting Maturity and conduct Validation study
Chapter 6
Analysis of Validation study of IRMM using Delphi participants and a control group
Stage 7 Review the outcome of Critical Success Factors and proposed Incident Reporting Maturity Model.

Figure 1-4 Research Stages in Graphical Form

The Thesis is organised in the following manner;

Chapter 1: Introduction

The introduction of the problem – the increasing reliance on cyberspace and the perceived lack of the reporting of information security incidents and its consequences to support the understanding of the information risk in cyberspace.

Chapter 2: Literature Review

Presents a review of the literature relevant to the subject from the information security sector and other sectors, such as healthcare, where there appears to be more research on incident reporting.

Chapter 3: Methodology

Sets out the overall research methodology outlining the pragmatic approach of a mix of positivism and interpretivist paradigms through the use of qualitative and quantitative questions through surveys, a Delphi study and validation study.

Chapter 4: Scoping Study

This sets out the detailed methodology and approach for the incident reporting scoping study and examines the results.

Chapter 5: Delphi Study

This sets out the reasons, detailed methodology and approach for the Delphi study and it examines the results and consensus of the participants in relation to the Critical Success Factors identified to improve security incident reporting.

Chapter 6: Validation Study

This sets out the approach to the validation study to test the findings and researcher analysis of the Delphi study and propose an Incident Reporting Maturity Model. This uses the original Delphi respondents as well as a control group formed of eligible security professionals not previously involved in any of the previous surveys to judge their views of the findings.

Chapter 7: Summary and Conclusion

This sets out a summary of the research, the conclusions and recommendations including the contribution to research and lessons learnt.

1.9 Summary

This chapter set out the research problem against the context of the growing use and value attached to information in today's world. The assumption made was that information security incidents are being under-reported and that research in this area is limited. It proposed a series of studies that involve security professionals that would seek to ascertain if the assumption of under reporting of security incidents was valid. If so, whether research into incident reporting in other sectors could have the potential to be re-used in the information security arena and to identify what the CSF's to reporting are; with a proposed Incident Reporting Maturity Model that could be used by organisations to judge their levels of maturity against those factors.

It set out the stages of research that were intended to tackle the research goals. It also introduced the conceptual framework which breaks down the components of information and which forms the basis of the literature review which is explained in more detail in chapter 2.

Chapter 2 Literature Review

2.1 Introduction

Chapter 1 set out the context for this research, particularly the concerns surrounding the perception that information security incidents were under-reported. This assumed under reporting and the subsequent potential adverse effect on the amount of empirical data available to support informed information risk analysis and risk management decision making could result in an a more interpretative approach to the available data. In turn this could adversely affect the confidence in the validity of these decisions.

A conceptual framework illustrates where incident reporting is situated in the wider information space with the sections relating to that framework indicated.

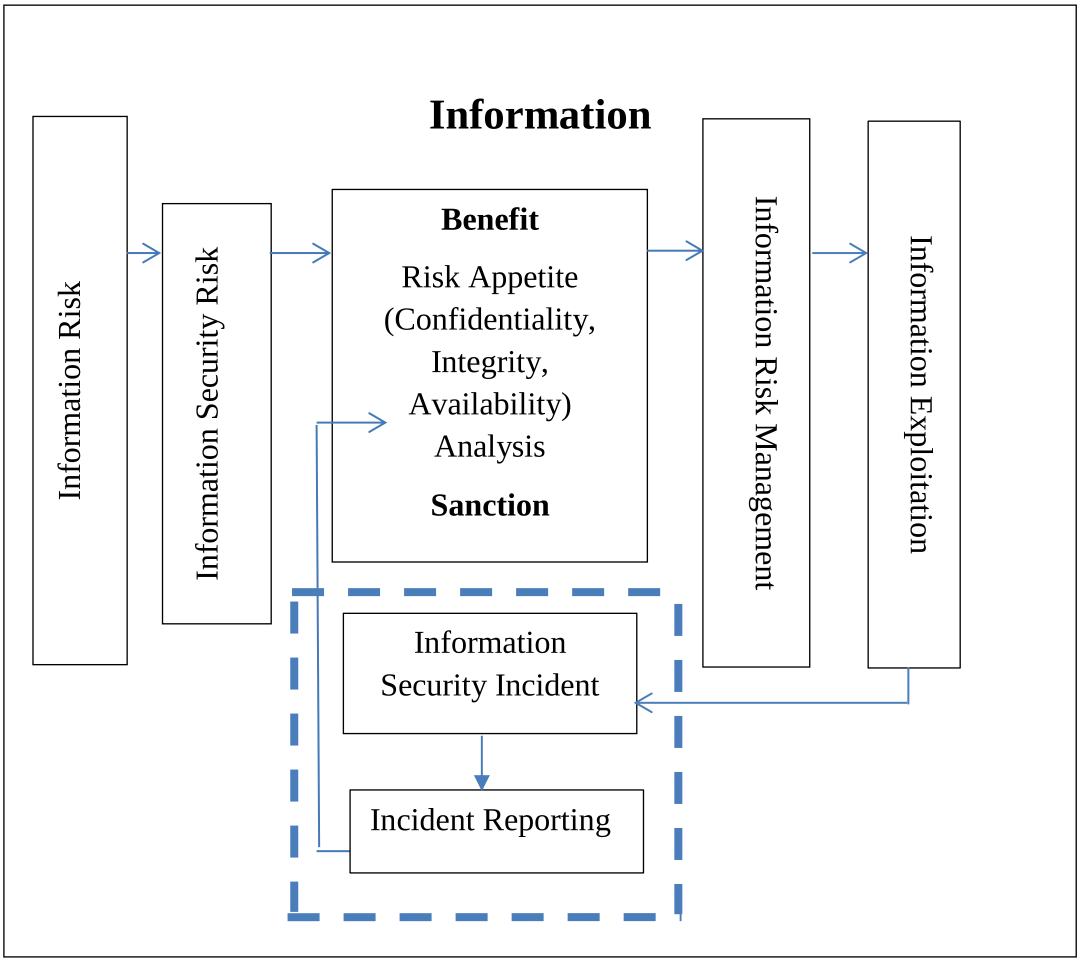


Figure 2-1 The Conceptual Framework

The concept framework is used to structure the literature relating to the relationship between possessing information, the requirement to use or exploit that information, the understanding of information risk, the potential consequences of a loss or compromise (an incident) and sanctions (regulatory, legislative, reputational). It is against these that the risk appetite is formed and finally the risk management process. Should the information risk management fail and an incident occurs, this should in turn create a review of the whole process, providing the incident is reported in the first place. Each of the framework sections are described in more detail together with the identified literature.

In the literature review the structure of the framework is followed except that 'Information Risk' and 'Information Security Risk' are grouped together. 'Information Exploitation' which is the actual use, storage, analysis, and publication etc. of the information that is in the possession of an organisation.

2.2 Key Security Incident Reporting Papers

Early research into information security risk and the relationship between managing risk and applying countermeasures was reported by Birch and McEvoy (1992). They recognised that the value of information stored on the information systems exceeds that of the value of the technology used to store and process it, but this is not always understood by the business. In a similar vein, Willcocks and Margetts (1993) conducted studies into risk assessment and information systems but there was little in their research relating to the outcome of risk management on security incidents. One of the earliest papers on the subject of information security incidents was by Blakley, McDermott and Geer (2002) who commented on the lack of information regarding security incidents and made the comparison that information security is now somewhat in the same position as the healthcare industry was in the 19th century to where it is now. More recently Lagazio, Sherif and Cushman, (2014, p.66) in their study of financial crime in the finance sector report that "underreporting is a major issue". Hove and Tarnes (2013) also report that the Norwegian CERT (Computer Emergency Response Team), despite an increase in security incident reports, believe there is a large number that are unreported or at least not discovered. They continue in that in their three case studies of large organisations to understand security incident management, a common identified theme was the belief of those responsible for dealing with incidents that there is under reporting and that many employees do not report due to not knowing what or how to make such reports. Some employees do not see the value of reporting and some “do not want to acknowledge potential mistakes they made.” (Hove and Tarnes, 2013, p.82). It is not necessarily just individuals who do not report Lagazio, Sherif and Cushman (2014, p.64) suggest organisations also under report;

> “while the banking and cards sub sector claim that the number of cyber security incidents is very low, the financial advisory services sub sector argues that cyber incidents happen on a consistent basis”

They offer possible reasons for this including under reporting and the value of such losses to large companies is negligible therefore implying there is no need to report them. “Even a few hundred incidents contribute to negligible losses” (2014, p.64).

One reason that there appears to be a lack of research is possibly due to the subject matter itself; Kotulic and Clark in their paper “Why aren’t there more information security research studies” (2004) found it extremely difficult to get organisations to respond to or take part in research. In their study, they found extreme reluctance to participate with 42 out of 43 organisations contacted refusing to take part in a field study and that the original 5 companies that took part in a scoping study declined to participate further. Others such as Flores, Antonsen and Ekstedt (2014, p.100) obtained a higher response in their survey managing a 15.2% response and put this down to the sensitive domain of security and the unwillingness to give out information and possibly survey fatigue.

Other research suggests potential reasons why incidents might not be reported. Choo (2011) suggests that organisations that have been victims of a cybercrime incident may be unwilling to report the incident due to a number of reasons which include the incidents not being of a serious nature, a low chance of prosecution and adverse publicity that would follow any reporting made public. It can be the case that where incidents are reported it is often not the company affected that initially reports it, the report will come from elsewhere (Tonsel, Line and Jaatun, 2014).

Parker (2009), when referring to business crimes in his paper on positive and negative security methods proposed that “business managers will find reasons not to report bad news, often looking to blame others.” (2009, p.31). He continues that many security professionals present security risk in negative terms. In other words, something bad will happen, data can be lost, viruses can infect. This is in contrast to presenting the same risks but describing mitigations as benefits and competitive edge. Could it be that one reason people are reluctant to report incidents is the whole security concept is viewed as negative?

However, outside of the information security sector much of the research appears to be found in the healthcare sector. Papers, such as the ‘An Organisation with a Memory’ (Great Britain, Dept. of Health, 2000) which examined incident reporting research across aviation, safety and healthcare, show that incident reporting in the healthcare sector is not all it should be, with many barriers to reporting adverse patient incidents being identified. Its aim was to identify the key factors involved in organisational failure and learning from mistakes. It was these barriers that are used in the scoping study, discussed in chapter 4, to ascertain if there was any potential for them to be recognised as relevant to the information security sector.

Amongst the Dept. of Health paper’s findings was a recommendation to create a national system to collate adverse incidents and enable their analysis. It also suggested this information could be used at a local level as well as nationally. The main point being many incidents were similar in nature and could have been prevented, if only the previous events been recorded, thereby enabling the lessons of those experiences to be learnt. Other research in healthcare regarding incident reporting includes Mahajan (2010) and Haines et al (2008).

Outside of health care a number of reports have been commissioned following high-profile data losses including the Burton (2008) report into the loss of MOD personal Data and the Poynter (2008) review into security at HM Revenue and Customs. These reports made detailed reference to the circumstances surrounding high-profile data loss incidents in the UK but did not specifically consider the issue of incident reporting in general.

The need for research into security incident reporting was identified as was the potential to reuse that conducted in healthcare research particularly that which identified barriers to reporting. This review will examine the available relevant research and by using the conceptual framework to place that research in the appropriate framework flow.

2.3 Literature Review Approach

The following sections provide a brief overview of the conceptual framework components before leading into more detail under each concept heading. It will describe the literature identified relating to each element of the Conceptual Framework. There will inevitably be some crossover of subjects and therefore some of the literature can be relevant under more than one heading. Firstly though is a description of the literature review approach.

When trying to identify existing literature surrounding the research subject of 'security incident reporting' the following approach was used to understand what literature was available. A traditional approach to the literature review of searching against key words was initially undertaken. The initial 'Scopus' search on the three parameters of 'incidents' AND 'security' AND 'reporting' only brought 18 responses of which 14 related to healthcare. Further analysis of the papers identified then gave other potential papers and literature to review. It transpired that little appeared to have been conducted into the subject of security incident reporting and that, although there was literature relating to security incidents, this was more related to after the event as opposed to the reporting of them. As a result, the focus of the review was to identify if research in other sectors could be applied in the information security sector. The review developed to understanding where contributions from other sectors could be used to "improve current knowledge" (Jesson, Matheson and Lacey, 2011, p.15) as to why there may be under reporting of security incident. A wider scan of similar incident reporting topics, such as within the healthcare sector on 'adverse patient incidents' or events reporting was undertaken, even this search sourced limited research.

An adverse patient incident, also known as a patient safety incident, is defined as

> "Any unintended or unexpected incident that could have led or did lead to harm for one or more patients receiving NHS-funded healthcare" (NHS Commissioning Board, 2015, p.88)

This apparent lack of research was supported by one particular report, the Department of Health 'An Organisation with a Memory' (2000) which recognised that research in the healthcare sector on ‘adverse events’ is limited and one of its recommendations was the need for further research in this area. The apparent limitations in the depth and amount of research undertaken in the subject of security incident reporting identified that this research topic could be of value and contribute to the increasing interest in the subject of cyber security and information assurance.

In addition to conducting research on published literature and papers, another recognised method of understanding whether there was a concern regarding reporting was to engage with professionals and practitioners at relevant conferences and other research networks (Easterby-Smith, Thorpe and Lowe, 2003). As a result, although this research initially intended to focus on the subject of incident reporting, it soon became apparent the problem appeared to be surrounding the issue of under-reporting. This research identified knowledge gaps and potential opportunities to consider a more refined research question based on the potential reuse of research already in existence in sectors other than information security. The outcome supports the view of Collis and Hussey (2009) that a preliminary review of research can assist in providing context for identifying the research question which has been developed in chapter 1.

2.4 The Literature Review of the Conceptual Framework Elements

In the following sections each of the elements of the conceptual framework are examined in more detail

2.5 Information Risk and Information Security Risk

Ultimately the use of any information should factor in the risk of a compromise to its confidentiality, integrity and or availability. These three terms set in their security context are defined as;

> “Confidentiality: Property that information is not made available or disclosed to unauthorised individuals, entities or processes
>
> Integrity: Property of accuracy and completeness
>
> Availability: Property of being accessible and usable upon demand by an authorised entity”
>
> (British Standards Institute ISO/IEC 27000:2014)

These three elements are often referred as CIA. An incident is the manifestation of a risk which has a number of definitions. The UK Health and Safety Executive define risk as;

> "A risk is the likelihood that a hazard will actually cause its adverse effects, together with a measure of the effect." UK Health and Safety Executive (2013).

Whereas, elsewhere there are different definitions. The section will demonstrate there appears to be a lack of common definition and propose a working definition of information risk. The growing recognition of the value of information is now beginning to be recognised in state organisations and private companies and individuals (Horne, 1995; Moody and Walsh, 1999; Keohane and Nye, 1998). Although it covers information risk this research section is more focussed on information security risk, and recognises the real threat to that information from cyber-crime and attacks as a national security issue has grown as a result of greater use of the internet.

> "If there is a single cross-cutting issue that has changed the landscape for serious and organised crime and our response against it, it is the growth in scale and speed of internet communication technologies." (National Crime Agency, 2014)

Ultimately the use of any information has to factor in the risk of a compromise to its Confidentiality, Integrity and or Availability.

Information security professionals may face uncertainty when assessing risk though analysis or assessment. This is partly due to the apparent lack of empirical data to provide confidence in potential likelihood of a risk, evidenced by way of past occurrence. This makes for a real difficulty in making a proper assessment as. Parker (2006, p.3), when referring to risk assessment and analysis suggests "there is not enough valid data to make risk assessment a straightforward and successful method". However, he continues this is not a reason to abandon such assessments. In the absence of known facts situational awareness and contextual knowledge of the business environment come into play. This is illustrated in Baskerville's (1991, p.756) assertion for the professionals need for the "a priori approach", or previous experience, and understanding within the context of the environment they work in. Currently security professionals do not appear to have a choice other than to use their contextual ‘a priori’ skill.

Adams (2003, p.2) proposes there are three kinds of risk that are perceived; through science such as a known disease; those perceived directly such as falling from a tree and thirdly virtual risk where it is not known or cannot be agreed up on. As illustrated in figure 2-2.

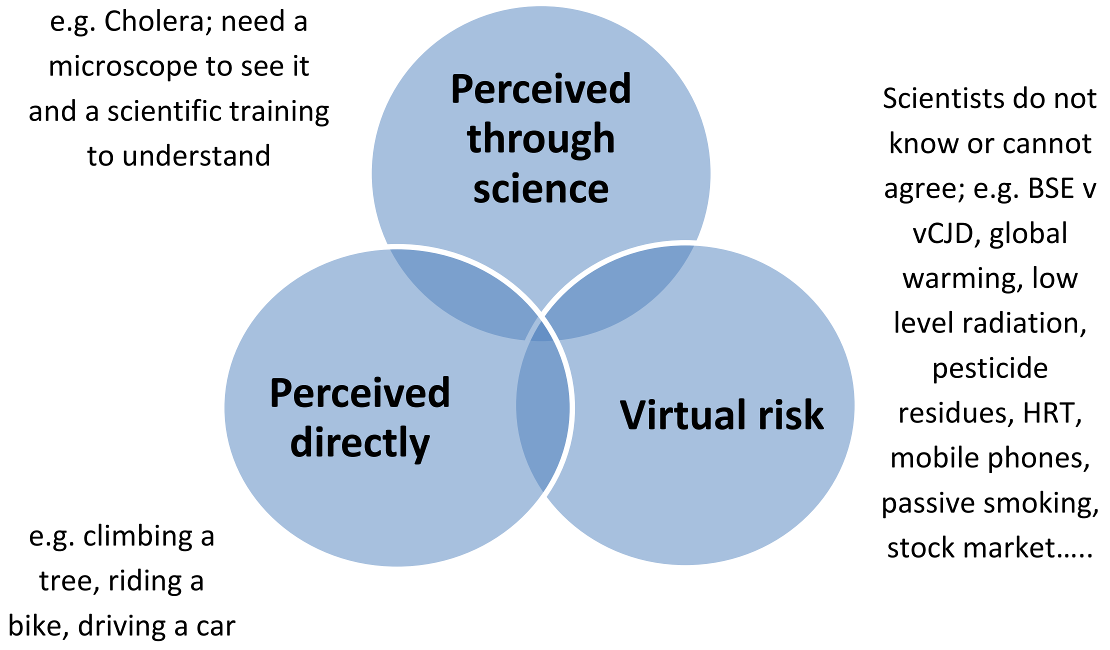

e.g. Cholera; need a microscope to see it and a scientific training to understand
Perceived through science
Scientists do not know or cannot agree; e.g. BSE v vCJD, global warming, low level radiation, pesticide residues, HRT, mobile phones, passive smoking, stock market.....
Perceived directly
Virtual risk
e.g. climbing a tree, riding a bike, driving a car

Figure 2-2 Adams (2003, p.2) Three Types of Risk

Information security risk could potentially fit across all three. Those perceived through science equating to the threat from cyber criminals using known vulnerabilities, computer viruses and other malware. Those perceived directly where information is compromised through known experience such as deliberate compromise by disgruntled staff; or important papers lost on a train or a CD going missing in the post. The virtual risk could equate to the real types and volumes of incidents are not known therefore it cannot accurately be quantified. It is these perceived but not necessarily experienced cyber security risks that could be considered virtual risks and therefore can be argued as adding to that element of the unknown.

Hurtzburg (2007) suggests a typology of risk perceptions characterised in cartoon form relating to the cultural theory of groups; these being Fatalists, Hierarchists, Individualists and Egalitarian. He describes each group with risk in mind as;

> *Fatalists* "Perhaps most of the people most of the time, having little control over the forces that buffet their lives."
>
> *Egalitarians* "Precautionary – if you cannot prove something to be safe you should assume it is dangerous.2
>
> *Hierarchists* "Institutional risk managers. They make rules and enforce the rules" often through knee jerk reactions to an event and have become risk averse, examples being Health and Safety Inspectors"
>
> *Individualists* "More optimistic – if you can't prove it is dangerous assume it is safe." (Hurtzburg, 2007, p.4)

Hurtzburg's (2007) view being that institutional risk managers fit the 'Hierarchists' group and it can be argued that certainly there are some hierarchic information risk managers who will not move away from rules and conduct knee jerk responses. However, the reality of managing information risk is accepting that, where information is needed to be exploited by a business, there will be an exposure to risk and this risk has to be managed and not avoided at all cost. The notion of risk appetite (and its subsidiary, risk tolerance), in relation to information risk is gradually being adopted across UK Government as part of any risk management approach. The UK Technical Risk Assessment Document IS1 referred to risk appetite as "logically a function of the organisation's capacity to bear risk, which should not be exceeded" (Great Britain. CESG, 2012, p.44). It continued by describing the close relationship between risk appetite and risk tolerance where it suggests that risk tolerance is the more fine grained approach to amounts of risk acceptable to particular systems or projects.

To make such decisions there needs to be an understanding of the threat and either locally or collectively such information needs to be available. (Jones, 2002) This requires the sharing of knowledge and understanding of the fact that incidents have occurred and what caused them. The revised UK Security Policy Framework (Great Britain, Cabinet Office, 2014) highlights its intention is to focus on outcomes that will enable proportionate risk management enabling government to operate in a way that maintains effectiveness but is still safe and secure. It is about getting the balance right.

Ultimately the use of any information should factor in the risk of a compromise to its confidentiality, integrity and or availability. An incident is the manifestation of a risk but what is understood by the term risk in the information security sector. Again, there appears to be a lack of common definition.

2.5.1 What is Information Security Risk?

The 2013 EU Commission Directive on "measures to ensure a high common level of network and information security across the Union" provides the definition of risk as "any circumstance or event that having a potential adverse effect on security" (EU Commission, 2013, p.19). In the security sector HMG's risk assessment, standard IS1 defines risk as "The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation". (Great Britain, CESG, IS1.2009, p.106)

In summary, some definitions refer to likelihood and others potential. To some extent similar words and both therefore need a benchmark to understand; has the event happened before and how many times on the assumption that the more occurrences of an incident, the more likelihood or potential for that risk to occur again. As there is a lack of a common definition of an incident, this thesis proposes a working definition of information security risk which will be used to provide clarity to this study. The definition extracted from review of the literature and used in the data collection phase is;

> *An information risk is an actual, perceived or virtual hazard faced by an information asset that, if realised (whether predicted, expected or presumed), through chance or probability may adversely affect or impact that information asset's Confidentiality, Integrity and or availability; thereby potentially becoming an actual incident or a near miss.*

In the above proposed definition virtual is used through interpretation of Adams (2003, p.2) risk model where he refers to virtual risk where there is no agreement of the type of risk as opposed to those perceived directly or through science (in other words a known risk).

2.5.2 The Need for Metrics to Understand Security Incident Risk

To understand these emerging risks and threats there needs to be usable data to assess them in a focussed and practical way. This is needed, particularly where there is regulatory control on securing customer data and information such as in the United States the Sarbanes Oxley Act 2002 and the Health Insurance Portability and Accountability Act 1996 (HIPAA) and in the United Kingdom the Financial Conduct Authority. Trusted empirical evidence or metrics on security incidents would normally be required to enable the formulation and interpretation of any risk assessment. Davenport and Harris (2010, p.3) argue that such regulatory oversight leads to the demand for better metrics and risk management models. Jones (2002) argues for the need to develop metrics to assist measuring the effect of vulnerabilities and later compares the way insurance companies use metrics in order to decide levels of premium against risks based on historical information. Baker, Wade and Tippett (2007) suggest that "metrics to quantify risk factors" are one of two elements required to enable a focus on threat the other being risk reduction strategies.

The United States Department for Homeland Security's (2009) Cyber Security Roadmap recognises the need to have metrics. The European Commission has also referred to this requirement suggesting that ENISA and National Authorities conducting similar work, such as the UK Centre for Protection of National Infrastructure (CPNI) should be in possession of the means to perform their role. This should include powers to access

> "comprehensive and reliable data about actual security incidents that have had a significant impact on the operation of networks or services." (EU, 2009, p.15 section 44).

The flaw in this being assuming "the power" to access the data relies upon data on incidents being available in the first instance.

It is not just in the cyber world that such information is required; following the UK HMRC data loss a review of data handling procedures was commissioned. This report also identified the practical issues surrounding the increased use of technology and risks and threats to information. The UK Data Handling Procedures in Government report (2008) suggests that the task of managing information risk for public sector organisations is likely to be harder in future due to the ever-changing technology and external threat. Particularly as the drive to become 'digital by default' in the UK permeates through those services delivered to the public. The term Digital by Default is described in the UK 2013 Government Digital Strategy, as:

> "Digital services that are so straight forward and convenient that all those who can use them will choose to do so whilst those that can't will not be excluded" (HMG, Cabinet Office, 2013)

The UK Govt. in recognising the concerns surrounding incidents included the aspects of incidents in its security policies

> "Departments and Agencies must have robust and well tested policies, procedures and management arrangements in place to respond to, investigate and recover from security incidents or other disruptions to core business." HMG Cabinet Office SPF v11 (Oct 2013, p.17).

The US Department for Homeland Security (2009) Cyber security roadmap concurs with Davenport and Harris's (2010) view suggesting that such metrics can steer investigations into the true cause of security incidents. The roadmap suggests that use of information on events that already exists should be gathered. This would produce "a list of metrics that might have avoided the incident if they had been known before the incident" (2009, p.19). The roadmap's long term objective being to foster the development of metrics and data collection schemes that produce actuarial-quality data on information security incidents. Although there appears to be a lack of information on incidents, and that can affect risk analysis even if more facts were known it is generally accepted that there is always an amount of risk that cannot be mitigated. The insurance industry is in place to cover on of the key mitigations, that of risk transference. The next section examines the emerging provisions and challenges in providing such transference of risk.

2.5.3 Information Security Risk and Insurance

Earlier in Chapter 1 the assertion is made that information security professionals appear to have little empirical evidence on which to factor into information risk assessments. In this respect the insurance industry is faced with similar problems when insuring against information or cyber security risk. The cyber insurance market, compared with the home or car insurance market, is in its relative infancy and began to emerge in the 1980’s (Bohme and Schwartz, 2010) although this is different to that suggested by Majuca, Yurcik and Kesan (2006) who believe it to be the late 1990’s. Whatever its actual start dates however the need for a strong cyber insurance market is supported by Gordon, Loeb and Sohali (2003).

Traditionally the insurance industry make risk based decisions against known historical and empirical data (Jones, 2002). They can quote a premium for a wide range of policies (car, home or life) based on factors such as age, location, type of vehicle, occupation, number of bedrooms and lifestyle. These decision influencing factors obtain information from other nationally or locally collated accepted data sources such as accident statistics, crime figures and death rates. Although insurance companies have a long historical experience in managing risk (Ashenden and Jones, 2005) the challenge is when conducting information security insurance risk assessments with little empirical evidence upon which to base any assessment and “hinder competitive pricing” (Bohme and Schwartz, 2010, p.2). In the absence of such information how can insurers assess the risk to provide adequate cover against information loss. This is also the view of Majuca, Yurcik and Kesan, (2006, p.13) who observe that “risk-metrics need to be developed to sharpen the estimation of risks.”

Gordon, Loeb and Sohali (2003) identified the problem faced by insurers providing cover in the cyber world because of the limited information on security breaches, exacerbated by the reluctance of companies who do not reveal details of their security breaches. Against this backdrop of lack of information some insurers have still managed to put a value against the risks. Gordon, Loeb and Sohali (2003) note that *“*They have quantified what some claim as unquantifiable risk.” (2003, p.82). One of the risks identified for insurance companies was that of those who felt most at risk may be more likely to seek insurance against this, possibly as a cheaper option than spending money on security. According to Gordon, Loeb and Sohali (2003) to mitigate this insurance companies use the analogy of the ill person wanting insurance against the well person. How do insurers assess the differing risk? They achieve this by subjecting those who wish to be insured to a health check, where lifestyle and previous medical history can assist in determining the level of exposure to a future claim.

There needs to be an equivalent for companies requiring information risk insurance. Gordon, Loeb and Sohali (2003) suggest that companies more likely to suffer an information security breach would be disposed to buy insurance as opposed to those with a lower chance of such a breach. This assumption does not appear to be based on hard evidence as it could equally be argued that firms assessing themselves to be very secure may still determine it is good practice to insure themselves in the same way as healthy people still buy health insurance. Gordon, Loeb and Sohali (2003, p.83) continue their comparison with other types of behaviours regarding insurance where they suggest those who have purchased fire insurance may be less likely to take necessary preventative steps as those who do not have fire insurance. The argument may be flawed as it is likely that householders who have good locks and an alarm system will insure against burglary using these protective measures as discounts off their premium and that not having basic security significantly increases the likelihood of being burgled (Association of British Insurers, 2017).

The other side to this could be described in the same way that many people have health insurance - because it is considered sensible to do so, likewise for house and life insurance. To some extent Gordon, Loeb and Sohali (2003. p.82) state the obvious in that it is "for insurance firms to identify high-risk users and differentiate the premium." Their paper gives the example of one firm of insurers charging a company a higher premium just because they were using Microsoft NT software. "Thus Wurzler [an insurer] treats the use of NT software as precondition, much like a life insurance policy treats smoking or high blood pressure." (Gordon, Loeb and Sohali 2003, p.82). They also suggest how insurance companies and the insured can reduce costs or risks through a Cyber Risk Management Framework (see figure 2-3) in a straightforward insurance risk of one company preventing attack and through insurance reduces the financial risk of loss through insurance either to themselves as the first party or subsequent loss to a third party.

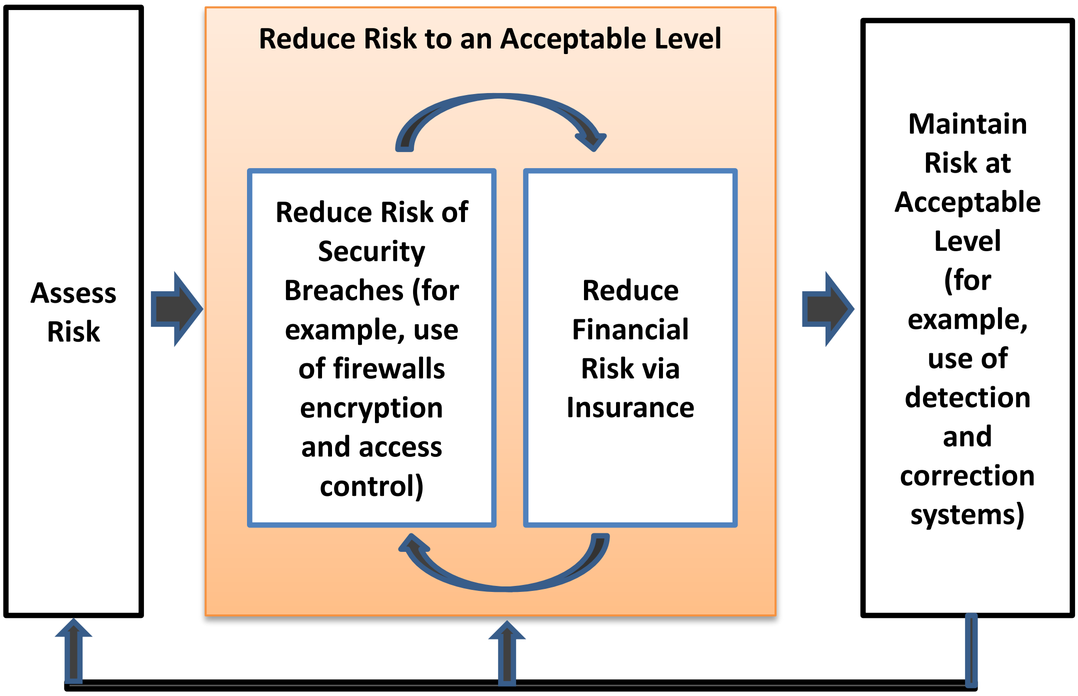

Assess Risk
Reduce Risk to an Acceptable Level
Reduce Risk of Security Breaches (for example, use of firewalls encryption and access control)
Reduce Financial Risk via Insurance
Maintain Risk at Acceptable Level (for example, use of detection and correction systems)

Figure 2-3 Cyber Risk Management Framework. (Gordon, Loeb and Sohali, 2003, p.84)

The nature of service provision today could involve other parties, for example where an insured company outsources some of its work to a third party or is a customer of another company and their IT is connected in some way to support the business. The hypothetical example below (figure 2-4) illustrates a scenario that may complicate the provision of information security insurance. There are dangers that have not yet been perceived by companies in that their assets may not be directly attacked, but some of their equipment may be hijacked for the criminal purposes.

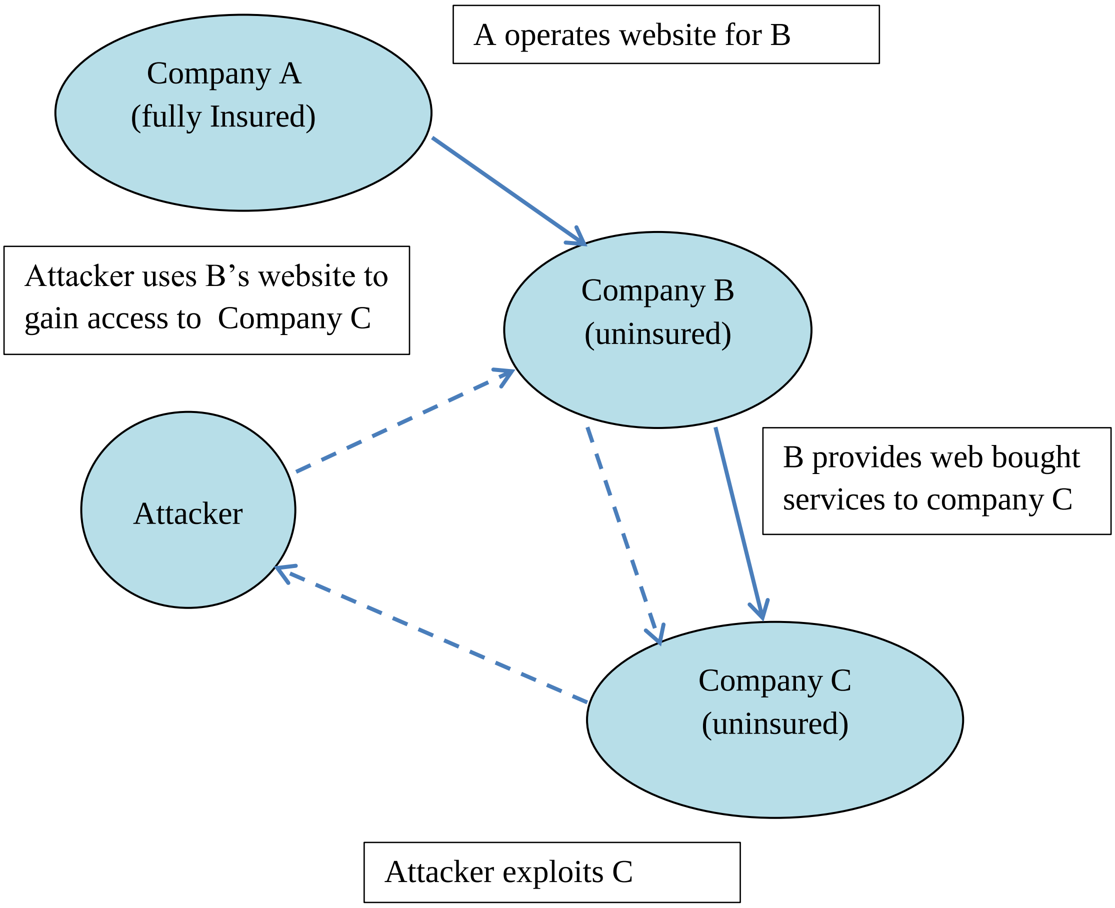

A operates website for B
Company A (fully Insured)
Attacker uses B's website to gain access to Company C
Company B (uninsured)
Attacker
B provides web bought services to company C
Company C (uninsured)
Attacker exploits C

Figure 2-4 Illustration of the Challenges for Insurance Liability

Instead of intruding into their network, the attacker uses their IT resources to mount an attack elsewhere. In this example Company A is fully insured against cyber security attacks and breaches. Company A operates company B's website, who are not insured, which offers goods and services. Company C, also not insured, is a customer of company B. An intruder then exploits a vulnerability in Company B's use of the website provided by company A and then, using company B's connection to its customer's, attacks assets belonging to Company C. Company C subsequently suffers a data breach which results in, for example, adverse media attraction. As a result, at worst, Company C goes out of business, but even if it only suffered a degree of financial difficulty the chances are that Company C may seek recourse to litigation against Company B who in turn will seek redress from Company A.

Even if the attacker is caught, should it transpire that Company A and/or B were found to be deficient in their security arrangements litigation could be aimed at both by company C. Company A's insurance may or may not pay out depending on compliance to any terms and conditions in their indemnity policies and it could be the bill for litigation and compensation would fall upon both company A and B who could be sued for poor security which allowed the offender to easily exploit their vulnerabilities.

Who is liable? That is one for the lawyers and outside the scope of this research. Company B could say their site was only compromised by company A's poor security and therefore Company A should reimburse company C for the loss of customer data and be responsible for the breach. Do insurers have to consider including conditions of insurance that companies have to be diligent regarding the security of any third party they do business with? Would these be pre-requisites to being insured or a factor that may affect the premium or whether any pay-out is made subsequent to a breach? At present there is insufficient historical information for insurers to have the same level of confidence in assessing risk and premium they currently have in other risks. Gordon, Loeb and Sohali (2003) highlight this issue by stating as information security or cyber security is relatively new and the normal process on basing price the risk is based on actuary tables these do not exist and this is further exacerbated by the fact that firms are reluctant to reveal details of security breaches.

2.6 Risk Assessment - Benefit v Sanction

The focus of this research section is around the risk assessment and the analysis of benefits against sanctions. There are, as would be expected, many methods and styles of assessment. All at some point use the elements of benefits against sanction which factor in impact and likelihood. Impact can often be understood in business terms; how long can a company or process survive without access to data before there is a level of disruption? However, without sufficient accurate information on the type and number of incidents that do occur, assessing likelihood can be a challenge. There is a need for meaningful assessment in order that organisations can make business decisions (Jones, 2002). The current assumption is that the true number of incidents and near misses is not known and therefore only a proportion of incident data is available to analyse to understand the problem. If any perceived barriers to reporting are reduced, it should logically follow that more incidents would be identified, thereby adding to the overall incident knowledge and subsequently improve the confidence in the outcome of analysis, sharing and usage of that incident data.

The conceptual framework shows the balancing of benefits against any sanction of the use of an information asset against the likelihood of anything untoward occurring. It is then the benefits against any sanctions that may result that are assessed. This is often referred to as a risk assessment. Risk assessment is described the overall process of risk identification, risk analysis and risk evaluation. (British Standards Institute, ISO/IEC 27000, 2014) It is here that the challenge sits as to properly assess such risks the assessment would need to understand the likelihood of an adverse event taking place. In the same way as there is a lack of empirical data on incidents Parker (2009) argues that there has equally been a lack of any studies into the "validity and accuracy of security risk assessments in practice" (2009, p.32). The risk models may be present but their usefulness has not been subject to rigour. The apparent lack of empirical incident data would a factor in any criticism of their true effectiveness. Parker (2009) proposes that security risk assessments should in fact come with a health warning that they are likely to be "incomplete and subjective" (2009, p.33). The situation has obviously not improved in his perception as previously Parker three years earlier (2006) in his paper 'Making the case for balancing risk based security' referred to the problem of there not being enough valid data to make risk assessment a straightforward and successful method. He argues that although there should be efforts made to improve this (although he does not suggest how) he doubts this will be achieved.

The ever-increasing growth and reliance upon computers, systems and infrastructure, together with the increasing criminal activity that exploits this growth of data means there is "no hope of ultimate success of risk management and assessment" (Parker, 2006, p.3). Dalkey (1969) refers to there being a spectrum of inputs; ranging from speculation through to knowledge. In between lies opinion which he believes is the flattering name for the collective 'products of judgement, wisdom, insight and similar intellectual processes'. (1969, p.2) The lower the probability of truth, or as can be extrapolated into knowledge of security incidents, results in more speculation as opposed to true knowledge. Using Dalkey's model (figure 2-5) the suggested lack of empirical evidence on security incidents would suggest that risk assessment and judgements on countermeasures may be more based on speculation and opinion rather than evidenced knowledge and therefore informed opinion.

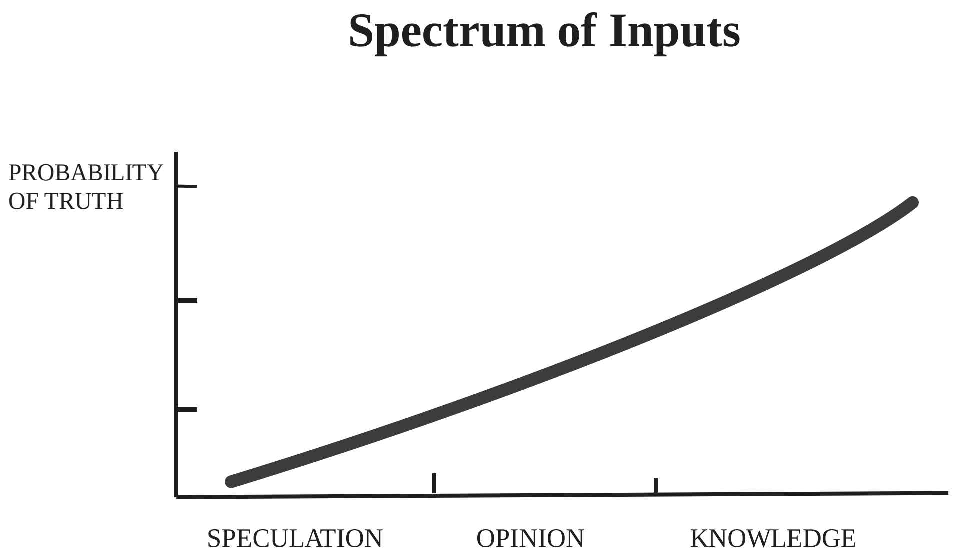


Figure 2-5 Based on Dalkey, N (1969, p.3) Spectrum of Inputs

2.6.1 Assessment and Analysis of Risk – Interpretivist or Positivist

When assessing the potential impact of loss, the calculation requires data to understand the potential likelihood of an incident that causes loss. Perry and Moffat (2004) in their paper on information sharing in a military environment identified that to make informed decisions certain elements of information need to collated and assessed as part of a process. They proposed an ‘information superiority reference model’ which incorporated “Situational awareness, shared situational awareness, collaboration, and decision making” (Perry and Moffat, 2004, p.xvii). It is interesting to note that part of the model requires prior knowledge, a concept referred to by Baskerville (1991) who describes the notion of risk analysis as professional interpretivistic knowledge. Baskerville (1991) outlines his position on the weaknesses of the positivist philosophical use of risk analysis against, in his view, the more important element of an interpretive use to which risk analysis can be deployed, particularly where it considers the professional and contextual, understanding of an information system and its controls. He examines the potential for risk analysis not to be considered in the same vein as other analysis methods that have empirical statistics available, but places it in an interpretative position.

Baskerville's (1991) focuses on two aspects of security risk analysis. The first from a positivist scientific method, the second as an interpretative scientific method. He states his paper's purpose is to "debunk much of the criticism of risk analysis as a tool" (1991, p.749) particularly recognising that risk analysis is used by information security professionals to support them in their role. He outlines his position on weaknesses of the positivist philosophical use of risk analysis as opposed to his view of the more important element of interpretive use to which risk analysis can be deployed. Particularly where it takes into account the professional and contextual understanding of a particular information system and its controls. He strongly argues that there is a place for risk analysis, despite the lack of empirical figures to populate any method of calculation, and that the professional experience of those charged with risk analysis should be recognised more. He suggests that improving the volume of evidence related to reported incidents could damage the 'priori knowledge' element of risk analysis.

> "Improving the positivist scientific accuracy of the statistical representation simultaneously reduces the interpretive scientific accuracy." (1991, p.756)

However, he also recognises that the lack of empirical evidence makes the findings of many risk analysis processes difficult to prove or disprove. It is this recognition that weakens his argument that more information could hinder rather than improve the analysis process. It is possible that any increase in the amount of statistical data to add to the risk analysis mix would still not be sufficient in accuracy to place it in the positivist area of risk analysis. It is far more likely to add value and enable more confidence in the 'a priori' knowledge of the individual to make sound interpretative risk judgements by utilising that additional information in the context of the risk environment they are analysing. Baskerville (1991) proposal that a professional security practitioner has values and 'a priori' knowledge can interfere with empirical observations. In other words the colloquial comment or views from a typical security manager such as 'in my experience and knowledge that cannot be right' will form a significant part of any risk assessment. When this inference is in play then it could be argued the risk analysis is interpretive.

Baskerville (1991) suggests that as security events are many and varied in nature, to enable an exact recurrence at a later date and therefore making any post incident examination will be very difficult. He continues with the view that such use of experience and knowledge makes for difficulty in stating any such study being a real science. Baskerville (1991) argues that risk analysis is also an important communication artefact. "It facilitates the translation of highly structured management decision data." (1991, p.757)

It would take some considerable time for complete confidence that all incidents are reported and, more importantly, properly categorised to allow sufficient reliance upon their accuracy. Irrespective of the amount of empirical evidence on incidents being available Baskerville (1991) asserts his view that a generalist or novice will not possess the 'a priori' professional knowledge and experience which is necessary to correctly interpret the complexity and context of specific organisational settings (1991, p.758). This view clearly indicates that Baskerville does not feel security risk assessments can be completely conducted in a positivist scientific manner. He maintains that even if all incidents are reported, there is still a requirement for experience, knowledge and understanding to interpret the findings of any statistical positivist output.

2.6.2 Other Approaches to Risk Assessment

Birch and McEvoy (1992) propose a different model. Their paper outlines an integrated approach to information risk analysis for information systems and sets out its own methodology - SRA (Structured Risk Analysis). It is stated this method has been used in the finance sector and elsewhere, specifically mentioning the European Space Agency (1992, p52). By removing some of the complexities that are found in safety critical applications the authors believe SRA can be adapted for Information security - termed SRA-IS. Their paper sets out a process that could be followed for Information Systems risk analysis by identifying the workflow of a system. In their introduction Birch and McEvoy (1992) suggest risk analysis must be able to answer the following questions:

> "How much is it appropriate to spend on countermeasures?" and
> "Where should spending be directed?" (1992, p.44)

The paper argues that, just as a system that is compromised can cost thousands in monetary terms, so can over spending on countermeasures in the first place. It should be recognised that at the time of writing this paper, 1992, the amount of compliance legislation surrounding data loss/ data breach was less than now. Therefore, the simple cost of loss versus cost of prevention now has additional factors to consider – fines by regulators or even the courts. The issue of reputational damage is not considered either in this paper. Again, they focus on countermeasures being the lead concern as opposed to risk management.

> "It is important an organisation has the best possible information on risks in order to decide whether or not to invest (scarce) resources in countermeasures and if so how much." (1992, p. 44)

Even in 1992, Birch and McEvoy's paper recognised that the value of information stored on the information systems exceeds that of the value of the technology used to store and process it. They argue that the main purpose of risk analysis and risk management is not solely for the determination of appropriate countermeasures (Ibid.1992) This is an interesting point, as it could be argued that the then mandated risk assessment methods such as the UK government's IS1 (Great Britain. CESG, 2012) for example, relies on assessments that relate to a pre-defined set of baseline controls. According to the asset value, the degree of control that should be applied to counter the threat is identified and either applied or reasons stated why the control is not applicable. The element of risk assessment only comes into play when, for whatever reason e.g. funding or lack of, technology legacy or operational reasons, certain countermeasures cannot be put in place. Therefore, the residual risk tends to be that which is not catered for due to the non-implementation of certain, most or all countermeasures identified as necessary to counter a specific threat.

Birch and McEvoy's (1992) paper argues that the approach of having tick lists of risks and countermeasures to those risks does not always cater for all risks. There is always a concern that perhaps all risks have not been identified in the context of the use of that system. The risks around protecting the data on the system were no doubt considered but the import and export of data, in particular large volumes of it, may well have not been on any tick list.

2.6.3 An Intuitive Approach to Risk

To understand if something may happen, past history is a good indicator. If that history is not available or only partly understood that can create difficulty. The research undertaken by Kahneman and Tversky (1977) on 'intuitive prediction' could be considered relevant here. They state that

> "many prediction problems are essentially unique in the sense that little, if any, relevant distributional information is available" (1977, p.2-1).

Distributional information, in a risk analysis context, being the information on numbers and types of reported incidents relevant to the information asset subject to that analysis, thereby enabling a more accurate analysis of the risks being assessed. Kahneman and Tversky (1977) identify the other element required for decision making as 'singular' information which describes the components of a problem that make it stand out from the rest. One aspect of mitigation, that is rarely considered, is to revisit the actual use of a system once it has been implemented to ascertain if it is being used in the manner for which it was originally designed. If any changes have taken place, has a review of the original risk analysis taken place to consider this change?

One paper that focuses on the lack of empirical data to enable accurate risk analysis is Baker, Rees and Tippett (2007) who call for more data, but do not go into detail about how to achieve this. They suggest creating some kind of coding for the risk and threat assessment which, in turn, if the threat occurs, it is already coded. However, they counter their own suggested benefit of pre-coding by recognising many other factors can come into play and, if included the final decision on the type of threat, the true incident code may be difficult to understand. Baker, Rees and Tippett, (2007) note even if data was forthcoming the problem of the lack of clear definitions still exists;

> "Current approaches recommend and employ estimates for such critical factors as frequency and countermeasure effectiveness because no clear and accepted framework exists for what real world measurements are needed to drive risk models or how they are to be collected." (Baker, Rees and Tippett, 2007, p.102)

This underlines the current predicament of a lack of data and how to share commonly occurring, but not similarly coded or classified incidents. Adams (2003) comments on risk in general as opposed to information risk. He argues everyone has "A propensity to take risks [which] leads to risk taking behaviour, which leads, by definition, to accidents," (Adams, 2003, p.6). He suggests responses to risk and risk averseness are in some part affected by the knee jerk reaction to events. This reaction can often occur before all the facts are known. Perrow (1984) also describes this approach of organisations after an incident, introducing short term reactive actions as opposed to taking a longer-term view by stating there is a need for;

> "long term strategies for handling risks rather than short run tactics of posting safety notices or levying trivial fines." (Perrow, 1984, p.63)

2.7 Information Risk Management

This section covers the need for risk management and how the apparent lack of empirical data from reported incidents can make this difficult. It builds on the previous section to manage risk down to prevent or reduce damage, loss or harm and reduce the likelihood of incidents or events occurring. This thesis offers the suggestion that significant risk management and investment is currently decided upon despite a lack of real evidence. The result being information security professionals making value judgements based on experience, together with some local or sector wide evidence of actual known incidents. Information risk management relies upon an understanding of the overall contextual security situation (Webb, Ahmad, Maynard and Shanks, 2014). One of the indicators of this awareness being knowledge of security incidents that have or are likely to occur. It is this reliance upon that awareness, where some key aspects are not fully understood (incident data) that this lack of knowledge approach is unlikely to be accepted in other risk based industries. Whilst experience and judgement is a necessary factor in risk based decision making these should be based on sound information.

The public may not be satisfied or reassured that safety decisions were not, as would be expected, based on the results obtained by thorough investigations and assessment of incidents, but on a professional's best endeavours. For example, it is inconceivable that, as a result of lack of information sharing and reporting on previous near misses and safety incidents, lessons learnt were not being factored into new aircraft designs. Why is it that information security incidents are not considered in the same light?   The next section will articulate the value in the reporting of incidents and examine a wider concern that the perceived lack of incident reporting has on traditional risk assessments.

As early as 2001 the Information Assurance Advisory Council (IAAC), in conjunction with the then National Infrastructure Security Coordination Centre (NISCC), published a joint report 'Sharing is Protecting' where it was clearly highlighted that;

> "In order to help managers and directors to make informed decisions about the risks they face and to demonstrate their exercise of due care and compliance with corporate governance obligations, IAAC and NISCC urge organisations to share information about Information Assurance incidents and threats.' (2001, p.2)

It also identifies the growing recognition that information security should be considered as a profession in its own right.

In todays interconnected world it is important that information security is not seen in isolation. Information security risk management should be part of the business and not just a technical matter (Ashenden and Jones, 2005). Elsewhere Blakley, McDermott and Geer (2002) suggest that information security is information management and state "information needs to be gathered about security incidents experienced by businesses worldwide" (2002, p.100). This is another example of a research expressing the need for metrics, but not how to achieve it. The information security sector appears to experiencing this lack of information. It may be just a problem associated with the information security sector or, as can be seen by research elsewhere, such as in health care, the issue is wider than any one sector.

As mentioned earlier in this chapter Blakley McDermott and Geer (2002) do offer comparisons to the healthcare industry from where it was in the 19th century to where it is now. Certain treatments and medicines worked but more was known about the outcomes of an illness and less about the cause and there was no real data collection. Blakley McDermott and Geer (2002) suggest there were three important developments that helped shape and modernise western medicine;

> "Mandatory professional education and licensure of practitioners
> Systematic collection and study of public health data
> Systematic observation studies of safety and effectiveness of treatments."
> *(*Blakley, McDermott and Geer 2002, p.101*)*

Blakley, McDermott and Geer (2002) continue by suggesting the information security sector consider introducing professionalism and a code of ethics, including the duty to report, in other words what the medical profession has in place now. They also refer to the fact that, as yet, no information security equivalent to ‘The Lancet’ exists to which security professionals can refer to for recognised published research. However, as can be seen later in the review of healthcare research, for example the Dept. of Health (2000), although the three elements cited above may be present in healthcare now, the ability to report on adverse patient incidents is far from perfect.

2.7.1 Professionalism in Information Security.

As professionalism is referred to by Blakley (2002) as a key element, this next section examines professionalism in the information security sector. It took some time for the medical profession to get where it is now but already some movement has started in the information security sector. Boards and leaders of organisations will normally take advice on legal and financial matters from staff or consultants who are members of professional bodies to provide an element of assurance and protection that due diligence in their decision masking can be evidenced. As boards understanding of the risks in cyber security and associated risks grow, as demonstrated in a top ten topics for directors in 2015 (Nili, 2014) which places Cyber Security at number two, they would be expected to seek advice regarding information risk and cyber security. It would therefore be a logical progression for boards to seek professional cyber or information security advice. Although electronic communications have been developing for longer than a century and professional bodies in fields supporting this such as electronic engineering have developed there is not the same range of professional bodies for information or cyber security (Jones and O’Neill, 2017, p.4).

In the UK, professional bodies such as the Institute of Information Security Professionals – IISP have been set up and professional certification schemes such as the UK HMG CESG Certified Professionals scheme (HMG CESG, 2015; see glossary) for competency based certification of Information Assurance professionals are in their infancy. These will take time before a tipping point is reached. To assist in reaching this point the CCP is now be embedded in the UK Certified Cyber Security Consultancy scheme (HMG CESG, 2015; see glossary). This scheme is to encourage properly certified and competency based professionals are employed by companies offering security advice and consultancy though a registered scheme. This is an enabling service to provide that level of professional advice to Boards referred to earlier. In the United States the Global Information Assurance Certification has been in existence since 1999 and received accreditation by the American National Standards Institute in 2007. This certification is course and exam based, unlike the UK competency based scheme.

2.7.2 Understanding the User when Managing Risk

When managing risk, it should be remembered it is not just about the technology and processes included in the complexity of information security are also the human factors (Ashenden and Lawrence, 2013). It is equally important to understand how human behaviour can equally impact security. In the UK, the Centre for Protection of National Infrastructure - CPNI published a set of guidance known as HoMER (HMG CPNI, 2015) which assists in managing what it calls ‘employee risk’ (HMG CPNI, 2012). Inadvertent behaviour would include human frailties such as gullibility of believing someone or something to be genuine but are not through social engineering.

People can be exploited, as described by Mitnick (2002), who identified that as technology to deter attackers improves those same attackers will turn to the staff to exploit their human vulnerabilities through social engineering. A company may deploy excellent defences at their network boundaries only for one of their staff to fall victim to a well-engineered social engineering attach that instead of an e mail containing a virus which would be detected at the company’s outer defence they include a genuine looking link to a website or document that contains malware, often known as a phishing attack (US-CERT 2008, p.4).

Dhillon (1995) proposed the view that within organisations the formal and informal systems are often not appreciated in the analysis and design of information systems. In other words, users often interpret the formal work requirements in a local way and then play out the processes to suit the informal element of their environment. This is a point worth considering that in one part of an organisation a set of behaviours could be interpreted as an adverse incident because it rails against a formal approach to using the system, whereas in another part of the same organisation, where the culture has taken on board the issues of informality in some of the processes and semi formalised these in the design, there is not the same concern resulting in incidents or potential incidents not being reported. .

This localised interpretation is also supported by Lipsky (1980) who uses the term of ‘street level bureaucracy’ to argue that often public sector workers when trying to cope with uncertainty or unusual circumstances not catered for in top level policy create local procedures that in turn become the accepted policy.

An example of human interaction with systems is in the use of passwords, where to protect unauthorised access a system enforces use of complex, difficult to recall passwords, which are frequently changed. This is backed up by a rigorous policy that passwords must not be written down. This was a formal process designed at the beginning. This is probably workable for staff that constantly use the system and are therefore well practiced at inputting the password on a regular basis ensuring they become easier to recall. It may have been that in limited analysis of the system requirements, the needs of frequent users were considered at the expense of those who use a system in an ad hoc fashion.

> “Security culture is the totality of patterns of behaviours in an organisation that contribute to the protection of information of all kinds.” Dhillon (1995, p.90).

In some areas of a business the use of that system is infrequent and therefore the opposite experience regarding the use of passwords is evident. It is then accepted locally that as these are impossible to remember, an informal process of recording and securing them by locking away is considered good practice.

This issue regarding human factors and passwords is also referred to in a study conducted by Brostoff and Sasse (1999) where they found the majority of users could not manage the number of passwords they were allocated. As a result, users would write passwords down or share with others and therefore reduce the effect of the secure control the passwords represent. The example described by Brostoff and Sasse (1999) as a situation that many security professionals would find unacceptable. This human factor and passwords is also referred to by Ashenden and Lawrence (2013) where the rationale for committing a password to memory or writing it down is sometimes down to the importance the user considers that password to have. Just to have a policy to do or not to do something without out an understanding of human factors can lead to predicable human behavioural outcomes.

There is a danger that professionals can be obsessed with risk prevention and not consider human behaviours and their attitude to risk. Wilde (1998) refers to the theory of "risk homeostasis" or, as it is also known as, risk compensation. This was primarily referred to and developed in road safety. Wilde (1998) observes that although the research was conducted mainly in road safety the fact that human behaviour and attitude to risk can be found in other examples such as smoking, even though the health dangers are known or why people live in flood prone areas. The rational being known risk versus benefit or perceived benefit. Wilde asserts that "the mechanisms that are involved in risk homeostasis are probably universal" (Wilde 2008, p.91). Therefore, it is likely these same behaviours and attitudes to risk can be found in people's attitude to information risk.

Wilde (2008) refers to a triggering event in Sweden relating to car driver's attitudes to risk which he states provided clear evidence of risk homeostasis. When Sweden changed from driving on the left to the right-hand side of the road, initially there was a marked reduction in the traffic fatality rate. However, the normal fatality rate returned after a year and a half. At the beginning of the changeover drivers' perceived risk was enhanced and therefore "adjusted their behaviour by choosing more prudent behaviour" (Wilde 2008, p.90). Once drivers and the associated media recognised the roads were not more dangerous, driver's attitudes to risk eased, "consequently, road users opted for less cautious behaviour alternatives and the fatal injury rate rose again." (Wilde 2008, p.90)

Whether there is a major disaster, such as the sinking of Herald of Free Enterprise in 1987, a serious data loss such as experienced by the UK HMRC (2008) or another triggering event, it appears that people's attitude to risk changes and policies and processes are introduced to prevent reoccurrence. However subsequent enquiries into such disasters highlight that the indicators of a trigger event were missed, ignored or not reported properly.

A classic example of not learning from previous, albeit minor, incidents that led to disaster can be found in the enquiry conducted by Lord Justice Sheen (1988) into the sinking of the Herald of Free Enterprise ferry in 1987 with the loss of 188 lives. Prior to the disaster there were numerous minor incidents that were noted by members of the crew but were either not reported or, if they were, the view of management was not to take them seriously or simply dismiss them "…every complaint was an exaggeration". (Sheen: 1987, Para, 19.3) In summary of the cause the whole approach was down to management failure "...the body corporate was affected with the disease of sloppiness" (Sheen: 1987, Para, 14.1)

Toft and Reynolds (1999) in the introduction of their book on 'Learning from disasters a management approach' note that:

> "The underlying philosophy of this book is that socio-technical failures are not the result of divine caprice, nor of a set of random chance events which are not likely to occur, nor simple technical failures. Rather disasters are incidents created by people operating within complex systems. The evidence suggests that where evidence is not learned similar accidents can and do occur." (1999, p.16)

Einarsson and Brynjarsson (2008) in their research of survey findings related to improving human factors, incident and accident reporting and safety management systems in the chemical industry, identified where procedures were put in place they often do not take account of the human factor.

It this lack of a user's knowledge of the reason behind the process they are undertaking can cause decisions made locally to be proved flawed with bad outcomes. Perrow (1984) makes a good point that without a good understanding of a process an operator may be limited in their response to an incident.

> "Computerisation has the effect of limiting the options of the operator, however, and does not encourage broader comprehension of the system – a key requirement for intervening in unexpected interactions." (Perrow, 1984, p.122)

In a survey of Chief Information Security Officers, Ashenden and Sasse (2013) reported that it was suggested in the responses that if staff were aware of the issues surrounding protecting information they would do the right thing when it came to reporting a security incident.

A situation echoed by Perrow (1984) in his analysis of incidents in the nuclear, chemical, aircraft and other types of industries and examines why they occurred, in particular focussing on the relationship between operators and systems. This view that complex systems and lack of relevant practitioner knowledge is also raised by Denyer, Tranfield and van Aken (2012). This situational awareness amongst different workers is also reported by Luokkala and Virrantaus (2014, p.194) where they refer to the fact knowledge is usually process in teams and that "to successfully perform an independent task need to coordinate their actions" and continue "each members actions depend on the other members' actions and communication between the team members". It is this interdependency that can fail and result in serious incidents where team members do not understand how they fit into a process.

Often operators are blamed but upon examination the sheer complexity of the issue and the fact in some industries, e.g. Nuclear power, the knowledge base is relatively new. Instrumentation can indicate one possible cause of a problem but these instruments can be affected by other issues of complexity that can give a reading that should perhaps lead to one course of action but due to other interdependencies this assumption is not always the correct one. In the technology world this contextualisation and situational awareness of what systems are reporting and how an operator is to act is also reported by Pfleeger and Caputo (2012) supporting the view although in a slightly different context to that reported by Perrow (1984). They refer to the problem of a use or analyst failing to "connect the dots" (Pfleeger and Caputo, 2012, p.602). This point is also made by Franke and Brynielsson (2014) who argue "situational awareness cannot be treated in isolation" (2014, p.20). They continue by referring to the;

> "combination of information from different arena's such as a sensor (an intrusion detection device) and what they term as 'an ordinary sensor (a human intelligence report)" (2014, p.20).

2.8 Information Exploitation

The term exploitation is not described in depth as it is purely relating to the use of information which in itself may expose it to risks and therefore incidents surrounding it use may occur and is out of scope of this research**.** Exploitation can mean the integration, management and analysis of data (Blasch, 2013, p.131). The use of the term 'exploitation' is not in the negative context of misuse of data such as that described by Snow and Snow (2007) when referring to the misuse for the purposes of manipulating data to create ‘facts’ out disparate pieces of available information, but in a neutral context of utilising the information.

Once risk assessments and risk management has taken place the information is then used. It is that information exploitation that may then expose it to risk. The use of an asset may result in its exposure to risk which is covered in the risk assessment section. If the risk manifests itself then that is when it is possible an incident is likely to take place.

2.9 Information Security Incidents

An incident could be said to be the manifestation of a risk but what is understood by the term incident in the information security sector is not clearly defined, probably due to the fact there is not yet a nationally or internationally recognised incident classification.

The research highlights the current apparent lack of, or consistency in, any definitions to support the understanding of what an incident is. In the health care sector the incidents referred to relate to adverse patient incidents as opposed to information security incidents. The potential reuse of findings from healthcare research relating to incident reporting could be reused in the information security sector.

A review of information security literature identified research that focussed on managing incidents once they had occurred., Henin, S (2008), Sommer (2012) and Wiik and Gonzalez, (2005) and for example. This research related to responding to technical incidents either, as in Sommer’s (2012) Guide to Forensic Readiness ‘how to forensically handle a security incident’, or Henin’s (2008) white paper that proposes the need to create protocols to share reported incidents of attacks on SCADA (Supervisory Control and Data Acquisition) systems.

There appear to be few sources of information that shed light onto the number of incidents occurring and subsequently to allow analysis and interpretation that would support risk analysis. Unlike other sectors such as health and safety or there is no single source of incident data upon which to base risk analysis on. In the absence of such empirical authoritative publications a number of bodies and companies produce surveys which attempt to fill part of this incident information gap. These include the PWC Information Security Breaches Survey (2012), Ponemon and Symantec cost of data breach 2010 and the Verizon Data Breach Investigation Report (2012). How accurate are the figures in these surveys. In fairness they do not claim to be the definitive source as they are snapshots of responses from a selection of organisations that have returned questionnaires. However, they do point readers where to focus their mitigation efforts. In the Verizon data breach investigation report for 2012 the areas are not specific but generalist. These include generic advice for the smaller organisation (Verizon, 2012, p.4) to implement a firewall and if a third party is managing your subsystems make sure they do this. It does not offer guidance as to how to do this or what the purpose of the advice is. For example, with regards to firewalls they do not refer to the need for a rule-set against which the firewall can accept or deny traffic. Advice to larger organisations is equally high level (Verizon, 2012, p.4) and includes; eliminate unnecessary data and monitor event logs. The report then refers to the appendices at the end for advice on mitigating common threats, note the emphasis is on the threats not necessarily on what has actually manifested itself. The latest Verizon report (2017) has topical advice under the heading "things to consider "at various locations within the report. These tend to be more sector focussed but are still high level.

Critical to managing risk is to understand and have confidence in the level of protection against known vulnerabilities and accurate data relating to the types of adverse security incidents that have occurred and still occurring. A good knowledge of trends and emerging threats is key to this. However, without sufficient trusted data, such decisions can never be truly fully informed.   Before incidents are reported there needs to be active and consistent involvement of the user community, both at the individual user level and the wider organisation level. Ben-Asher and Gonzalez (2015) propose that if the user does not understand the situation surrounding them they may not detect something is wrong. The degree of knowledge, even with analysts task with monitoring events and systems, can impact on the likelihood of an incident being detected (Ben-Asher and Gonzalez, 2015) As will be seen in this literature review there is also a real concern over the ability to identify and classify incidents to provide a true analysis of the number of type of incidents actually occurring.

2.9.1 What is a Security Incident?

Identifying that a security incident has occurred has to happen before it can be reported. It could be argued that not all incidents can be of direct use to an overall Cyber security strategy, but not all attacks are totally technical. Many require elements of social engineering and the targeting of key employees can ensure an easier method of breaching the defences of an IT system. Security incidents involving the loss of an ID or door entry pass, the misplacing of a relevant technical document or inappropriate actions of disgruntled employee, if not reported, can provide the elements of a combination of factors that could lead to a successful cyber security attack.

There is no nationally or internationally recognised incident classification criterion. Even the recognised ISO standard for managing security incidents, BS ISO/IEC 27035 (2011) does not include a definition of an incident. Within the standard it states;

> "Organisations should ensure that information security incidents are documented in a consistent manner, using appropriate standards for incident categorisation and classification, and sharing, so that metrics are created from aggregated data over a period of time. This provides valuable information to aid the strategic decision making process when investing in information security controls." (British Standards Institute 2011, p. 4)

On further examination of this statement phrases such as "'incidents documented in a consistent manner" may be acceptable if only collated and used locally but do not add value when any sharing of incident information is required. Likewise, where the standard continues in the same vein regarding categorisation and classification it really exposes the standard as a unilateral one.

This is not to criticise the current focus of the standard but there needs to be more consistency and common classification if the wish for wider industry sectors and governments to be able to truly understand the information risks they are facing. This "strategic decision making process" referred to in the ISO/IEC 27035 (2011, p4) will remain aspirational until there is some consensus, whether voluntary or regulatory, on incident categorisation and classification.

The lack of common definitions is evidenced through an examination of a number of CERTs (Computer Emergency Response Teams). These CERTS are either run by Governments (e.g. GovCertUK, GovCertNL, US-Cert and CERT Australia) or are collaborative, not for profit organisations (such as AUSCERT and CERTNL). All of these have differing incident classifications and criteria which tend to focus on technical incidents. Whilst it may be relatively easy to generically describe an incident, the real problem appears to be in obtaining a consensus on classification of incident type, without this, analysis is problematic. For example; GovCertUK is the Computer Emergency Response Team (CERT) for the UK Government. The definition they offer of an incident in their Incident Response guidelines (2008) is; "any real or suspected event in relation to the security of data or computer systems". This can be compared with the definition offered by NIST, the US National Institute of Standards and Technology in their Guide for Incident Handling (2012) "An incident is the act of violating an explicit or implied security policy". This in reality links incidents to local policies or definitions. These two national CERTs appear to suggest a different approach to defining an incident. The UK suggests incidents are the product of a data or systems breach and the US that incidents are a breach of policy. The recent issue of BS ISO/IEC 27035-1:2016 gives a high level definition of a security incident as

> "one or multiple related and identified information security events (referring to their definition of an event – occurrence indicating a possible breach of information security or failure of controls) that can harm an organisations assets or compromise its operations."(British Standards Institution, 2016, p.2)

With such apparent differences the ability to compare and contrast incident data will be flawed from the outset. Both definitions are high level and focus on technology incidents. In terms of incident classification, the UK CESG site publishes a categorisation matrix setting out degrees of seriousness of impact and identifies types of incidents as those that are network related and other incidents. It further describes some types of incidents such as targeted attack, website defacement, spam and unauthorised access. The matrix guide states "these categorisations are general". NIST, like CESG, also provide high level definitions for types of incident such as e mail, web, improper usage and attrition. Interestingly it clearly states "these categories are not intended to provide definitive classification for incidents." (2012, p. 11).

In their suggestion that cyber security can also be described in terms used by information Solms and Niekerk (2013) suggest:

> "Cyber security incidents could also be described in terms used to define information security Thus, a cyber-security incident would for example also lead to a breach in the confidentiality, integrity and availability of information" (Solms and Niekerk, 2013, p.99)

However, they do not state what the definition of an information security incident is. Without definitive incident classification, how can these organisations provide true comparisons of incident type and therefore frequency, likelihood and ultimately identify trends. This lack of commonality may also impact on information sharing. Whilst they may be sufficient for individual countries or organisations, and that is debatable, any attempt to extrapolate the data to gain a wider risk picture would be a challenge.

These national organisations are attempting to offer a central facility that should provide an overall picture into the national threat levels, but without clear definitions of what an incident is, or a standardised categorisation of incident type, such threat analysis and assessments can, at best, only be considered generalist.

The International standard ISO 27035 (2011) provides an annex C which suggests example incident classifications and even an example incident report form. The standard recognises the need for standardisation but has no authoritative influence at present. The standard states;

> "These approaches enable personnel and organizations to document information security incidents in a consistent manner, so that the following benefits are achieved:" (British Standards Institute, 2011, Annex C, p.50)

The ISO Standard list of benefits includes the promotion and sharing of information on security incidents, making it easier to automate incident reporting, improving efficiency and effectiveness of incident handling and facilitating collection and analysis of data and finally identifying severity levels and using consistent criteria. What is clearly missing is that element of consistent classification criteria.

As described earlier in this chapter at 2.5.1 the 2013 EU commission Directive on 'measures to ensure a high common level of network and information security across the Union' provides the definition of risk. It also gives its definition of an incident as "any circumstance or event having an actual adverse effect on security" (EU Commission, 2013, p.19). Interestingly their definition of risk is very similar "any circumstance or event that having a potential adverse effect on security" (EU Commission, 2013, p.19). This risk definition, and its closeness in words to the incident definition, does not spell out the hazard element that any information asset faces.

Therefore, for the purposes of this research the author, in the absence of any obviously agreed definitions, proposes the following as a working definition of a security incident to compliment the definition of information risk in section 2.5.1.

> *An information security incident is either, an actual or potential event that has, or is likely to, cause harm to the confidentiality, integrity and/or availability of data, assets, systems or infrastructure whether caused by people, processes or technology.*

This suggested incident definition incorporates near misses and the three key elements of information security as described in the ISO/IEC 27000 (Confidentiality, Integrity and Availability). Additionally, it incorporates the need to reflect a wider aspect than purely technology based incidents i.e. those involving people and processes as well.

Perrow (1984) identified a situation where a good knowledge of a process and also again 'a priori' knowledge can come into play only if the staff involved are closely involved with the process. He cites the example of the Apollo 13 mission and how the issue of a faulty part earlier in the pre-launch testing stage had resulted in a potential hazard. Initially the stance of the space program was based on a greater reliance on instrumentation however; the astronauts have something that instrumentation cannot cover; situational and contextual awareness and intuition. The crew of Apollo 13 felt a jolt which was not detected and therefore when looking for the problem this was in their minds and as a result took the issue more seriously than if it was just left to follow the information provided by instruments alone. Perrow (1984) makes the point the appropriateness of the job can often affect an individual’s ability to identify a problem. By looking out of the craft’s window they could see gas venting, the combination of instrumentation, felt experience and training resulted in;

> “the first thing the crew did, even before discovering the oxygen leak, was to try to close the hatch between the CM [Command Module] and the LM [Lunar Module] They reacted spontaneously, similar to a submarine crew, closing the hatches to limit the amount of flooding.” (NASA, 2009)

The additional information assisted in understanding what had happened. In information security the contextual awareness is similar in that what an alert might be suggesting and having an understanding of the true cause. In complex systems, there are often inter dependencies that are not readily known and often become apparent when things go wrong. It is in these circumstances that operators or managers, due to their specific knowledge and expertise in one part of the overall system, find it difficult to "predict, note, or be able to diagnose the interdependency before the incident escalates to an accident." (Perrow, 1984, p.87)

In the Rail Standards and Safety Board's report 2011 'Independent review of reporting by Network rail and its contractors' it identified a number of RIDDOR (Reporting of Injuries, Diseases and Dangerous Occurrences) and reports were wrongly classified. Many factors were found to account for this including the fact Network rail were using more than one database for recording incidents and the lack of cross checking of the validity of the original incident classification. A problem that exists in a wider context for information security incidents where no common accepted classification exists. This is also apparent in vulnerability classification as reported by Schiffman (2011) and even in naming conventions for computer viruses despite organisations such as CARO (Computer Antivirus Research Organisation) that have tried to introduce one.

There are a number of differing security standards (ISO2700, PCIDSS and others) that arguably are trying to achieve the same result but are often contextual to certain industries as suggested by Browne et al (2011). There appears to be an, as yet, link between governments waking up to the real national security threats posed by cyber-attacks and companies facing increasing regulation and legislation and regulators looking to protect individual's data. There is however some work now taking place to try to improve the situation. There is the challenge of upgrading existing standards such as the ISO27000 series or creating wholly new ones to face the cyber challenge. In 2013 the UK Govt. put out a call for views on cyber security organisational standards (2013) in an attempt to understand what would be the best way forward and the discussion is still ongoing. Some of these same companies being regulated and monitored are also key components of nations' critical national infrastructure. Surely there is a real potential to draw these synergies together. All however still require that basic commodity; management information and metrics to monitor levels of threat, trends, and potential future threats as well as identifying near misses that could provide a rich vein of information to prevent a serious breach. In fact, the identification of incidents and analysing the cause and taking positive action to learn from them and preventing reoccurrence could in turn reduce the number of serious events. Unfortunately for many reasons there seems to be a problem with learning from mistakes.

2.10 Incident Reporting

This section is where the research has identified the greater gaps in knowledge. Although there is research on incidents and events that have an adverse outcome, less is apparent covering why they are not being fully reported. What are the barriers, why is it difficult to report? The research starts from the premise that not all information security incidents are being reported (later tested in the scoping study in chapter 4) and the effect this can have on sharing and the challenges faced by organisations and governments to achieve this. It includes research that covers the increasing policy, regulation and legislation which requires reporting to take place. It also includes identified research into other factors that may affect reporting including; the seniority or grade of staff, the degree of harm caused, informing victims and blame culture.

2.10.1 Security Incidents –Sharing what is Reported, Situational Awareness and the Changing Threats.

The various national administrations aim to be a position to better defend their critical national infrastructures and interests and rely on centralised capabilities to do so. In the United States the White House Executive Order “Improving Critical Infrastructure Cybersecurity” (Feb 2013) highlighted the need for improved cyber security evidenced by the continual intrusions into critical infrastructures. The directive continues by describing a way to achieve this is through a partnership of those responsible for the elements that form the critical infrastructure to “improve cybersecurity information sharing and collaboratively develop and implement risk based standards” (2013, p.1). Initiatives such as in the US of Information Sharing and Analysis Centres (National council of ISACs, 2017; see glossary) which has been in existence since 2003, the UK Information Exchanges (CPNI, 2015; see glossary) and new structures such as the UK Cyber Information Sharing Partnerships (CPNI, 2013; see glossary) are an attempt to widen participation in sharing of threats and associated experience and knowledge. The UK CiSP was launched in 2013 as part of the strategy to tackle the growing concerns of cybercrime. The problems possibly lay in the fact that the fundamentals required to gather a more complete and rounded situational awareness may not have been grasped.

Whilst the top level and high-profile incidents may be shared, the grass roots level of incident data appear not to have been. The challenge is to identify the incidents and even when they are will security professional go on to share with others. As identified by Messenger (2005) in interviews with security professionals on sharing they referred to;

> "various aspects of Knowledge-Based trust, which is about knowing another person well enough to predict their behaviour and is likely to develop over time, through interacting with the person." (2005, p.21)

Sharing relies on the information being available in the first place from individual organisations and the way they structure their security governance can influence sharing internally (Flores, Atonsen and Ekstedt, 2014). If organisations cannot share internally then any external sharing for the common good is a challenge.

The difficulty lies in the fact that, as yet, no one appears to have the full picture. Perry and Moffat (2004) refer to a model named 'CROP' - Common Relevant Operating Picture; a view of the battle space shared by all friendly forces. If the term battle space was replaced by 'cyber' this model may be useful for governments' to consider when forming their cyber defence capabilities and sharing initiatives as a wider view of the threats which in Perry and Moffat's (2004) approach is termed Cooperative Engagement Capability

> "a capability that combines data from all platforms in an operation and allows the combined data to produce a better CROP" Perry and Moffat (2004, p. xxxiii)

Again it is the collation of information to enable informed decisions that is required. This research will suggest there is insufficient commonality in the cyber security world to use a model such as CROP. Without a full contextual understanding of the incidents that affect and organisation or system decision makers in Government or commerce will face the same problems as identified by Perry and Moffat (2004). In their study of the challenges faced by military commanders when command and control is more centralised, and the challenge of varying information sources and the amount of validity in such information they reported:

> "In most cases decision makers must make decisions without full understanding of the values of the critical information elements needed to support the decisions". (Perry and Moffat, 2004, p.xiv)

The increased threat and manifestation of attacks could have a military aspect as well as the accepted criminal activity. The concern over cyber criminals and nation state involvement in cyber incidents has been increasing (MacAskill and Syal, 2017; UK National Crime Agency, 2017) The reference to cyber in UK Government publications does not directly mention cyber warfare. Terms such as Cyber defence and Cyber-attacks, possibly by foreign nation states, are referred to. For example, the threat in the Strategic Defence and Security Review (2010) identified a key risk as that of "Hostile attacks upon UK cyber space by other states and large scale cybercrime" (2010, p.27). In its 2012 UK Cyber Security Strategy it recognised that Cyber was a Tier 1 National Security threat (2011). In the 2015 strategy, the wording has changed referring to;

> "growing numbers of states, with state level resources, are developing advanced capabilities which are potentially deployable in conflicts, including against CNI and government institutions. including against CNI and government institutions."

It continues in support of the link between cyber criminals and states by stating

> "and non-state actors, including terrorists and cyber criminals can use easily available cyber tools and technology for destructive purposes" (2015, p.20).

However, other research does use the term warfare. Cyber warfare has many definitions and a review of definitions was conducted by Robinson, Jones and Janicke (2015, p72 and p.73) who cite a number of them in their paper 'Cyber Warfare: Issues and challenges'. These ranged from Alford (2001) on page 73

> "Any act intended to compel an opponent to fulfil our national will, executed against the software controlling processes within an opponent's system."

This relates to pre-planning a disruption of infrastructure to others where the potential influence of other actors such as criminals could be involved.

Carr (2012) on page 73

"Cyber warfare is the art and science of fighting without fighting; of defeating an opponent without spilling their blood)"

and

Cornish, Livingstone, Clement and York (2012) on page 73 who suggest

"Cyber Warfare can be a conflict between states, but it could also involve non-state actors in various ways…"

The Chatham House Report. 'On Cyber Warfare' (Cornish, Livingstone, Clement and York, 2010) does refer to notable incidents that have occurred such as 'Stuxnet' (Norton.com, 2015) and the cyber-attacks on Estonia in 2007 and Georgia in 2008. Choo (2011, p.724) poses the question "how can we determine whether an attack is criminal or an act of cyber war?" and continues that it may be some governments choose to accept that some criminal led cyber-attacks are allowed if targeted against nations that fit into their own government interests. In effect Choo (2011) is agreeing with the views of Cornish, Livingstone, Clement and York (2010) and Denning (2014) that attribution of the actor can be difficult to determine.

Incidents such as 'Stuxnet' no doubt started in a way that unusual events or behaviours in systems could have been noticed by staff but initially not necessarily reported until the real impacts became evident. Thus, making it difficult for understanding that either a small event was taking place or that many of events were leading to something more significant.

Cornish et al's (2010) paper does not suggest that many incidents lead to such serious events however, the issue of recognising, reporting and collating such events forms part of empirical evidence of the numbers and types of security incidents. There may well have been near misses (or reconnaissance in these more major incidents) that went unreported. Now that the stakes are higher, attention on the identification and reporting of all security incidents, and not just the technical ones, may become more important.

There are potentially greater challenges to sharing and threats from the more tradition owned infrastructures to outsourced ones where the control of security and reporting is changing too. The main change being the gradual but increasing use of cloud computing. Whilst it could be argued such cloud use has been around for some time, the concern being there will be good, secure providers and others that are less secure and it may be the case of 'caveat emptor' when the selection of the service provider is made. Companies that are currently subject to breach notification laws may find an increasing complexity if they outsource more of their data storage to such providers. Research such as that conducted by Robinson et al (2010) in their study of security, privacy and trust in the cloud identified considerable challenges and opportunities in this relatively new service provision which included governance and ownership of risk. More issues may emerge once significant incidents start to manifest themselves and become of media and public interest.

Some researchers have suggested how to fill the information gap where there is a lack of incident data. Bodin, Gordon and Loeb (2008) propose a methodology for measuring risk. Using the term 'PCR - Perceived Composite Risk'. The problem with it is it uses figures which again are not based on empirical evidence. It is perceptive in that respect and Bodin Gordon and Loeb (2008), base their model on using the equivalent to the Annual Loss Expectancy (ALE) measure and they argue that the degree of risk is directly related to the size of any financial impact. The problem with this paper is it provides a mathematical and statistical method to equate potential or perceived loss. It does not state where the source data for such calculations will come from other than using an interpretivist approach.

> "The PCR combines three risk measures through a procedure that determines the decision maker's relative rating of the risk criteria. The weights are decision maker dependent" (2008, p.67).

In other words, potentially using Baskerville's (1991, p.756) 'a priori' approach.

Bodin, Gordon and Loeb's (2008) risk is based on;

> "The expected severe loss focuses on the breaches that would put the survivability of the organisation at risk. In order to calculate the expected severe loss, the decision maker (such as a CISO) first specifies the magnitude of a loss that if it were to occur would threaten the organisations survivability." (Bodin Gordon and Loeb, 2008, p.65).

This places considerable reliance upon a perceived severity of loss. With the current apparent lack of empirical data on such losses this is in fact the equivalent of an impact assessment of what the consequences, for example reputational and financial would be should an incident occur, as opposed to the likelihood of it occurring. Until more visibility of the actual likelihood and impact is mainstream this will always be based on reported high-profile cyber security incidents such as experienced by the UK HMRC in 2008, TK Maxx in 2007, RSA in 2011, SONY in 2014, Talk Talk (2015) and others.

2.10.2 Incident Reporting in Healthcare

This section focusses on literature from the Healthcare sector where it appears more research surrounding incidents has been conducted, albeit where they relate to patients. However, it is suggested the findings may well be relevant to the information security sector.

The Department of Health Report (2000) introduces the notion of two types of incident. Those classed as 'active' failures or unsafe acts which are the result of the behaviour or actions of front line staff and these are considered to be "short-lived and often unpredictable" (2000, p.ix). The other type being 'latent' conditions which can exist and develop over a period of time without coming to particular notice but, when combined with other factors, can result in an incident occurring. This is similar to the 'Swiss Cheese' model as proposed by Reason (1990) where safeguards may be by-passed or fail due to the coming together of a number of factors which, when combined, lead to a break in a safety mechanism. Mahajan (2010) supports this view by giving more detail of these 'active' or 'latent' failures, describing active failures as;

> "omissions, unsafe acts etc. performed by front line staff. Slips (wrong labels, wrong syringe) cognitive failures (memory lapses, ignorance, misreading a situation) or violations (deviations from safe practices, procedures or standards)" (2010, p.71)

Mahajan (2010) then describes latent failures as near misses suggesting these are elements that make up the conditions that eventually lead to an incident occurring. He argues that near misses occur more frequently than the actual incidents that cause harm. Barach and Small (2000, p.760) citing research by March, Sproull and Tamuz (1991), Battles, Kaplan, Van der Schaff and Shea, (1998) and Petersen et al (1998) suggest that near misses can occur between 3 to 300 more times than adverse incidents. There is no benefit in just identifying a problem; the real benefit comes from learning from it. The Department of Health Report (2000) in its assessment of the two types of incident (active and latent) describes two particular types of response to and learning from an incident. These being 'passive' where, although the lessons have been identified, they have not subsequently acted upon and 'active' whereby any lessons learnt become embedded into an organisations processes and culture.

In many disciplines, there have been major incidents and subsequent enquiries. These have included, the Bradford Football Club fire in 1995 (Popplewell, 1985), the sinking of Herald of Free Enterprise 1987 (Sheen, 1988) and the Kings Cross Underground fire 1987 (Fennell, 1988). The subsequent enquiries identified the cause being the culmination of a number of smaller events which, if individually had been reported and tackled, the disaster would never had occurred. Many of these minor incidents, although different in nature, were often not reported for very similar reasons. This situation was reported by Perrow (1984, p.9)

> "Small failures abound in big systems; accidents are not often caused by massive pipe breaks, wings breaking off, or motors running amok. Patient accident reconstruction reveals the banality and triviality behind most catastrophes."

The next major disaster may not be a fire or a shipping disaster but a failure of one or more elements of Critical National Infrastructure facilities resulting in civil unrest and or harm. Will the inevitable subsequent enquiry highlight a lack of incident reporting as a cause? Time will tell.

Having examined relevant research from the information security sector this section reviews current literature that relates to incident reporting, particularly adverse patient incidents, in the healthcare sector. In the health care sector, adverse patient incidents normally result in physical harm as opposed information security incidents that relate to loss of data. There are a number of reports and research papers that focus on the aspect of incident reporting. Whether it be doctors, nurses, physicians or pharmacists tasked with examining samples as part of the analytical care of patients, the findings across the sector appear similar. The Dept. of Health report entitled "A learning Organisation" (2000) was commissioned investigate the issue of 'adverse events' in relation to patients. The primary aim being to learn from past experiences and part of that learning involved the reporting of such events in the first place, potentially minimising the risk of avoidable harm to patients. The report identified that

> "NHS reporting and information systems provide us with a patchy and incomplete picture of the scale and nature of the problem of serious failures in health care". (Great Britain, Dept. of Health 2000, p.vii).

This could easily be read across into the information security incident reporting concerns.

The issue of failing to report incidents is covered in many healthcare research papers including Chiang et al, (2010), Lawton and Parker (2002) and Schectman and Plews-Ogan (2006). Chiang et al (2010) suggest this failure to report is due to unhelpful administrators and other workers, as well as those responsible for the incident, being subjected to challenges over their ability and facing the potential for disciplinary action. Lawton and Parker (2002) focussed on measuring attitudes of medical staff when responding to a number of scenarios. They observed there is evidence that under reporting is a significant problem, particularly for non-confidential reporting systems. With regards to the NHS they suggest;

> "The culture of the medical profession, which discourages reporting, and increasing fears of litigation are therefore likely to constrain the reporting of errors to the NHS" (2002, p.15)

Further research with regards to perceived lack of reporting in healthcare comes from Firth-Cozens (2002) when commenting on the setting up of the National Patient Safety Agency to study errors so that lessons can be learned. Firth-Cozens emphasise "this all depends upon errors being reported, and considerable research shows this is far from the case today". (2002, p.7). An opportunity to test this is provided by Hutchinson et al (2007) through analysis of patterns in the reporting of patient safety incidents from hospitals in England to the National Patient Safety Agency (NPSA). These incidents were collated through the National Reporting and Learning System (NRLS) that was implemented in 2003. This reporting system was one of the recommendations made by the UK Dept. of Health Report;

> "We recommend that a single overall system should be devised for analysing and disseminating lessons from adverse health care events and near misses." (2000, p.83)

During the period of analysis those hospitals that had reported a higher number of incidents also had a lower proportion of incidents in the

> " 'slips, trips and falls' category, suggesting that these hospitals were reporting higher numbers of other types of incident". Hutchinson et al (2007, p.5).

This could indicate that a number of other hospitals who had recorded proportionality higher numbers of 'trips and falls' were not necessarily recording other types of adverse patient incident. One possible theory is that in those hospitals reporting a lower number of trips and falls their patient safety awareness had improved through reporting and learning from these types of incident potentially encouraging further reporting. Hutchinson et al (2007) argue this by stating

> "staff perceptions of the culture of safety and reporting within their hospital influence the actual number of reports being made." (2007, p.8).

One of the benefits of a national system that was reported by Hutchinson (2007) is that reports increase over time and that higher reporting rates can be correlated to a more positive safety culture. This type of central reporting facility at least enables questions to be asked of the data and resultant benefits from that analysis could lead to indications of incident trends. The notion of a national reporting system like the NRLS has its attractions, however Hutchinson et al (2007), whilst recognising there are benefits, also identify drawbacks in such systems. Particularly those associated with their implementation and development.

In a different study on the aspect of adverse patient incident reporting to the National Reporting and Learning System (NRLS) by Olsen et al (2006) they noted that in the first full year of the system being in operation more than 500,000 reports were received, of which, 79% were reported by acute hospital Trusts. Beneath these figures, Olsen et al (2006) discovered that "only 25% of incidents were related to medical care and only about 10–15% came from doctors" (2006. p.43) This indicates support for other research that shown in section 2.10.3 that doctors are less likely to report than nurses. In a separate study of different types of reporting in anaesthesia by departmental, hospital wide and national methods Rooksby, Gerry and Smith (2007) examined examples of different types of incident reports. They all have strengths and weaknesses; local forms were paper based and gave space for free text under heading such as 'what happened' and 'how could this have been prevented'. The downside was there was limited scope for external issues to be flagged. Hospital wide forms were more limited in the ability to write freely and were viewed with suspicion by staff and the local forms were not allowed to be completed further causing difficulties. Nationally the challenge was to get sufficient participation. Their summary described the need for a reporting system that could to tell a story that could be understood at all levels to obtain the best value from the report.

A study by Tighe et al (2006) into adverse patient incident reporting and its effectiveness at one hospital Accident and Emergency department identified a number of issues with the reports. These included not all incidents being reported, lack of consistency in incident classification and excessive use of ‘other ‘as a classification. This points to the concern that when reporting systems are introduced, even the incidents that are reported may not contain the levels of accuracy and consistency in classification to make analysis into themes and trends reflect true reality. All the above research highlights various problems with reporting. Are there any other factors to be considered. The next section examines whether there is any correlation to status, grade or role that may affect the level of reporting.

2.10.3 Is the Level of Reporting Affected by Type and Grade of Staff?

Hutchinson et al (2007) noted that falls tended to be reported in greater numbers by nursing staff. The issue of who reports is found in other research in the health care sector that suggests the apparent existence of a difference in attitudes to reporting between doctors and nurses. As identified by Lawton and Parker (2002)

> “Even when the behaviour concerned reflects the deliberate violation of a clinical protocol; doctors are less likely than nurses or midwives to report colleagues to a superior” (2002, p.17).

The study undertaken by Lawton and Parker (2002) did have some possible flaws, which they accepted, but findings appear to be consistent with that of other research. Hutchinson et al (2007, p.5) identified that, “many incidents still go unreported, with doctors being less likely than nurses to report” from the research undertaken by Kingston, Evans, Smith and Berry (2004). Schectman and Plews-Ogan (2006) found that, upon analysis of the incident reporting system of the University of Virginia VA Hospital in the US, out of 1200 incident reports only 3% were reported by physicians.

It is of interest to note that this figure was obtained by sampling as the hospital system could not differentiate this automatically. This deficiency supports the earlier comments by Hutchinson et al (2007) on concerns regarding implementing and developing such reporting systems. Incident reporting systems have to be designed appropriately to ensure learning is possible. Having identified this low figure from senior staff, Schectman and Plews-Ogan (2006) asked them what would increase reporting. The responses showed the most likely method of increasing reporting would be to allow electronic reporting followed by a group of three elements, clarifying the reporting mechanisms, clarifying what constitutes and incident and to allow anonymous reporting (taken from Schectman and Plews-Ogan, 2006, Table 2 p.340). A difficulty in completion of reports was raised by Kingston Evans, Smith and Berry (2004) in their study of attitudes of doctors and nurses towards incident reporting. The responses to questions asked of the study's focus groups provide a good insight into the doctors versus nurses' propensity to report. From the doctor's perspective, their responses implied that more serious incidents were frequently not reported as incidents but instead referred to as 'known complications' (2004, p.37). This suggests the interpretation from the professional body of doctors is 'adverse patient' incidents are considered as not so much as something that went wrong as a result of their actions, but occurred as a consequence of a patient's condition. Further examples of this came from general discussions with doctors that revealed "a preference for doctors of all seniority to keep adverse events 'in-house." (2004, p.37). In contrast Kingston and Evans (2004) assert that from a nurse's perspective, they were more likely to report incidents citing responses such as; "Our organisation tells us that we need to fill out these forms, therefore we do." (2004, p.37) They continue by suggesting an interesting perspective of the potential or perceived difference in standing between doctor and nurse, where a nurse was more likely to report an incident. "because of their relative powerlessness, it being their only recourse to improve a situation." (Kingston and Evans, 2004, p.37).

In another study, Nguyen, Weinberg and Hillborne (2005) describe the experience of a web based incident reporting system introduced in five University of California medical campuses. Despite a threefold increase of reports after a new electronic system was introduced only 1.7% of safety reports were submitted by physicians. Nguyen Weinberg and Hillborne (2005) suggest there have been numerous calls to tackle apparent reluctance to report through better education and training particularly for the next generation of physicians.

In a paper by Soderberg, Grankvist, Brulin and Wallin (2009) into errors and mistakes that took place in Swedish laboratory testing, the findings are consistent with others. They conducted a survey of 70 primary health care centres and two hospital clinical laboratories studying a specific health area, that of venous blood sampling, and the reporting of adverse incidents relating to the errors in such testing. Soderburg et al (2009) identified that even though errors occurred, 69% staff had never filled out an incident report. They observed this despite it being mandatory to report all incidents that relate to patient safety as required by the National Board of Health and Welfare in Sweden. Many reasons were given by respondents for not reporting including; "lack of time, a complicated reporting procedure, no one else reports incidents and the belief that the reporting of an incident would not make any difference." Soderburg et al (2009, p.733)

In the same area of patient care incident reporting Mahajan (2010) suggests the volume of incident reporting in healthcare is less than it should be and certainly lower that in the aviation industry or other high-risk industries. He argues that the lack of reports prevents learning from the causes of incidents and therefore hinders any future learning in the organisation to ensure that type of event is less likely to occur in the future. He also suggests that blame culture can prevent reporting and that the absence of punitive measures should improve reporting. Throckmorton and Etchegaray (2007) also included other studies based on reporting and the relationship with the organisational culture, whether it is punitive or not. The concept being, in a less punitive organisation the likelihood that reporting would take place increases, as opposed to a punitive organisation that would result in a suppressed number of reports. From the above research, there appears to be several potential factors which can affect reporting.

Does the degree of harm or loss caused because of an incident have any impact on the likelihood it is reported? The next section reviews the literature that provides an insight into this.

2.10.4 Is the Degree of Harm Caused a Factor in Reporting?

A factor that needs to be considered what does the actual or prevention of harm have on the reporting of incidents as opposed to data loss does not necessarily have the same impact on the person or organisation experiencing a data loss. Whilst some research referred to earlier identified a link between grade or seniority and reporting other research focussed on the level of harm and the likelihood to report. Throckmorton and Etchegaray (2007) rather than compare grades of worker and their likelihood focussed on one type - Registered Nurses. They based their findings on a widely-distributed survey that had a relatively low response rate however, the findings are of note. The degree of harm to a patient was graded and the responses recorded against the likelihood to report an incident against the severity of harm caused to the patient. Interestingly Throckmorton and Etchegaray (2007, p.408) reported 55% of respondents would report an incident with no harm having resulted, whereas 94.7% would report where the harm was minimal.

Throckmorton and Etchegaray (2007, p.408) identified the largest response, 99%, would report serious injury and a similar number for death. This indicates that low or no impact adverse incidents do not attract the same high levels of reporting that the more serious incidents enjoy. This appears to slightly contradict research by Kessels-Habraken et al (2010) that where a near miss resulted in no harm to a patient, employees may be more likely to report as they would have less fear of repercussions. The same respondents were then asked; would they share the knowledge of the incident with a colleague? The result for sharing the error where there was no harm was far higher at 67.8% but for the rest of the incidents, where there was a greater degree of harm, the respondents appeared slightly less likely to share the error with a colleague. No reasons for this were given. It could be argued that where an incident is of low severity, the need, or perceived need to report the incident is lower than where there is a greater degree of harm caused. It appears that although the inclination to report increases for a more serious incident the opposite occurs when it comes to sharing knowledge of the error.

Flaaten and Hevroy, (1999) in their study into the relationship between the seriousness of an incident and the subsequent consequence identified that despite the facility for anonymous reporting being in place even low level harm incidents were not always reported to a reasonable level. Schectman and Plews-Ogan (2006) made similar findings in their research linking the degree of harm to reporting. In their survey, many the respondents indicated that where an event was not considered to be serious it need not be reported. In addition, there were some comments that where an individual had made a mistake, and had the error pointed out and corrected for the future, a report would not be required. Hagan (2009) similarly observed a tolerance amongst staff to new recruits and, if they made a mistake that should have been classed as a security incident, rather than reporting it properly they would talk it through with the new employee instead. The danger with this is, firstly no report is made and, secondly any lessons that could be learnt from a training need are not centrally collated. The security manager would not be informed as to what additional input would be required for new recruit training. Part of the solution could be ensuring employees understand the importance of the processes they undertake in their employment and therefore the need to report something when the process is either, not working or an incident within that process occurs.

Many no harm incidents could be arguably thought of as near misses. In other words, if no harm is caused there is not a need to report. However, the opportunity to learn from these is lost. Similar findings regarding the type of severity of incident and the likelihood to report are made by Haines et al (2008) through staff comments derived from a widespread survey of 30 ward staff across seven hospitals in Queensland Australia. They identified there was some degree of influence on increased levels of reporting if it was felt that litigation may follow. Equally staff were less likely to report if the patient was not injured, where the attitude of the staff to reporting was poor or particularly dependant on how busy the staff member was at the time of the fall. In Haines et al (2008) there is also a reference to the problem of incomplete data when shared for wider analysis as there are a;

> “complex hierarchy of determinants that can impact upon the recording of hospital falls on incident reports that exist within the context of a range of environmental/cultural factors that can also impeded incident reporting.”
> Haines et al (2008, p.7)

Again, as in Throckmorton and Etchegaray (2007) , the research by Haines et al (2008) appears to indicate serious incidents are more likely to be reported but not as readily shared where lower harm incidents are concerned Where it is felt only serious incidents are reported other methods could be considered to identify the lower level incident rate. The 'Dept. of Health. An Organisation with a Memory Report' (2000) suggested this very concept of extrapolation in one of its comments where it referred to research into the relationships between volumes of incidents and their seriousness, citing the Heinrich Ratio (1941)

> "As far back as the 1940s, research in industry demonstrated that for each accident causing serious injury, there were a far greater number of accidents which resulted in minor injuries or no injury at all – 'near misses." (2000, p.53)

The report referred to Heinrich's (1941) rationale that for every 1 Major injury there were 29 Minor injuries and 300 No-injury accidents. It should be noted that there are counter views on the Heinrich ratio for example Taxis, Gallivan, Barber and Franklin (2005) argued that from their research into the Heinrich ration they could not find evidence to validate it. In their research, they did identify;

> "there is an urgent need for a common taxonomy in medication error research for defining, classifying, measuring and reporting medication incidents." (2005, p.8)

Arguing more in favour of Heinrich are Jones, Kirchsteiger and Bjerke (1999) who suggest that "that the more near misses (or other deviations) you have the more frequently you will have accidents" (1999, p. 62). Others such as Kessels-Habraken et al (2010) argue near misses occur more frequently than actual incidents; they also raise the concern that without a definition of what a near miss is it is difficult to encourage reporting. Kessels-Habraken (2010, p.1306) research offered the definition of a near miss that differentiates between incidents that did not reach the patient and those that did, but no harm was caused. The point being the absence of true empirical numbers on incidents makes it difficult to judge the efficacy of Heinrich's theory. Even then, with the varying degrees of incident classification discussed earlier in this chapter, this may never be possible.

2.10.5 Does Informing the Patient or Victim Affect Reporting?

It is also important to consider the subject of any adverse incident; the patient themselves. In the information security sector, there are a growing number of legislative and regulatory requirements for breaches to be notified to victims. These requirements also exist in some legislation relating to patient breach notification. In Ontario, Canada there is the Personal Health Information Protection Act (PHIPA) introduced in 2004. The issue here is this legislation mandates the notification to the patient of any personal data loss but does not relate to other types of medical incident or adverse patient incident. Cantor (2002) discusses the notion that patients should be informed of incidents that involve them. After all, they are the victims and could offer valuable learning and knowledge as part of any post incident review. Cantor (2002) refers to opposing research views whether the patient should be informed they have been the 'victim' of an adverse incident. He identified that Witman, Park and Hardin (1996, cited in Cantor, 2002, p.7) in their paper 'How do patients want physicians to handle mistakes?' suggest that patients want to be informed of even minor events. Whereas others Lo B (1995, cited in Cantor, 2002, p.7) argue that patients only need to be informed of an adverse incident where actual harm has been caused to that patient.

If the reporters of incidents, or even those who did not report them, understood the needs and intentions of patients once they were informed, this could affect the inclination to report in the first place. Some medical staff may be less likely to report an adverse incident if they knew the affected patient was to be automatically informed in every case.

Garret and Reeves (2009) in their survey of Australian pharmacists from one area health service investigated interventions made to a patient's treatment or care, where intervention is classed as, "to eliminate or mitigate harm resulting from clinical incidents." (2009, p.99). When asked if they always or almost always reported an intervention; 35% responded yes where an actual incident had occurred as opposed to 19% saying yes where there was a near miss. The survey also identified pharmacists believed 65% of incidents are only reported sometimes, rarely or never, with an even higher score of 81% sometimes, rarely or never for near misses (2009, p.100). Again, the issue of seriousness of incident appears to increase the likelihood of reporting. 81%

of errors would be reported if a patient was transferred to intensive care as a result of an incident.

The numerous studies in different healthcare sectors appear to show a link between the seriousness of an event and the subsequent likelihood of it being reported, resulting in many unreported low harm incidents potentially leading to a more serious incident - the ‘Swiss Cheese’ model again. The resultant factor being by not reporting any opportunity to learn from a near or series of near miss incidents is lost. This is referred to by Lukic, Margaryan and Littlejohn (2010) that incidents tend occur after other, smaller non-reported events, such as near misses. Toft and Reynolds (1999) were not researching health care or information security but how to learn from the causes of disasters. The sad fact is it is often only after a disaster occurs that the subsequent enquiry identifies a number of minor reported or unreported incidents which highlighted the potential for a disaster but were not acted upon.

Peer pressure can be a factor in reporting of near misses. Hagen (2009) identified that attitudes to reporting can relate to the action of others. One of the responses to his survey sums that up in the comment; “why should I report near-miss incidents when nobody else does”. (2009, p.66)

Attempts to improve reporting in the health care sector continue. In 2015 in the UK the Care Quality Commission introduced a new statutory ‘Duty of Candour’ Care quality Commission (2015, p.8; see glossary) as a result on enquiries into events involving patient care at Winterbourne View Hospital, Mid Staffordshire NHS Foundation Trust. The purpose of this new power is “to encourage a culture of openness and to hold providers and directors to account.” (2015, p.4). It sets out specific requirement that health service providers must follow when things go wrong which includes informing the patient.

In summary, it could easily be argued that the research and findings from the healthcare sector point to considerable failings even where there is a requirement to report an adverse event. Whether this is due to peer pressure, the lack of understanding or appreciation of the impact, the consequences of that event or even its potential to cause harm. The main area of concern is that under reporting is adversely affecting the ability to understand the true picture. The initial findings from what research that does exist in the information security sector show potential similarities that indicate such healthcare findings could be of use in the information security area should it wish to learn from them. This leads to the question; what if incident reporting was mandated in legislation as opposed to as currently in many organisations it is a policy or compliance requirement? The next section examines the impact on reporting where the reporting of incidents has been made mandatory through legislation.

2.10.6 Does Policy Affect Reporting?

An investigation to ascertain whether security policy in healthcare had any effect on reporting (Wiant, 2005) identified the lack of research in security incident reporting and was hampered by low response rates. Wiant (2005) concluded that if reporting is included in security policies additional study is required to determine what actions are necessary to.

In the Health and Safety sector it is mandatory to report certain types of incident. However, even despite this mandation there can still be under reporting. The Rail Standards and Safety Board (RSSB) were asked to review the number of RIDDOR (Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995) lost time injuries reported by network rail and its contractors when compared to the number of major injuries being reported. The report 'the Independent Review of RIDDOR Reporting by Network Rail and its contractors (2011)' also refers to Heinrich (1941) as an indicator that not all incidents were being reported when the number of serious incidents were extrapolated using the Heinrich ratio.

It is interesting to note that the report's authors used the Heinrich Pyramid principal which has been used in other official reports such as the Dept. of Health - a Learning Organisation (2000), particularly as other academics (Taxis, Callivan, Barber and Franklin 2005) have questioned Heinrich's model. Whoever is right, it is not so much the accuracy of the ratio that is the point in question, but a reasonable assumption in that if there are serious incidents there should, by rational thought, be a number of less serious ones as well. And this number would be expected to be greater than the number of serious ones.

The RSSB report (2011) identified barriers to reporting and that there was an assumption by senior management that measures put in place to improve safety were the direct cause of lower numbers of incidents being reported. In fact, the review identified other behavioural factors came into play. One of these being the adverse effect of league tables for safety, which encouraged the under reporting by managers to improve the figures.

This adverse effect of incentives is also referred to by Wilde (2008) where he suggests that such incentives can have undesirable effects manifested by under reporting. Wilde (2008) suggests that "the basic strategy of injury prevention should be to reduce the level of risk that people are willing to accept." (2008, p.90) This view could equally apply to information security risk. If within an organisation individuals were encouraged, as part of a culture to accept a lower (or more appropriate) level of risk for the activity they are involved in, this should over time bring the level to an accepted norm. This is opposed to offering incentives as these can have the wrong effect and encourage under reporting. The RSSB (2011) report highlights that when under reporting is tackled and incidents are being reported there is still the issue of incorrect classification. A factor that needs to be taken into account is that Health and Safety has direct relationship to the actual or prevention of harm whereas data loss does not necessarily have the same impact on the person or organisation experiencing a data loss.

Sveen, Sarriegi, Rich and Gonzalez (2007) investigated the correlation between the reporting of high priority and low priority incidents working on an assumption if the focus is made on increasing the reporting of high priority ones and learning from them could have an effect on the low priority incidents that may have developed into high priority ones if not tackled. They also suggest that if the focus was one improving all incidents then those charged with handling the incident could be swamped by the volume of low priority one and not be able to deal with the more serious ones. Working on the assumption that high priority incidents have a potential for greater impact on the organisation by focussing on these types it is argued has the greatest benefit.

Sveen, Sarriegi, Rich and Gonzalez (2007) also considered the incentivising of reporting to improve the flow of reports. Their view was that if such a move to encourage took place the increase in lower level easier to notice and report incidents could have an adverse impact on the resource allocated to investigate incidents. Sveen, Sarriegi, Rich and Gonzalez, (2007) also recognised that the setting of incident reduction incentives can, as described in the RIDDOR (2011) report, have negative implications in that actual incidents that should be reported are not in order to meet reduction targets.

The subject of mandating incident reporting or Breach notification as it is also known has been commented on by Room, S (2009). High-profile losses such as the HMRC disc incident in November 2007 has created what Room (2009, p.285) refers to as a "regulatory bear market". He describes this as where the main regulators, the Information Commissioner and the Financial Services Authority, are very pessimistic about the state of data security within regulated organisations. He poses the question,

> "should data controllers be under a legal obligation to notify security breaches or the loss of data to the authorities or to people affected?" (2009, p.377).

Room (2009) argues that the current cycle of development of security law began in 2003. He states the significance being the introduction of breach notification legislation on California. He feels that arguably this type of legislation has done more than anything else to encourage improvements in data security. Although this view may be correct, even with legislation to ensure incidents are reported there is still the issue of the barriers to report and importantly accurately report, classify, collate and analyse that incident data. If mandation is in place does it bring any benefits.

2.10.7 Mandated Breach Reporting.

What if the reporting of all incidents were to be mandated? There has been research in the area of data breach legislation including Hagen (2009), Cavoukian, (2009), Regan (2009) and Romanosky and Acquisti (2009), Romanski, Acquisti and Sharp (2010) and Romanski, Hoffman and Acquisti (2012).

Romanosky and Acquisti (2009) pose an interesting question;

> "Is the legislature trying to fine tune an optimal balance between the costs and benefits of data privacy and commercial flows of information, or trying to achieve a standard of protection, independently of its economic trade-offs?" (Romanosky and Acquisti, 2009, p.1075).

It appears that an emerging consequence of legislation, originally aimed to provide a mechanism to inform victims that their data may have been compromised, is instead increasingly resulting in opportunities for that victim to take litigation against the company notifying them of that potential compromise, despite some companies offering victims the opportunity to monitor their finances for exploitation of any such breach. Hagen (2009) conducted research into a number of organisations in Sweden following the introduction of a Security Act in 1998 designed to protect information. The observation was that even though the organisations were complying with the same rules there were noticeable differences between organisations in attitudes to security incident reporting. Hagen (2009) identified that even if a report is compiled it may be incorrect or incomplete as there were many options available to report an incident open to staff. Although Hagen (2009) focuses on the relationship between legislation, policy and employee's attitudes and behaviour, the reporting of incidents is touched upon in his paper. He identified that despite legislation mandating the reporting of incidents, it was an employee's attitude and understanding of the need to report, rather than legislation that determined whether incidents are reported.

2.10.8 Does Breach Notification Bring Benefits?

Schneier (2008) proposes that mandated breach notification is a good thing for three reasons. Firstly, it is good practice to inform someone they are or are potentially a victim and may have their data exploited to their financial disadvantage. Secondly, the notifications may produce statistics for research purposes and thirdly the fact that companies suffer adverse publicity as a result of a breach may force them to spend more on security to prevent breaches in the first place. He also suggests, as a consequence, companies may therefore be less likely to store as much customer data.

This may be starting to occur but are the priorities balanced correctly? In the Ernst and Young survey on cloud computing (2011) they identified that data leakage and data loss protection technologies were rated second to business continuity plans (BCP) by companies who responded to the survey. 36% of respondents stated BCP would attract the most funding against 13% for data loss protection. It may appear the value of the data for the company could be perceived to be more important than the actual data subjects after all without the data, the company cannot function and may go out of business.

Research by Lukic, Margaryan and Littlejohn (2010) suggests that how an organisation learns from incidents, in this case health and safety incidents, depends on that organisations attitude and approach to safety. The objective is not just to share information and knowledge about an incident but to "aim for a safety culture where learning is a process of continuous knowledge flow." (2010, p.429). They suggest that knowledge and information that is gleaned from one incident may be particularly relevant to other incidents that initially do not appear to be of a similar nature. Lukic, Margaryan and Littlejohn (2010) refer to single and double loop learning in relation to incidents as do Voss and Wagner (2010). The term 'double loop learning' originates from Argyris (1997, p.116) who reports on the challenges and lost opportunities of learning from staff when things are not working as they should. He suggests this stems from "The inability to uncover errors and other unpleasant truths arises from faulty organizational learning" (Argyris, 1977, p.115) Managers when receiving reports do not always act upon them or filter the 'bad' news slowly. Argyris continues regarding the challenges for employees to report by saying they are in a 'double bind' which is;

> "when employees adhere to a norm that says hide errors they know they are violating another norm that says reveal errors. Whichever norm they choose, they risk getting into trouble" (Argyris, 1997, p.116)

The single loop learning is in effect a sticking plaster approach or knee jerk reaction compared to double loop learning where a root cause analysis of the event would take place. Lukic, Margaryan and Littlejohn (2010) refer to double loop learning as important due to its ability to "surface latent and systemic causes that might be contributing to incidents at a later stage" (2010, p.431). Voss and Wagner (2010) when referring to learning from small disasters suggest understanding the true impact of such incidents by proposing two measurements. One being scale. "How severe is the destruction and distress?" The other being scope "How widespread is the disruption within the community?" (2010, p.658) This approach could be considered when assessing the impact of any incident or breach that a company has experienced when assessing the real impact on its customer base.

Mandating that breaches are reported will not necessarily improve any learning from that incident. The culture of an organisation can often determine how, and indeed, whether an incident is addressed. Other research namely by CIPPIC (Canadian Internet Policy and Public Interest Clinic) 2007 and Romanosky, Telang and Acquisti (2008) focus on data breach notification. CIPPIC argue for data breach notification to be introduced nationally and concentrate on the effect of security breaches on victims, suggesting there is no incentive for organisations to report incidents and breaches unless forced to do so by legislation. In particular, by reporting a security incident, companies would have to identify their security failures which could have an adverse impact on their reputation. CIPPIC (2007) identify differing standards and interpretation of the various breach notification laws within in the United States; where there are differences between States in the reporting criteria. For example, in some States there are exemptions for the requirement to report if the lost data was encrypted or redacted. Interestingly there is often no clarification on the degree or standards of encryption required to meet this exemption. The degree of this mitigation varies from State to State. The commonly known 'triggering event' for notification also varies as do the definitions of breach and harm. There is also an argument that even with definitions there will be local interpretations of them (Kessel-Habraken, 2010; Tamuz, Thomas, 2006).

If the thresholds for reporting, or indeed being exempt from reporting are not standardised, any attempt to understand a country wide picture is limited at best. The reason for mandating is primarily to protect an individual from being a victim of fraud or ID theft. There does not appear to be an intention to understand the true cause of the incident or apply any consistent standards. Therefore, any opportunity to learn from the incidents may be lost. In fact, CIPPIC (2007) suggest that although breach notification can provide organisations with an incentive to improve security, if the sanctions are not of a sufficient nature such mandation can have the converse effect by providing some organisations with the potential to hide breaches.

Conversely, Romanosky Telang and Acquisti (2008) suggest that breach legislation could offer incentives for companies to report incidents based on the consequences of not reporting. Romansky, Telang and Acquisti (2008) also raise concerns regarding standardisation of classification of 'trigger events'. They do focus on the potential for such legislation to influence behaviours, in particular the customer making a demand on their service provider to provide for more security of their information. This has the potential to make security a customer driven benefit that companies would consider offering. There is also the risk that by continually informing victims they have been subject to a breach may result in the phenomenon known as ‘notification fatigue’, Cavoukian (2009). The next section looks more closely at the impact of breach notification on the victims and offenders particularly relating to the resultant litigation that may follow.

2.10.9 The Compensation Culture and Breach Notification

Victims of data breaches appear to be increasingly seeking compensation often in the US through class action (Kim, 2016), which can focus companies’ attention on the wider cost implications of any breach. A study by Romanosky, Hoffman and Acquisti (2012) identified that the “odds of a firm being sued in a US Federal Court are 3.5 times greater when individuals suffer financial harm.” (2012, p.1) Where the company that was responsible for a breach provided free credit monitoring after the breach had occurred, it was identified that such companies were six times less likely to be sued. It appears that by putting in place mitigation after an event can in fact reduce the financial impact of any litigation made against the company involved and potentially reduce, or at least identify, any attempt by criminals to exploit the victim’s data. Regan (2009) and Cavoukian (2009) both refer to the situation that although an organisation may have to report a loss or compromise of a customer’s data as a breach, in reality this data is invariably not lost in the true sense. That data is still available to the organisation on their systems for them to carry on their business. The impact of that breach is arguably felt more on the customer who may have had to cancel credit cards, check credit references and other counter fraud activity. Harm has been caused to the customer, not the data owner. The only harm that could be inflicted upon the organisation is through any fine, regulatory notice or through reputational damage.

Romanosky and Acquisti (2009) researched the issue of breach notification further in their paper examining consumer data protection laws in the US and their impact and the cost implications for organisations. This is in response to the inevitable growth in the costs of compensation or regulatory fines being imposed on organisations that suffer a data breach, particularly where there is a requirement to notify the victim. Romanosky and Acquisti (2009) propose that some standards such as PCIDSS (Payment Card Industry Data Security Standards) are becoming the de-facto legal compliance standard for organisations that process consumer credit cards. The issue here being not so much the common good for protecting critical infrastructures, such as finance, but ensuring the victim of a breach receives some form of compensation. This element is outside of the scope of this research but certainly is of note regarding the consequences of organisations not having in place robust and efficient incident reporting systems and processes. The reference to standards such as PCIDSS and the different interpretation of breach notification exemptions highlights the problem that there may be too many standards.

The question is what affect will this have on encouraging greater reporting of incidents in the first place. Whether such legislation reduces instances of identity theft or not is hard to distinguish. Romansky and Acquisti (2009) summarise by recognising there is limited empirical evidence on the effect of data protection legislation mandating incident reporting; a common theme in the literature reviewed. There does appear to be an effect on organisation and consumer practices in response to such legislation, however this appears only to have a minor effect on identity theft due to a breach.

2.10.10 Does a Blame Culture Affect Reporting?

Hood’s (2002) blame avoidance theory describes the extent to which organisations are willing or prepared to share are directly related to managers or key professionals fears in relation to being blamed for any failures that may occur because of sharing and collaboration or where there is a loss of direct organisational control of that data. In other words, once it is shared it is no longer controlled. The consequences being they will either share, or not share, based on whether they feel the risks of personal criticism of their decision to be grater or less. It could be argued that to some extent this is risk management but not so much in a controlled manner more as Hood (2002) suggests that the result of a serious high-profile incident can lead to ‘defensive risk management’. This can result in individuals and organisations trying to avoid blame and shifting it elsewhere. Hood (2002) may offer an explanation to the knee jerk reaction referred to earlier where he suggests “protocolizing behaviour for due-diligence defences may produce ill-considered and inflexible responses to complex problems.” (2002, p.65). This is linked to the earlier views of Hurtzburg (2007). As argued by Perrow (1984) risks will always exist but not to know the true cause can be as damaging as the original incident itself.

> "Risk will never be eliminated from high-risk systems….at the very least, however we might stop blaming the wrong people and the wrong factors and stop trying to fix the systems in ways that only make them riskier." (Perrow, 1984, p.4)

A study by Shekelle (2002) suggests the reason physicians do not fully support any improvement initiatives is partly due to their view that such programs provide the vehicle to apportion blame for anything that might or might not happen to a patient in their care. Shekelle, (2002, p.6) refers to the historical position as the physician being seen as the 'captain of the ship' as does Cantor (2002). This captain analogy and the issue of autonomy and feeling of responsibility are also discussed by Perrow (1984) when studying incidents in the maritime sector. This analogy probably relates to the authority and autonomy a captain enjoys. The crew may not like some of the decisions but will not challenge the captain's authority. Shekelle (2002) also raises the issue of litigation as being of concern to physicians through malpractice. The main challenge being trying to change a culture from one of blame, to that of learning from mistakes. Shekelle (2002) proposes this will be difficult and Tondel, Line and Jaatun (2014) reported that system administrators were often not sure if they should report an incident as by doing so could result in 'worst case consequences' (2014, p.48) particularly as they were responsible for the system and therefore could be responsible for the incident itself. Waring (2005) suggests that there are 'significant barriers' to the successful implementation of incident reporting systems referring to the "fear of blame" or "culture of blame" that inhibits participation in reporting (Waring 2005, p.1928). If reporting is to be improved, then the concerns that individuals have about apportioning of blame need to be tackled. In Waring's (2005) study the notion that the inevitability that an error will occur and that this is accepted within the medial culture is something that is a main factor in the regarding attitudes to reporting. As errors or incidents are inevitable they somehow become accepted as such and subject to 'normalisation' and routine. As a result doctors may therefore see reporting as a management exercise rather than a method to which service could be improved. (Waring 2005, p.1932)

2.10.11 Incident Reporting in the Aviation Sector where Harm is a Known Factor

The aviation sector has a number of approaches to the reporting of incidents and near misses. The main aspect of aviation that possibly differs from security incidents and possibly even health care is there is an obvious and clear assimilation of harm. If a plane has a problem or there is pilot error serious incidents involving mass casualties can occur. It is possible that due to the potential scale of the losses and the fact that reporting is more likely to occur. Often headline grabbing and so the expectation to report from the travelling public is likely to be greater than for individual incidents of harm to patients or financial harm caused by an intrusion incident that compromises financial or personal data. Aviation incidents and near miss reports are reported through confidential reporting systems such as the US Aviation Safety Action Program (ASAP) and NASA's Aviation Safety Reporting system (ASRS) which provide limited immunity from prosecution (Beaubien and Baker (2002, p.3). In the UK there is the Confidential Human Factors Incident Reporting Programme (CHIRP). In themselves these reporting systems are different and suffer from clarity on taxonomies to which Beaubien and Baker (2002) research looks to address. In a similar way that this research has identified the lack of a common definitions in terms such as a security incident and the classifications of types of incidents.

The key issue and possible difference from other incident reporting challenges is that the aviation sector's reporting relate to threats to safety which is understood and recognised by the general public and, when things go wrong, are reported widely in the media.

2.11 Lessons Learnt from Other Industries

One of the main issues identified is that incident reporting is not as good as it should be across all sectors perhaps except for the Aviation industry. Even where they have been significant research in the healthcare sector there are still issues with under reporting despite recommendations that are intended to improve the situation. There does appear to be a relationship between the degree of harm and likelihood to report as well as differences in grade or stature (doctor versus nurse). Where there have been disasters these were often caused by a series of smaller events not being reported or acted upon until too late.

If anything, this makes improving security incident reporting a challenge as despite lessons from other industries the improvement is perhaps not as good as it might be. The difference in this research is by using the findings and turning them into the critical success factors that could improve reporting, thereby focussing on less buy more important elements of the lessons learnt and developing them into terminology more readily accepted by information security professional as well as looking at the potential for the deployments of such CSFs through an Incident Reporting Maturity Model may have a better chance of success.

2.12 Research Gap and Sumary

It is apparent that the amount of research into the reporting of security incidents is limited. Critical to managing risk is to understand and have confidence in the level of protection against known vulnerabilities and accurate data relating to the types of adverse security incidents that have occurred and are still occurring. Knowledge of trends and emerging threats is key to this. However, without sufficient trusted data, such decisions can never be truly fully informed. There is also a real concern over the ability to identify and classify incidents to provide a true analysis of the number of type of incidents occurring.

Examination of the literature relevant to incident reporting so far has identified there is research into sharing of incidents but are gaps in research in the area of security incident reporting. The particular gap being why are security incidents not being reported. This creates a concern that what is being shared is not the full picture. The research has also identified a lack of standard taxonomies for security incidents and information security risk which could result in what is shared is not truly comparable.

Whereas in the healthcare sector this has been examined and key factors identified such as the relationship between harm and reporting and to an extent the level of seniority in the staff involved and their likelihood to report. These factors will require further research to identify if they are also evident in the information security sector. Supporting elements of these apparent factors to reporting will be incorporated in the understanding of the Critical Success Factors that could improve information security incident reporting which are reported in more detail in Chapter 5.

This research appears to identify that there is potential relevance in studies relating to reporting of incidents conducted in healthcare and elsewhere that could be carried across into information security. Whether it be a general propensity in all sectors to refrain from reporting, the difference in reporting according to rank or job designation and also the severity of the incident. By identifying the potential to utilise research conducted elsewhere can make up for the specific immaturity of the information security sectors depth of research into this area. This reuse may assist in future modelling of ways to improve the situation and to assess the impact on current risk assessment and analysis methods. If the relevance of the healthcare research is supported in the information security sector then the findings of this literature review have identified there is the potential to re-use the research conducted in other sectors and apply to information security incident reporting. Although the sector subject is different incident reporting, other than those incidents identified by electronic logging and detection systems, is still in the hands of staff and individuals. The human factors that affect the likelihood to report identified in this review are likely to be similar.

Chapter 3 Research Methodology

3.1 Introduction

The literature review in the previous chapter highlighted the differing levels of research conducted on incident reporting. It suggests that far more research on incidents has been conducted in other sectors, such as healthcare and transportation, than had occurred with respect to information security incidents. The identified research that was conducted into information security appeared to be more focussed on outcomes such as risk analysis, incident management and information sharing as opposed identifying reasons why there is an apparent lack of security incident reporting.

Although the healthcare research focussed on patients, and the harm caused by adverse patient incidents, there does appear to be the potential for the research conducted into that incident reporting to be applied to information security incident reporting.

This chapter sets out the philosophies considered, the approach, methodology and methods to achieve the research goals set out below.

> (1) To test whether the assumption that not all information security incidents are being reported is correct.
>
> (2) To examine whether research on incident reporting conducted in other sectors, such as healthcare, can be applied to the information security sector.
>
> (3) To identify the Critical Success Factors that may be applicable to information security incident reporting.
>
> (4) To propose an information security Incident Reporting Maturity Model that could be applied by organisations and may improve the flow of incidents that are reported.

It also provides further information on the types of methods used to gather information, such as the scoping study described in chapter 4, the Delphi study described in Chapter 5 and the Incident Reporting Maturity Model validation study described in chapter 6. Though full discussions of those individual methods are described in other specific chapters

3.2 Research Philosophy - Natural Science or Social Science

Approaches to research continue to cause arguments between theorists as to which is the right approach. In the past it was the natural sciences that took prominence, particularly relating to quantitative research, where the emphasis was on describing events as opposed to understanding why things occur (Easterby-Smith et al, 2003) but times have changed leading to the opposite research paradigm to natural science, that of social sciences. The social sciences lean more towards how individuals respond, not just to the situation being researched, but also to the researcher (Bryson, 2011).

Onwuegbuzie (2003) observes that over the last century a rigorous debate has continued in the United States over the quantitative and interpretative research paradigms. In his view this has led to a divide between opposing camps of researchers, resulting to some extent a division of opinion and the competitiveness between the two groups as to who is right or wrong. There are researchers who effectively nail their paradigm position to the mast and refuse to move. Onwuegbuzie (2003) believes this is a real threat to improvement or advancement of research methods and, all the time this mono research theory divide continues, suggests;

> "as long as we remain polarized in research how can we expect stakeholders who rely on their research findings to take their work seriously." Onwuegbuzie's (2003, p.2)

His paper emphasises the need for researchers to appreciate and utilise both quantitative and interpretative research methods as equally valid. As a result Onwuegbuzie uses the term 'pragmatic researchers' (2003, p.3). This notion is supported by Robson (2011, p.18) who suggest a sort of "détente" has developed and that these paradigms are not exclusively separate and that many researchers combine both styles. Indeed the scoping survey, Delphi study and validation survey in this research incorporated both quantitative and qualitative methods. A brief comparison of the two types is shown in Table 3-1.

Quantitative	Qualitative
The emphasis of **Quantitative** research is on collecting and analysing numerical data; it concentrates on measuring the scale, range, frequency etc. of phenomena.	**Qualitative** research is more subjective in nature that Quantitative research and involves examining and reflecting on the less tangible aspects of a research subject, e.g. values, attitudes, perceptions.
This type of research, although harder to design initially, is usually highly detailed and structured and results can be easily collated and presented statistically.	Although this type of research can be easier to start, it can be often difficult to interpret and present the findings; the findings can also be challenged more easily.

Table 3-1 Quantitative v Qualitative Research Methods. Extract from University of Bradford (2005, p.3)

Collis and Hussey (2009, p. 66) assert that "most students find their paradigm falls broadly between one of the two main paradigms" Onwuegbuzie (2003) continues in his view that pragmatic use of either side of the research paradigm in his references to Sieber (1973) who argues both research methods have advantages and disadvantages and that researchers should "utilize the strengths of both techniques in order to understand better social phenomena." (2003, p.8) Indeed, he continues by referencing (Miles & Huberman, 1984, p. 21) that staying pure to one or the other "epistemological purity doesn't get research done." Durkheim (1982) suggests that when trying to explain phenomena there is a need to understand the cause as well as the function it fulfils. This has also been referred to as 'phenomenology' (Bryman, 2004, p.13) who describes this view being attributed to Alfred Schultz (1899-1959) whose works were not well known until later translated in the 1960's. Buckingham and Saunders (2004, p.19) use the description by Kolakowski (1972) of the term phenomenalism as

> "the insistence that scientific knowledge has to be grounded in sensory experience of phenomena, or things. If we cannot see, tough, smell, taste or hear something, either directly or indirectly, then we cannot study it scientifically."

Additionally Buckingham and Saunders (2004) in relation to survey methods, propose the phenomenalist approach is that

> "Facts exist prior to, and independently of, research, and can be discovered by asking questions and recording answers systematically." (2004, p.20),

Where does this research sit on the research continuum from positivism to interpretivism? Due to the apparent lack of identified research this thesis has to look to interpretative methods and utilise qualitative data. However, that has not prevented the acquisition of quantitative data as a result of the studies undertaken. On a continuum scale this research philosophy could be argued as being pragmatic and located to the right of centre of that paradigm. Therefore this research philosopher sits in that 'pragmatic researcher' position. This is due to that apparent lack of empirical evidence and research in the information security sector to understand why the true number and types of incidents is not known and the reasons that prevent reporting. Research identified elsewhere, healthcare for example, may have the potential to be reused, even though it may not have even been used fully within the sector that conducted the research in the first place.

3.2.1 A Perceived Lack of Empirical Data – what Approach to Adopt?

Positivistic approaches are founded on a belief that the study of human behaviour should be conducted in the same way as studies conducted in the natural sciences (Collis and Hussey 2003, p.52). Bryman (2004) explains that positivism is the application of methods of the natural sciences to the study of social reality and beyond. Knowledge to test theories is derived from fact or science. Stahl (2005, p.4) describes positivism as "subscribing to empiricist epistemology" whereby "true statements about reality can be deduced from impartial observation and experience." The research subject by its very nature is lacking in empirical information. Had the reporting of information security incidents been recorded with reasonable diligence over a period of time the research would have been more based on a positivist method. In the same way that in the early days of the insurance industry loss or claim information was not collated and widely available. Any initial research there would have been based on theory as opposed to observation and interpretation of fact, interviews and opinions as opposed to formal study. A positivistic approach will often seek to research a problem or subject and describe a rational reason for it. This would normally be achieved through proving a link between a theory and the variable in the subject being researched. This is the natural science approach with a belief people respond to stimulus, or forces, as opposed to the relatively new social science interpretation of human behaviours in that they do not necessarily follow a natural order. The study of human motivation and behaviours can be shaped by elements that are not always easy to observe. External or internal cultural or peer pressure issues can often fashion behaviour. The phenomenological style particularly attempts to interpret the behaviours of research subjects from their own perspective. In the absence of empirical information on security incidents that would allow for a positivist approach to any research an interpretivistic approach was selected.

With a positivist research approach there is an independence where the researcher and the subject are different entities and their "interaction needs to be strictly controlled in order to avoid contamination or bias." Jacobson, Gewurtz and Haydon (2007, p.2) suggest in an interpretive approach to the research there is social imagination whereby the researcher will be "drawing on their own life experiences to describe and theorise their subjects of interest." Jacobson, Gewurtz and Haydon (2007, p.3). This can lead to a risk of bias being introduced and, having recognised this, the researcher must try to avoid introducing bias into their interpretation of their observations. The notion of researcher bias is covered is section 3.7.

As there is an apparent lack of data to base the research in a positivist style the alternative interpretivist style was adopted. An interpretative approach in information risk is not a bad thing and is considered healthy when putting the information into the context of its use and the organisation using it. Baskerville (1991), when referring to the making of risk assessments in information security, suggests it would take some considerable time to have complete confidence that all incidents are reported and, more importantly, properly categorised to allow sufficient reliance upon their accuracy. Irrespective of the amount of empirical evidence on incidents being available Baskerville (1991) asserts his view that a generalist or novice will not possess the 'a priori' professional knowledge and experience which is necessary to correctly interpret the complexity and context of specific organisational settings (1991, p.758). This view clearly indicates that Baskerville does not feel security risk assessments can be completely conducted in a positivist scientific manner. He maintains that even if all incidents are reported, there is still a requirement for experience, knowledge and understanding to interpret the findings of any statistical positivist output. In other words; despite there being a large amount of trusted empirical data there is always a place for interpretivism of that data, particularly in the context of the environment to which it applies. This contextual impact will differ from organisation, sector or location.

3.3 Research Approach

3.3.1 Deductive, Inductive or Abductive Research

The three stages of abductive, deductive and inductive were identified by Charles Pierce (1839-1914). The three stages are described by Ho (1994, p.1) as;

> "at the stage of abduction, the goal is to explore the data, find out a pattern, and suggest a plausible hypothesis; deduction is to refine the hypothesis based upon other plausible premises; and induction is the empirical substantiation"

This approach can lead to more than one cycle of the above as, once a particular set of data has been analysed and researched, it is then possible to go back to the original hypothesis and refine it to start the abductive, deductive and inductive approach again. Staat (1993, p.227) describes this reuse as;

> "the testing of the consequences so that new or more precise hypothesis can be suggested – obviously resulting in another three phase enquiry."

Ho (1997, p.16) describes the notion that not all possibilities can be tested and therefore

> "we abduct only what is more plausible".

This research approach starts from an assumption that information security incidents are not being reported in sufficient numbers to reflect the real position. This then leads to an approach to test the hypothesis to understand if it is in fact true by the use of the surveys described in chapters 4, 5 and 6. It could be interpreted that, as there are few security incidents being reported therefore it follows there are only a few incidents occurring. This deductive approach could be accepted if there were accurate empirical evidence to back up the statement and that it was the view of those in a position to state the accuracy of incident reporting metrics. It is in fact that apparent lack of any real information that makes the deduction, although on the face of it accurate, subject to scrutiny. It is this logically correct but not necessarily true position that Williams and May (2000) refer to in their deductive statement that “all pigs can fly, Porky is a pig and so, Porky can fly” (1996, p.25)

This research then takes an inductive approach that asks through research what is the reason why there are few security incidents. It may be that is because few incidents actually occur or few are reported, but in reality more may be happening. That would be in its simplistic form. The example given by Williams and May (2000) where they propose that a deductive statement is where the conclusion follows the premise. This theory is based not on empirical data but the lack of it. The deduction to some extent being the lack of information supports the reason for the assumption in the first place.

Deductive approaches can be very linear as (Bryman, 2004, p 9) outlines below sequence;

1. “Theory
2. Hypothesis
3. Data collection
4. Findings
5. Hypothesis confirmed or rejected
6. Revision of theory”

Whereas, with an inductive approach, the theory is often the result or outcome of the research. An inductive approach draws conclusions from research findings and observations (Collis and Hussey, 2009). A different approach could be made thereby making this research deductive. There are few incidents because few incidents are reported. Either could be argued but each in reality requires further investigation. However, as the research develops the use of studies in the form of questionnaires, the Delphi study and validation study the research gradually becomes more inductive. The assertion that the number of incidents being reported is below the actual level is based on assumption and lack of empirical evidence to test the theory. Therefore, at the first stages of this research the methodology could be argued as being deductive. The theory being a lack of reported incidents due to a number of as yet un-evidenced barriers, but this deductive approach can change once the research provides more information and the resultant thesis will identify or infer broader general ideas or theories, an Abductive approach.

Bryman proposed a simple model to demonstrate the inductive, deductive approach. (2004, p.10)

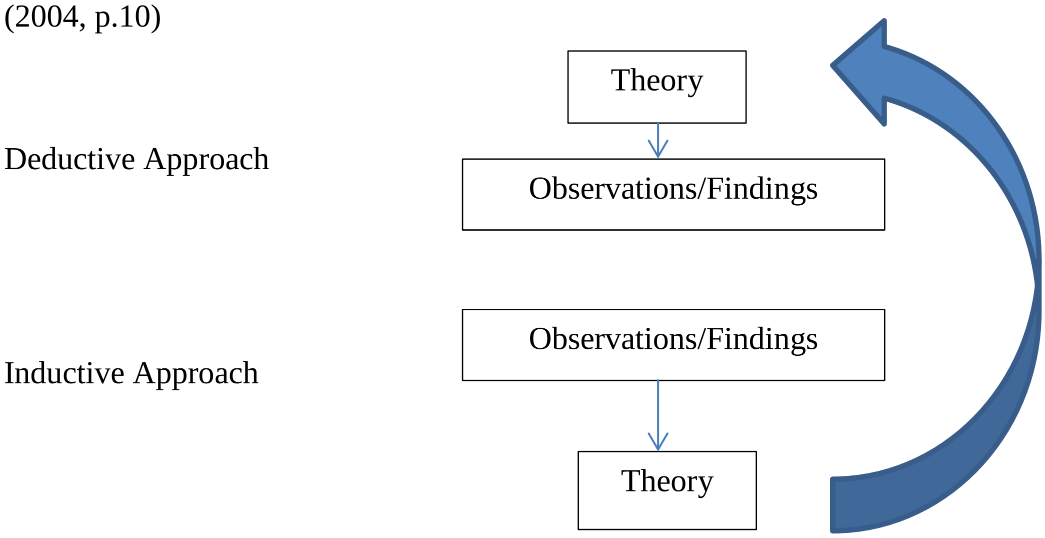


Figure 3-1 Deductive v Inductive Approach Bryman (2004, p.10)

To further identify where this research sits it sets out to test the theory that not all incidents are reported evidence is collated through a survey which contained both qualitative and quantitive questions. The results confirm the theory that incidents are not reported but does not identify the reason(s) why, as there are no empirical data sets to work from. Therefore the natural science approach cannot support the research. Social science in the form of opinions and views of those who work in the field have to be sought. Once sufficient information is received, although there is still a lack of empirical data, there is sufficient to firm up the initial theory but with more evidence through opinion as to why this should be. It could be argued this is an inductive approach that leads to a deductive one. This notion of both types being applicable is reported by Perry (1998, p.788) and that a researcher would find it unlikely to separate the two. This can continue until sufficient information is available to achieve a consensus of opinion on methods to tackle the problem that, if successful, could result in sufficient empirical data to be used in a more positivistic manner.

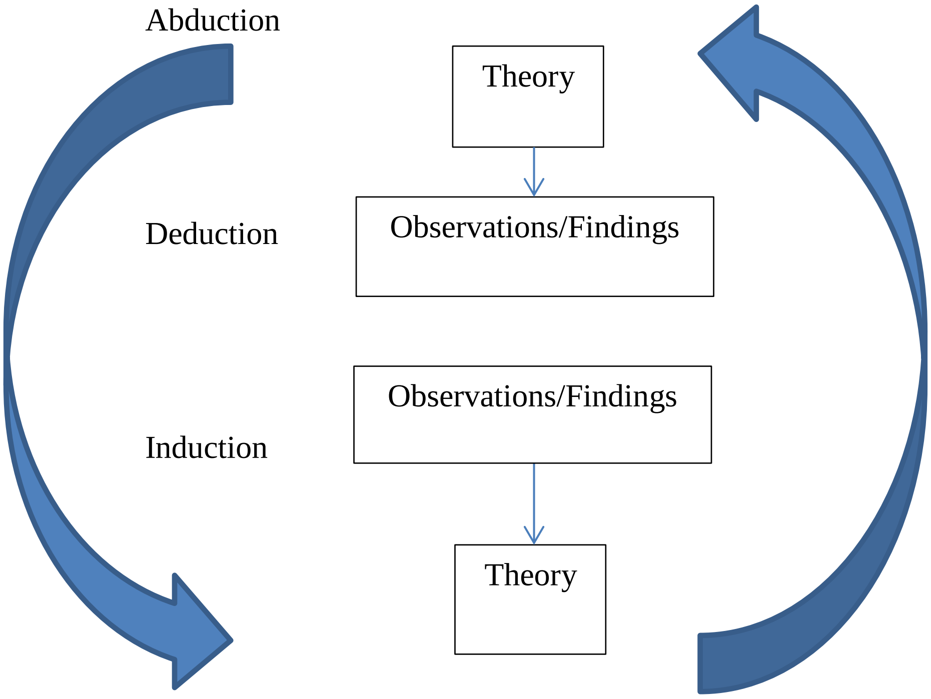


Figure 3-2 Deductive, Inductive, Abductive Circular Approach. Authors Adaptation of Bryman (2004, p.9)

This leads to the notion that the approach was actually following an abductive then deductive followed by inductive approach which can be repeated.

3.4 Research Methodology

To support the research goals there needed to be an appropriate methodology that could understand the view of the world of the studied group (information security professionals) in relation to information security incident reporting. The research is based on a pragmatic researcher approach which uses an interpretivistic philosophy. The most appropriate methodologies to obtain the data and opinions of security professionals were the use of surveys. This took the shape of a linear mixed methods approach where, using questionnaires, each type of survey was different according to the specific research aim. All made use of the collection of mixture of qualitative and quantitative data from the studies group. By taking the Onwuegbuzie (2003) "pragmatic researcher" approach this methodology of a mixture of types of data from the positivism and interpretative paradigms can give cause to concern that, as Robson (2011) describes being seen as a "pretty minimal theoretical underpinning to multi-strategy research verging on an 'anything goes' philosophy."(Robson, 2011, p.171). This could lead to the research being criticised as lacking in "dubious rationale and validity". However by having a clear conceptual structure – the conceptual framework outlined in Chapters one and two – these concerns can be allayed and particularly by having a "feasible research question as well as other aspects of the design" (Robson, 2011, p.171). This design framework is set out as;

> "Purpose(s)
> Conceptual framework
> Research questions
> Methods
> Sampling procedures"
> (Robson, 2011, p.168)

It is strongly believed that the logic and design of this research meets those design framework elements to enable the pragmatic researcher approach to be considered valid for this research question. As Bryman (2004, p.463) reflects that "a multi strategy approach is becoming far more common". He agrees with Robson (2011) that such research must be "competently designed and conducted" (Bryman, 2004, p.464)

By taking the framework set out by Robson (2011) this research does have

i) Clear purpose – the four goals

ii) A conceptual framework

iii) A Research question that is based on the goals

iv) Methods to support this in the three studies

v) Sampling methods by ensuring the participants are representative of the wider group being studies and were eligible for the particular research subject.

The research methodology selected was considered the most appropriate to support the research goals outlined in the introduction. Goals 1 and 2 were tested through the scoping study; goal 2 was also examined as part of the Delphi study as was goal 3. The Validation study incorporated some aspects of goal 3 but focussed mainly on goal 4. All three surveys would obtain the research material through data gathering. "You cannot be analytical without data" Davenport, Harris and Morison (2010, p.23). In the absence of research in this area the ability to test some of the assumptions regarding incident reporting was required. Asking standard questions of a group and then analysing the various responses, in particular noting any if there are any differences from industry sectors, would provide a good source of data. It would also serve the purpose of defining the problem space.

The general view is that other research methods such as questionnaires or interviews should be considered by those undertaking research against the practicalities, logistics and the research questions themselves. "Attention must be given to other data collection methods," (Hasson, Keeney and McKenna, 2000, p.1009).

One approach that could be considered is that of a case study. A case study is a methodology that is used to "explore a single phenomenon (the Case) in a natural setting" (Collis and Hussey, 2009, p.82). Bryman (2004) refers to case studies normally being associated with a location, such as a community or organisation and continues that often case studies are associated with qualitative research but often utilise both quantitative and qualitative research. This stance is supported by Yin (1981, p.58) who continues that their supportive evidence can take many forms "fieldwork, archival records, verbal reports observations or any combination of these". There are risks that a case study can presume that a finding in one community can be replicated in another.

The disadvantage of a case study is that if based on one community, although having some validity, it may not be considered as truly representative of a wider group. In particular one of the sectors may be subject to specific regulatory controls or community security policies relating to incident reporting. This could result in any extrapolation of the findings from such singular groups not necessarily reflecting the true situation of the wider security community

A scoping study was considered that would be used to ask the opinions of security professionals what their experience of and confidence in the levels of incident reporting. At the same time testing a possible re use of research from other sectors that may assist in increasing reporting, if there was indeed a problem. The challenge was to find an appropriate audience to test these assumptions.

The first methodological approach was to undertake a scoping study used a mix of interpretative and some qualitative analysis of the scoping questionnaire text responses. Its main aims were to gain an understanding of a number of information security professionals as to their perception and experience of incident reporting. The opportunity was also taken to test whether initial findings from research in the healthcare sector could be considered as valid, and re-used by those professionals and the sector as a whole. The scoping study is discussed in Chapter 4.

Subsequent to the analysis of the scoping study results were provided in a series of presentations to information security seminars and conferences. The purpose was to examine the responses of information security professionals in both the public and private sector to identify if any adverse reaction or comment to those results was made. It would also identify the level of support for the research, and provide an indication as to whether the findings were truly reflective of the reporting of security incidents in that sector.

A number of potential research methods to obtain consensus were considered. These were; case studies, focus groups, interviews and questionnaires and the Delphi study. This section outlines why a Delphi study, was eventually selected.

It is often the case that when a report publishes its findings, whether it is the result of a disaster or significant event or one commissioned to resolve a problem, the valuable content is not always taken up in practice as organisational cultures are resistant to change (Perrow, 2007). The elements identified in the literature review that could influence and potentially improve incident reporting may be able to form the basis of a series of Critical Success Factors (CSF's) required to improve security incident reporting. These CSF's could be considered to be a vehicle to identify what was essential for an organisation to focus on should it wish to improve the reporting of incidents.

To gain consensus from a wide community of information security professionals a Delphi study was considered an appropriate method. The Delphi method originated from research conducted by the RAND group in the 1950's to identify the impact of technology on warfare. Rand (2017). A Delphi is a method of “eliciting and refining group judgements” (Dalkey, 1969, p.v) who continues by describing the method as having three features; “Anonymous response, obtained by a formal questionnaire; iteration and controlled feedback and statistical group response” i.e. the consensus.

This research used a group of expert opinions to obtain consensus through an iterative process (Erffmeyer, Erffmeyer and Lane, 1986). The study would set out the potential CSF’s identified from healthcare and other research and, using a Likert scale, the iterative Delphi process would gain consensus to what elements were considered as critical to improving incident reporting. A wide range of information security professionals were invited to participate ranging from those belonging to the information security professional body, the Institute of Information Security Professionals – the IISP, Information Asset Owner’s in UK government, members of CiSP and other recognised communities of interest.

Respondents were given the opportunity to add other factors they felt warranted inclusion and consideration by the wider Delphi group. Consideration as to which study methods would be the most suitable to achieve a valid and unbiased outcome, predominantly through maintaining confidentiality in any responses, was given and of course the university’s ethical committee approval was sought.

A validation study was considered to identify what, if any, of the CSF’s identified through this research and the Delphi study had the potential to impact on the improvement in reporting. Particularly whether any alignment can be made with the proposed incident reporting Maturity Model identified as a possible vehicle for organisations to judge their level of maturity against those CSF’s. The validation study involved a control group who had not previously been involved in any of the Delphi study process but would have met the eligibility criteria to participate in the Delphi if they were available at the time. This control group was used to identify if there were any opposing views relating to the identified CSF’s.

3.5 Research Methods

There are a number of potential methods available for the gathering of research. These are outlined in this section.

3.5.1 Scoping Study

The scoping study was designed using a questionnaire to test the assumption that the true level of incidents is not known due to a number of issues surrounding the reporting of them. It also aimed to study whether research into incident reporting undertaken in other disciplines is relevant and has the potential to be reused to good effect in the information security sector. To achieve this a representative group needed to be identified and, as some of the questions required responses that could identify failings in their organisations incident reporting processes, the participants would need assurance that their responses were kept strictly confidential.

In the field of information security there is a common understanding of the need for trust. When asking for sensitive details of a company's ability to report incidents and the fact they may be subject to regulatory controls and the answers will cause embarrassment or worse still censure from a regulator if disclosed. The subject needs to be assured of the researcher's intentions, professionalism and ability to maintain the confidentiality assurances made at the outset. As the author is part of the subject group as an information security professional, and therefore aware of this situation, the need to assure information obtained from any questionnaires was done so in a confidential manner. It was also important to ensure there was no potential to influence the outcome of any contributions and reduce the challenge of bias.

3.5.2 Delphi Study

The technique known as a Delphi originated from research conducted by the RAND group in the 1950's to identify the impact of technology on warfare (Rand, 2017). The research used a group of expert opinions to obtain consensus through an iterative process (Erffmeyer, Erffmeyer and Lane, 1986). Since then the method has become popular as a research method. It is described by the originator of the Delphi, Norman Dalkey, as "a rapid and relatively efficient way to 'cream the top of the heads' of a group of knowledgeable people" (Dalkey 1969, p.16). A Delphi Study was chosen as the most appropriate method of obtaining consensus on what were the Critical Success Factors to improve security incident reporting.

The use of a distributed questionnaire was considered which could alleviate the discussed concerns. To identify an agreed set of CSF's a degree of validated consensus would be required. As the CSF's had not yet been identified the limits to case studies, focus groups and interviews in this research would be time consuming and labour intensive, particularly if a wide group of security professionals needs to be involved to achieve a more relevant and acceptable consensus. The scope of the subject is narrow and will rely upon participants with subject matter expertise. The use of a Delphi in this research to assist in identifying CSF's that ultimately led to a Maturity Model drew on the research from De Bruin, Freeze, Kulkani and Rosemann (2005) who used the Delphi to identify Maturity Models and suggest the Delphi could be used as a two-stage approach. In this case, it may be used in the first stage to achieve consensus on the CSF's required and, then be used to validate a subsequent Information Security Incident Reporting Maturity Model. Becker, Knackstedt and Poppelbub (2009) suggest the use of literature analysis to identify the assessment criteria required to formulate material for Maturity Models based on the identified success factors. They continue by suggesting the use of explorative research methods citing Delphi methods as suitable to achieve this aim. Therefore the Delphi was considered as the most appropriate method for this research. Chapter 5 sets out the Delphi study and how it was used to identify the Critical Success Factors required to improve security incident reporting.

3.5.3 Validation Study

The purpose of the Validation study was to give the Delphi participants the outcome on the consensus achieved regarding the identification of and final wording of the four CSF's. In addition it was asking whether, having come to that consensus and identified the CSF's could the results of their contribution be placed in an Incident Reporting Maturity Model that could be used as a method of improving the reporting of security incidents. This method was intended to add confidence that "the data collected reflects reality and is a true picture of what is being studied". (McNeill, 1992, p.15)

There is an accepted risk of misinterpretation by the researcher of a response to a question. The fact that a Delphi was used, which returns the findings to respondents for reconsideration to obtain consensus, adds to the validity of the process as any unusual interpretation may be further challenged by respondents. However, as described earlier there was not sufficient text to apply coding to conduct a true content analysis. The iterative rounds of the Delphi would to some extent enable participants to question the researcher's analysis of comments. Although they would not have had access to the full set of responses, they were still able to comment on the interpretation of the overall wording changes and results by challenging or suggesting amendments as part of the iterative Delphi process.

To add another element of validity a control group would be identified. This control group had not previously been involved in the Delphi study. They did meet the eligibility criteria of those in the Delphi study and by involving such a group would also provide a level of assurance as to the identified CSF's as they would also have an opportunity to comment on the wording and usefulness of the CSF's within a Maturity Model.

The Validation study would also incorporate a method that could be used by organisations to make practical use of the identified CSF's. An Incident Reporting Maturity Model would be developed that incorporated the identified CSF's and place them into a Maturity Model to test the potential to judge an organisations level of maturity in relation to each of the identified CSF's. The original Delphi participants, together with the control group, not previously involved in the research but who met the eligibility criteria, would also be used to test the IRMM as a potential method of adopting the CSF's as opposed to just publishing a list of them.

3.5.4 Data Collection

Having decided to take an interpretivist approach then the data required a method of collection. The Scoping, Delphi and Validation stages would all make use of questionnaires. In particular the Delphi approach uses questionnaires as part of the process to "minimise the biasing effects of dominant individuals, irrelevant communications and of group pressure towards conformity," Dalkey, 1969, p.v)

Semi structured and unstructured interviews, although challenging, are appropriate in some circumstances (Collis and Hussey, 2009). For example, where the interviewer wishes to understand the respondent's world or where the interviewee is uncomfortable about answering specific questions. The issue that will arise with any form of interviewing is the process of interpretation (Buckingham and Saunders, 2004), as the real challenge is to ensure the planning of the interviews recognises that the interpretation of a question by an interviewee can be different to the understanding of the response by the interviewer.

The general view is that other research methods such as questionnaires or interviews should be considered by those undertaking research against the practicalities, logistics and the research questions themselves. "Attention must be given to other data collection methods," (Hasson, Keeney and McKenna, 2000, p.1009). The use of structured questions using a mixture of questions to provide quantitive and qualitative responses was selected as the most appropriate method.

3.5.5 Data Analysis

As all three studies had the facility for free text comments an analysis of these needed to be undertaken. A recognised approach being content analysis. Content analysis is where qualitative data is converted into numerical data (Collis and Hussey, 2009). This type of analysis is firmly embedded where objective and systematic analysis is required. Content analysis is often thought of in terms of conceptual analysis. (Colorado University Guide, 2013, p.2). Although a questionnaire, if properly and strictly managed, can be considered unbiased. Any subsequent analysis of free text, unstructured additional comments should be conducted in such a way that a different researcher following the same process should come up with the same or very similar findings. To some extent a controlled laboratory experiment not in the positivist discipline but that of the interpretivist. As commented by Bryman (2004) it has to be recognised that although the initial rules and style of questions may be that of the researcher and contain an element of bias. However, it is the methodological and systematic approach to the interpretation of any research material emanating from those questions that should be replicable.

By using a scoping study, Delphi study and subsequently a validation study allows for the resultant qualitative responses to be subject of content analysis. In the scoping study although there were a number of set questions with a selection of response criteria against a Likert scale. This scale was originally developed by Rensis Likert in 1932, (Robson, 2011, p.303). There was also the provision of additional comments and observation which a number of respondents took advantage of. It is these additional free text comments that provide additional information, value and the opportunity for further analysis.

A key issue in numerical coding of content or words is regarding is whether to code for the existence of a term or its frequency. In the limited scoping study the amount of additional comment could yield some interesting insights into the respondent's additional views on a particular subject. The volume of responses was not an issue as the total number of respondents was 38 but even here the time and resource to apply this method can be considerable. Consistency is also vital. The term' lack of' for example may have the same meaning as 'there are no' it is the subsequent words that accompany these short descriptive phrases that may need examination to be really sure the two phrases are used in the same context. The decision on what to code or count "are bound to be affected by the nature of the research questions under consideration" (Bryman. 2004, p.187)

Disadvantages of content analysis will always be the element of bias whether intentional or not, as they rely on the interpretation of the researcher. Bryman (2004) there is also the potential for the analysis to be considered atheoretical where consideration is given more to "what is measured as opposed to what is theoretically significant or important" (2004, p197)

To some extent the content of the questionnaire in the scoping study could be considered as secondary analysis where the findings of other research, in this case the where some of the findings in the Department of Health report (2000), notably the list of potential barriers to reporting and learning, were re used to ascertain if similarities of identified barriers in the healthcare sector were relevant in the information security sector. It is the subsequent free text comments made to these barriers and other questions that is the subject of the content analysis.

The intention being to identify any points or relevant comments that could be incorporated in the main face to face interviews that take place or in the case of the scoping study the planned subsequent Delphi study. Partly the idea of a scoping questionnaire is to test the design flow and efficacy of the original concept albeit there was considered thought and pre-launch testing of the scoping questionnaire. The fact that the respondents came from a wide range of companies and countries may have a cultural impact on some of the responses that also needs to be considered in any analysis. The potential benefit of the approach of using content analysis was twofold.

Firstly, to identify additional research material that came as a result of the responses the second as a method of further improving, focussing and fine tuning the face to face stage of the research. As suggested by Bryman (2004) there is always a risk that such an approach could be considered as atheoretical. However if the method and process are sufficiently grounded in logic and accountability then this concern should be alleviated.

As many of the comments from all the questionnaires contained a mix of suggested re-wording, support for the research, general observations on the problem of reporting or additional sub sections of a potential CSF the approach of coding was not considered appropriate. Instead where there appeared to be some consensus or argued need for an amendment this was made. This amendment was of course then visible to participants either as part of round 2 of the Delphi or the validation survey. The researcher's interpretation of such comments can always have the potential to lead to bias which is covered in more detail in section 3.7. To illustrate the types of comments Appendix 9 shows the suggested additional CSF's; Appendix 10 shows participants comments from round one and round two of the Delphi. and Appendix 16 shows the comments and observations from participants of the Validation study.

3.6 Ethics

Bryman (2000, p.509) referring to ethical principles describes the approach by Diener and Crandall (1978) who have broken the components of ethics into four main areas.

> "Whether there is;
>
> harm to participants
> lack of informed consent
> an invasion of privacy
> deception involved"

Harm can mean many things but in general can include physical harm, participant's development, loss of self-esteem and the inducement to perform certain unacceptable acts. (Bryman, 2004). In the case of this research the potential harm could be to a participant's self-esteem through a reputational risk should any information provided by a respondent to a survey being attributed to them that may have repercussion either professionally or relating to their employment. This element is covered within the various survey designs. This is illustrated by McNeill (1990) in relation to anonymity and confidentiality. Although he is referring to the question of asking people what criminal offences they have committed, his observations are still valid in this area of research. He asserts that to achieve truthful answers there needs to be a guarantee to those providing them that their responses would be confidential. He continues this includes answers given by a particular individual are not identifiable (McNeill, 1990, p.41). In addition there was only one person conducting the analysis of the responses so no secondary analysis of questionnaire took place. Potential participants need to be given as much information as possible regarding the survey in order that an informed decision on whether or not to participate can take place (Bryman, 2004). The three surveys included the right to withdraw at any point. The privacy aspect has been covered under the confidentiality and anonymity assurances and the aspect of informed consent is catered for the instructions included as part of each survey.

For the research studies in Chapter 4, 5 and 6 the intention was to achieve as honest and open response as possible from the selected community invited to take part in the Delphi. Buckingham and Saunders (2004) consider that anonymity and confidentiality are crucial and, as discussed earlier, that despite complete anonymity within a Delphi being harder to achieve, it is still highly important to assure participants their responses are kept secure and not shared. In particular by not linking an individual's identity with any findings. As the invite to participate was sent to several communities of interest it is likely that some would know who else is participating. The critical element is to ensure any responses are kept confidential.

In the Delphi there were no questions that were of a sensitive personal nature. McNeill (1990) asserted that to achieve truthful answers there needs to be a guarantee to those providing them that their responses would be confidential, emphasising that any responses given by an individual are not to be identifiable (McNeill, 1990, p.41). This is equally important for the Delphi as it was to the scoping study. Although the responses to this Delphi were more related to views rather than individual personal and confidential issues, the respondents, by the very nature of the fact they work in information security and the in-built need to be circumspect in relation to their employer's information, McNeill's approach remains valid. Collis and Hussey (2009) advocate that when setting out a questionnaire it should include a reference to the confidentiality of information provided. To ensure the research was ethically sound, the proposed methods, controls for anonymity and confidentiality together with the questionnaire and supporting documents was submitted to the university's ethical committee and approval granted. (Reference number CURES/662/2015)

Other benefits of a Delphi study are that it offers considerable anonymity between respondents though an iterative process, whilst allowing a form of conferring but without the social pressures to conform to the views as expressed by others (Skulmosky, Hartman and Krahn, 2007, p.2). The advantage of using a Delphi questionnaire is that (Goodman, 1987, cited in Hasson, Keeney and McKenna, 2000, p. 1012) the true ethical anonymity is easier to evidence. Although in a Delphi the participants can present and react to ideas unbiased by the identities and pressures of others they do not see their individual responses only the outcomes of the consensus forming. This has been referred to as "quazi-anonymity" (McKenna, 2004. Cited in Hasson, Keeney and McKenna, 2000, p. 2012). Having identified potential Communities of Interest that represent a range of information security professionals, approval of those responsible for such groups was sought and obtained as part of the ethical approach. This was achieved by contacting the relevant governing bodies of those groups and seeking formal approval to use their members, having outlined the research subject. It was also important to recognise that as the recipients were security professionals they are likely to be suspicious of unsolicited requests for information regarding the security of their organisation.

This potential reticence can also be countered where the researcher can demonstrate empathy with the participants through recognised professional involvement, skills and experience in information/cyber security. This enabled the gaining of acceptance of peers that there was knowledge of and a genuine intent to allay those potential concerns. To explore the opinions of security professionals on how much credibility they put upon the reporting figures within their own organisation it was imperative to instil a high degree of confidence in the anonymity of any response. By demonstrating an understanding of the potential reluctance to give honest answers on organisational weaknesses and failings in the reporting of incidents enabled honesty of the responses as many reported low confidence in the reporting of incidents and associated reporting systems.

3.7 Researcher Bias

Where an interpretive approach is undertaken due to the relationship between the observed and the observer there is always a risk that the observer can introduce bias into their interpretation of the element studied. Whilst there is recognition that ethics is a central aspect of such research Stahl (2005) believes it is of such importance that it should not be left to individuals or institutional ethic committees alone. Ethical considerations should be considered a “necessary consequence of the choice of certain research approaches.” (Stahl, 2005. p.1). Bryman (2004, p.134) refers to research by Sudman and Bradburn (1982) who suggest that “postal questionnaires work better than personal interviews when there is a possibility of bias contained within a question”. Where Bryman (2004) refers to postal questionnaires in the case of this research where they were handed out at the scoping study stage and then later emailed as attachments during the Delphi and Validation questionnaire stages this would equally apply.

There were two elements of potential bias to be considered. Firstly; during the scoping study where the author was trying to encourage the conference attendees to complete the scoping study questionnaires. To avoid this the approach was to use the conference chairman to introduce the research in a formal way and request participation as it as seen of benefit to the security community rather than face to face requests through the author. There was an opportunity to engage with the audience at the invitation of the conference chairman to provide brief reasons for the research, giving assurances by referring to the sections in the survey describing the process to maintain confidentiality and anonymity. The author was careful to ensure this engagement did not create any bias for its completion including intonation or emphasis in voice or tone. It was judged the attendees would feel sufficiently interested in the subject to want to participate. Secondly; the presence of the author at the scoping study and the involvement of the author through communities of interest at the Delphi and Validation stages may have caused some influence or bias. As best as possible, by keeping to best academic practice in design and keeping one to one engagement to an absolute minimum, the distance between author and participant was maintained. The exception to this was where it was necessary to clarify an unclear answer and the fact they were know n to some of the audience. The researcher, by being part of the community, may be more likely to be accepted and trusted. It was believed this would result in obtaining information in a subject area that, to individuals and organisations, is sensitive and where other researchers would have experienced difficulty in eliciting the same level of detail and data. This issue of keeping responses confidential or anonymous is supported by Dalkey (1969) in his description of the three features of a Delphi;

> "i, Anonymous response – where a questionnaire is used to obtain a groups opinion.
>
> ii, Iteration and controlled feedback - is the examination of those responses with carefully controlled feedback to enable further iterations from the group.
>
> iii, Statistical group response - where the opinions of every member of the group are defined as an aggregate of those responses, following the final round of iterations." Dalkey (1969, p.v)

The main aims of these three elements are to minimise any bias from dominant participants, irrelevant communication and group or peer pressure.

Consideration as to which study methods would be the most suitable to achieve a valid and unbiased outcome, predominantly through maintaining confidentiality in any responses, will be given and of course the university's ethical committee approval will be sought. As commented by Bryman (2004) it has to be recognised that although the initial rules and style of questions may be that of the researcher and contain an element of bias. However, it is the methodological and systematic approach to the interpretation of any research material emanating from those questions that should be replicable.

3.8 Summary

The intention of this chapter was to identify the philosophical and methodology approach to the proposed research question in Chapter one. It identifies that the methods to identify the reasons for an apparent lack of incident being reported were abductive using an interpretivist approach supported by series questionnaires each with a different emphasis on the research with the aim of identification of the CSF's. The aim was to test the potential to re-use research from another discipline relating to difficulties in reporting adverse patient incidents in health care and using the in the information security sector. The re-use of previous research to provide the catalyst for further research provided a sound position on which to base the questionnaires, the

Delphi and Case Study. This use of methods to elicit views and opinions from information security professionals ensure the research approaches to support and interpretivist methodology were maintained.

The stages to support the methodology are

Stage 1. To understand if the perceived problem of a lack of reporting of information security incidents is supported and whether research on incident reporting from other sectors has the potential to be re-used.

The literature reviewed already provided evidence that it was of concern to a number of authors and researchers studying information security, but no specific research on why could be identified. The nearest that could be considered came from the healthcare sector where considerably more research into the concerns surrounding the reporting of adverse patient incidents had been conducted.

Stage 2. Identify the appropriate research methodology.

This included consideration of the use of qualitative and quantitative research through the use of questionnaires, a Delphi study and a validation study to identify the opinions of information security professionals.

Stage 3. A scoping study of a number of information security professionals was undertaken to test the initial assumption that there was indeed a problem with security incident reporting.

The scoping study used a mix of interpretative and some qualitative analysis of the scoping questionnaire text responses. Its main aims were to identify the understanding of a number of information security professionals their perception and experience of incident reporting. The opportunity was also taken to test whether initial findings from research in the healthcare sector could be considered as valid to be used by those professionals and the sector as a whole. The scoping study is discussed in Chapter 4

Stage 4. Subsequent to the analysis of the scoping study results were provided in a series of presentations to information security seminars and conferences.

The purpose was to examine the responses of information security professionals in both the public and private sector to identify if any adverse reaction or comment to those results was made. It would also identify the level of support for the research, and provide an indication as to whether the findings were truly reflective of the reporting of security incidents in that sector.

Stage 5. Conduct a Delphi study to test the potential for consensus using the information gleaned from the identified research and the scoping study.

It is often the case that when a report publishes its findings, whether it is the result of a disaster or significant event or one commissioned to resolve a problem, the valuable content is not always taken up in practice as organisational cultures are resistant to change (Perrow, 2007). The elements identified in the literature review that could influence and potentially improve incident reporting may be able to form the basis of a series of Critical Success Factors (CSF’s) required to improve security incident reporting. These Critical Success Factors could be considered to be a vehicle to identify what was essential for an organisation to focus on should it wish to improve the reporting of incidents.

To gain consensus from a wide community of information security professionals a Delphi study was considered an appropriate method. The study would set out the potential CSF’s identified from healthcare and other research and, using a Likert scale, the iterative Delphi process would gain consensus to what elements were considered as critical to improving incident reporting. A wide range of information security professionals will be invited to participate ranging from those belonging to the main professional body, the Institute of Information Security Professionals – the IISP, Information Asset Owner’s in government, members of CiSP and other recognised communities of interest.

Respondents will be given the opportunity to add other factors they felt warranted inclusion and consideration by the wider Delphi group. Consideration as to which study methods would be the most suitable to achieve a valid and unbiased outcome, predominantly through maintaining confidentiality in any responses, will be given and of course the university’s ethical committee approval will be sought.

Stage 6. Conduct a validation study using the Delphi findings to be incorporated within an Incident Reporting Maturity Model

The validation study will be in a form of a survey that tests the potential use of an Incident Reporting Maturity Model which uses the CSF’s identified in stage 5. This stage will also involve a control group who have not previously been involved in any of the study processes but do meet the eligibility criteria. This will enable any challenges to the identified CSF's and the notion of an IRMM as a possible delivery vehicle for those CSF's to be adopted within organisations

Stage 7. Review the outcome of Critical Success Factors and proposed Incident Reporting Maturity Model.

The intention is to analyse the findings of the Validation survey to identify whether the IRMM could be applied by organisations to improve their information security incident reporting. It is intended that the IRMM could be offered as a potential tool to assist in improving incident volume reporting using a non-proscriptive, iterative, contextual approach.

The next chapter sets out the scoping study referred to in stage 1 that was intended to test the assumption that information security incidents were under reported and that research from other sectors had the potential for re use by the information security sector.

Chapter 4 Scoping Study Information Security Incidents. Seeking the Views of Information Security Professionals

4.1 Introduction and Background

Chapter 4 describes the scoping study that was designed to test the assumption that the true level of incidents is not known due to a number of issues surrounding the reporting of them. It also aimed to study whether research into incident reporting undertaken in other disciplines is relevant and has the potential to be reused to good effect in the information security sector. It sets out the method of design and distribution of the series of questions and the subsequent analysis of the results. The survey was constructed to gather both qualitative and quantitative data.

It contains the views and opinions from a small group of information security professionals who attended recognised information security conferences in June 2011. It examines their experience of the reporting of security incidents and the level of confidence they had in the actual number reported. Included in the scoping study were a number of identified barriers to learning and, potentially therefore, reporting incidents from research in the Healthcare sector. It starts by outlining why a survey and what were the aims then describes the survey design process through which the data was collected and analysed to understand whether it is feasible that some of the identified reporting barriers and methods to improve reporting could be imported into the Information Security arena.

The issue of incident classification is also a consideration, and this was included in the scoping study. Even where incidents are reported there appears not to be a commonly accepted or agreed classification. This in itself can lead to problems when comparing incidents from either the same or different sectors; in particular this has the potential to lead to the false or misleading interpretation of trends. Where reporting is mandated, there is the risk that if the incident is not identified, or the reporting of it and learning from it is suppressed through one of the many identified barriers, then the requirement to report cannot take place. The consequences being that any statistics produced are likely to be inaccurate. There are a number of papers and studies on the efforts to share incident information between groups and sectors or on risk methods that comment on the lack of accurate data of reported incidents but none tackle the reason why (Baskerville, 1991; Baker, Rees and Tippett, 2007).

The literature review in chapter 2 identified that little research in the reporting of information security incidents had taken place. In contrast, in the HealthCare sector, there are numerous published papers and reports on ‘adverse patient incidents’ (Hui-Ying Chiang, Shu-Yuan Lin, et al 2010; Lawton and Parker, 2002; Firth Cozens, 2002) and the possible reasons why there was under reporting.

This chapter will set out why a scoping study was chosen, how the survey was designed and developed. It then outlines the selected conferences where it was to be distributed, its participants and the response rate. The chapter then examines the results of the survey logically examining each sector of the survey. It will include a selection of relevant comments from respondents and a number of tables setting out the comparison of each conference as well the overall picture against each question. It concludes with an analysis of the results before identifying the lessons that were learnt and finally a conclusion and identification of the next steps. At the same time that the survey was undertaken the organisers at one of conferences invited the researcher to conduct a work shop into the reporting of incidents. This workshop did not influence the scoping study but does produce some interesting outcomes and the details and outcome are included at the end of this chapter.

4.2 Testing the Assumption

At this stage of the research it was necessary to identify whether the assumption that security incidents were subject to under reporting was correct. The literature review in Section 2 tended to support this but there did not appear to be research that had actually asked the security professionals who would receive and manage such reports. There was a need to test the assumptions and three security conferences were identified where the attendees would be asked to participate in a scoping study. A formal questionnaire was developed and, at one of the conferences, a workshop was also conducted on the issue of security incident reporting. If the assumption was proved to appear valid then further research could be planned. If not the outcome may have resulted in a different research focus.

Under reporting of incidents was understood to be a problem in the healthcare sector. The report 'Organisation with a Memory' (Great Britain, Department of Health, 2000) identified a series of barriers to learning from adverse incidents. These were based on the reports widespread review of adverse patient incidents and included research conducted by Smith and Elliot (1999), Firth Cozens (2000) and Wason (1960). If a study of security professionals was to be undertaken relating to under reporting, it made sense to incorporated within the scoping study the views of information security professionals on the potential applicability of those identified barriers in the information security sector.

These barriers were;

- "An undue focus on the immediate event rather than on the root cause of problems;
- Latching onto one superficial cause or learning point to the exclusion of more fundamental but sometimes less obvious lessons;
- Rigidity of core beliefs, values and assumptions, which may develop over time – learning is restricted if it contradicts these;
- Lack of corporate responsibility – it may be difficult, for example, to put into practice solutions which are sufficiently far-reaching;
- Ineffective communication and other information difficulties – including failure to disseminate information which is already available;
- An incremental approach to issues of risk – attempting to resolve problems through tinkering rather than more fundamental change;
- Pride in individual and organisational expertise can lead to denial and to a disregard of external sources of warning – particularly if a bearer of bad news lack legitimacy in the eyes of the individuals, teams or organisations in question;
- A tendency towards scapegoating and finding individuals to blame – rather than acknowledging and addressing deep-rooted organisational problems;
- The difficulties faced by people in "making sense" of complex events is compounded by changes among key personnel within organisations and teams
- Human alliances lead people to "forgive" other team members their mistakes and act defensively against ideas outside of the team;

- People are often unwilling to learn from negative events, even when it would be to their advantage;
- Contradictory imperatives – for example communication versus confidentiality
- High stress and low job satisfaction can have adverse effects on quality and can also engender a resistance to change;
- Inability to recognise the financial cost of failure, thus losing a powerful incentive for organisations to change." (Great Britain, Department of Health, 2000, p.34)

For example if a health organisation has, or the staff believe there to be, a 'blame culture' the likelihood of an individual reporting an incident would be less than if the organisation was focussed on learning from incidents. (Kingston, Evans, Smith, Berry, 2004: Schectman, Plews-Ogan, 2006). Was this true for information security. In order to try to prevent reoccurrences of incidents it is important to embrace reporting to assist in this learning process.

With regard to the information security sector the scoping study aimed to identify the perceived level of reporting together with reasons why people, departments or organisations find the reporting of security incidents a challenge. What are the barriers? Are they people specific, organisational or a mixture of both?

The assumption is therefore, if a significant number of incidents are not reported, the data upon which decisions are made could be flawed. Subsequently initiatives to share security incident data to gain insight into the wider threats to sectors such as finance, pharmaceutical, government etc. would be adversely affected. Incomplete incident data could result in a false sense of security through lack of reported incidents and erroneous inputs to risk assessments. This in turn could place a higher degree of focus on certain types of incidents that are reported as being the main threat vectors.

The scoping study was constructed to gather both qualitative and quantitative data. The aim was to understand their experience of the reporting of security incidents and to understand the level of confidence they had in the actual number reported. Included in the survey were a number of identified barriers to learning and, potentially therefore, reporting incidents from research in the Healthcare sector. The identified barriers to learning from incidents may translate into similar reasons why people would not want to report information security incidents.

As there was little research undertaken in the information security area into barriers to reporting information security incidents, the research utilised findings from the Health Care industry as to the perceived barriers for reporting and learning from incidents (not security related, but relating to patients). It was felt that this would enable an examination of information security professionals' views on the relevance and portability of those findings to the information security arena.

The aim of the scoping study was to test the possibility that reasons for not reporting something were not necessarily related to a specific industry, but more to do with human behaviour and general reluctance to report something that went wrong. Elements of these findings were incorporated into a scoping study of the views of information security professionals.

The researcher was able to facilitate this through attendance at Information Security Conferences during 2011. The details are set out later in this chapter together with the method of design and distribution of a series of questions and the subsequent analysis of the results.

4.2.1 How does the Scoping Study Link to the Research Goals

Two of the four goals outlined in chapter one that this scoping study was intended to tackle these were;

(1) To test whether the assumption that not all information security incidents are being reported is correct.

The scoping study was aiming to provide an indication from the security professionals attending the conferences whether the assumption had any support.

(2) To examine whether research on incident reporting conducted in other sectors, such as healthcare, can be applied to the information security sector.

In a similar fashion if the assumption had support that incidents were under reported could research elsewhere assist in improving the level of reporting.

This scoping survey was intended to be used to provide an indication the support for both.

4.3 Survey Design Process

There is considerable guidance on survey design. Robson (2011) provides guidance on how to avoid problems with the wording of questions; whereas Bryman (2004, p.137) recognising that response rates to such questionnaires can be low and focusses on areas such as the attractiveness of layout, style and length of questions to improve this. Similarly Buckingham and Saunders (2004) provide guidance on layout length and types of question. Collis and Hussey (2009, p.192) suggest the following stages in designing a questionnaire.

> "Design the questions and Instructions
> Determine order of presentation
> Write accompanying letter/request letter
> Test questionnaire with a small sample
> Choose method for distribution and return
> Plan strategy for dealing with non-responses
> Conduct rests for validity and reliability"

It is the above framework that the scoping study and, if successful, subsequent surveys in this research will follow the same approach.

4.4 Development of the Survey

The section sets out how the scoping study questionnaire followed the guide set out by Collis and Hussey (2009) but also includes the element of representativeness not listed in their guide.

4.4.1 Design the Questions and Instructions

The survey mixes two types of questions that would result in quantitive and qualitative responses. This was a conscious decision; if only closed questions were asked, although statistics and inference could be achieved, the real insight, views and experience of such professionals would not be drawn out. The purpose of open questions enabled the respondents to contribute to the research qualitatively and not just respond to the question, thereby providing added value from personal and sector experience. The open questions offered a specific easy to answer tick box with the facility to expand the reason for their choice of answer if they wished. One section of the questions contained the findings from research in the healthcare sector as part of the test of portability of research from one sector to another. There were no questions that were of a personal or sensitive nature. A Likert scale is used in many of the questions. The survey contained instructions for its completion and return, as well as an overview of the research and how the respondent could contribute. The questions asked can be seen in section 4.6

4.4.2 Determine Order of Presentation:

The survey was set in a logical flow and included the opportunity for comment to clarify any answers given together with a final section which was free text for any comments the subject wished to add. The fact that it was completed by a worldwide audience without any questions regarding its completion does speak for itself, especially as the number of human errors in the responses was low. The majority of those who replied included their views in the various sections provided.

The survey was set out in 5 sections to ease the flow of requested information.

Section 1: This section was mainly used to identify certain information about the person completing it. This did not include gender or age as it was considered as unnecessarily personal necessary to identify the assumptions and the sample size was likely to be such that it would not be statistically significant in any case. This could be left as anonymous but primarily the request was to obtain sufficient information to place respondents in the public or private sector, business area and gauge the size of organisation.

Section 2: This section included a mix of question types investigating the methods by which incidents are reported that provided qualitative and quantitative answers. There was opportunity for the person completing this section to elaborate or clarify their answers. These text boxes were optional to complete but do add an insight into the rationale for the choice of answer.

Section 3: This section focussed on the respondent’s confidence in the level of reporting in their organisation and in general. This section primarily sought quantitative answers with the option to add value to the response through clarification or the opportunity to state a point of view.

Section 4: This is the main qualitative section as it places fourteen statements taken from the Healthcare report considered to be barriers to learning from and reporting incidents and thereby learning from them identified from the research findings ‘Department of Health: Organisation with a Memory, (2000)’. It was considered a good test of portability of research findings from one specific sector – health - and testing if they could be considered valid in another sector - information security. The respondents completing the survey were asked to state their view of each ‘barrier’s’ relevance to their industry through a 5 point Likert scale. A space for comment was provided offering insight into any selection made.

Section 5: This section did not contain any questions. It was designed to allow the person completing the survey to add any additional views or comments should there be insufficient space elsewhere

4.4.3 Write Accompanying Request Letter

Instead of a letter at all three events, the Chair of the conference introduced the survey and the importance of the research subject as well as the benefit of attendees having the opportunity to influence research in the subject at hand. On each occasion the chair introduced the author who referred to the questionnaire and the instructions, particularly focussing on the aspects of confidentiality and the voluntary nature of the survey. The questionnaire itself had a one page introduction.

4.4.4 Test Survey with a Small Sample

The draft survey form was tested and refined and then tested on some trusted colleagues to ascertain any issues with its design, flow and clarity. This resulted in a reduction in the size of the survey form.

4.4.5 Choose a Method of Distribution and Return

A printed version of the survey was selected. This was a deliberate choice, although the option for advance or subsequent completion of an electronic version was considered, as there are a number of versions of office software, and not all are compatible, this could prove problematic and detract from the completion of the survey. The NISC conference organisers in fact included an electronic version of the questionnaire in their pre-conference pack which was emailed to attendees and for which gratitude is given to the event organisers for doing so. Therefore the simplest method was to request they be completed by hand. This had the added benefit of ensuring the subject could remain anonymous should they wish to. The other method was to scan and e-mail the completed form back to a University address. This was chosen over a works address as this could possibly put some respondents off, again for fears of being identified, not just by the author, but by others monitoring such traffic. The use of the university address is more neutral and a requirement of the Cranfield ethics process.

The added benefit of being present at the events was to be able to identify and respond to any major discrepancies in the design or flow of the survey. Those completing it at the conferences could also hand it in at the event via the organisers, again providing a degree of anonymity should they wish. In the end there were no apparent problems in the completion of the survey.

Services such a ‘survey monkey’ do offer anonymity. However, a more personal, albeit confidential, approach was selected. The future use of an online version has not been discounted particularly as there is confidence that those completing the survey did not raise any concerns.

In the end, anonymity did not appear to be of great concern. As all attendees at the NISC and NG conferences had the opportunity to see and hear the author and to some extent understand they were not a distant researcher but someone from the same community they were, in the majority, more than happy to identify themselves. This was less so for the Oil and Gas conference as the author was unable to stay for the whole event. In fact the subject matter was of such interest that many wanted to have some form of feedback of the results when known, and were happy for further contact with them to be made. This opportunity was made clear on the first page of the scoping questionnaire itself;

> *If you do not wish be identified, could you at least indicate the nature and size of your organisation to assist in identifying any specific sector trends. If you are willing to engage with me for further discussions on your views and opinions I would be most grateful.*

The resultant proportion of respondents who took advantage of the ability to remain anonymous was interesting. Out of the sixteen survey respondents from NG Europe, fourteen provided their details representing 88% of the group content to be identified. For those attending NISC, sixteen out of the twenty respondents (80%) were happy to provide full details and one of the two Oil and Gas respondents did. Overall for the three conferences 85% were comfortable in providing details bearing in mind some of the sensitivity of the questions, and possible reputational damage should their identities and that of who they worked for, this figure is surprisingly high. Anecdotally it could be argued that there is a willingness to contribute further in the research as well as the acceptance of the assurances given regarding the protection and confidentiality of any responses.

A method was needed to distribute the survey forms. Three information security conferences being held in June 2011 were identified. One in Scotland, one in London and one in Lisbon, Portugal. The researcher was presenting at all three conferences and this provided an ideal platform to distribute the survey forms to the attendees. An approach was made to the organisers of all three events, seeking approval to utilise the opportunity to introduce the research subject and distribute the survey forms. All three were very supportive and included the survey within the delegate packs.

There was an opportunity to engage with the audience to provide brief reasons for the research, giving assurances by referring to the sections in the survey describing the process to maintain confidentiality and anonymity. The researcher was careful to ensure this engagement did not create any bias for its completion. It was judged the attendees would feel sufficiently interested in the subject to want to participate.

The survey content and design for all three events was the same, except that it indicated what event had been attended by those who completed the survey. There were two reasons for this; firstly, it made it more specific to that event and, secondly, it provided the possibility to identify if there were any significant differences in responses, depending on the conference that may require further investigation. It was anticipated that the type of attendees expected at each event, although in the main working in information security, were going to be diverse in the level of seniority, industry sector and location they operate.

To ensure anonymity there were a number of options available to return the completed survey. It could be completed then scanned and emailed or returned by post. The other method was simply to hand it in personally to an event organiser or the researcher. Anyone who wished to remain anonymous could choose the method in which they had most confidence. The majority of those completing the survey handed it in during the event. A smaller number chose either to complete it and post back or to scan it and e-mail it back.

4.4.6 Plan a Strategy for Dealing with Non-Responses

Determining what a good response rate is can be a challenge. It was accepted that paper based surveys often returned greater responses than online ones (Nulty, 2008) although, as more confidence grows in on line surveys, this could change. “As a general rule a response rate of 30% or greater for a postal or externally sent questionnaire is generally regarded as reasonable. A goal of 50% or more responses should be attempted in any questionnaire that involved face to face interviews.” (Neville, 2005, p.33).

In this survey this was a challenge as no written reminder could be sent as the survey was distributed to attendees by the organisers. The author did not distribute them personally, so could not send reminders. This is interesting, as to some extent it goes against most academic advice to ensure anonymity. If you target those who did not reply, this implies you know the identity of those who did. This was not achievable due to the anonymity of the survey. The request to complete the survey was reinforced at several opportunities during the conferences. The Chair at all of the events introduced the survey and at varying points during the event reminded attendees to complete the questionnaire if they wished. This was often made at the same time as the request for delegates to complete the normal conference feedback forms as the events progressed. However, at the end of two of the conferences the Chairman made the request to anyone who had not completed the survey to do so when they returned home.

4.4.7 Conduct Tests for Validity, Reliability and Representativeness

Collis and Hussey’s (2009) guide refers to validity and reliability but not representativeness. Easterby-Smith Thorpe and Lowe (2003) refer to reliability, validity and generalization. McNeill (1992) introduces his concept of three key areas regarding research; reliability, validity and 'representativeness'.

Validity

This relates to being confident the data collective reflects reality and is a true picture of what is being studied. (McNeill, 1992, p.15) The rationale for asking the completion to be anonymous was to elicit answers that were as near to reality as possible. Asking someone if they are doing something they know they should be, and getting them to say they do not, requires considerable assurance regarding confidentiality. There is an accepted risk of misinterpretation of a question. By going through trial runs with different people before deploying the survey should have reduced the likelihood of this occurring to a low level.

The fact that it was distributed at three completely different events demonstrates its potential portability across organisation seniority and countries.

Reliability

By ensuring the process and method of collecting evidence is reliable any future use of this method should result in similar findings. (McNeill, 1992, p.14).

The survey was designed so that it could be completed anonymously by attendees at the three information security conferences. If they were to be asked to complete it again anonymously, it would be safe to assume they would complete it in a similar fashion. The only exception being where any changes had occurred at their place of work regarding reporting processes. For example, if they had subsequently implemented a method of incident classification or introduced incident recording software their answers would be different. In general the facts should be the same, but some of the perceptions of the person filling the survey may have changed slightly. It very much depends on the time difference between the first time the survey was sent out and if it were to be re- issued.

Representativeness of the Participants

McNeill (1992, p.15) suggests it is important to ensure the group that are being studied are a true reflection of others in that group. As it is often too difficult to send questionnaires to the entire eligible group it is important the selected group are typical of others. Bryman (2004) comments that the researcher would wish to be able to report that the sample is representative of a wider group to enable the findings to be generalized beyond those who participated. Buckingham and Saunders (2004, p.70) also refer to the importance of the "people you interview need to be representative of the wider population from which they have been sampled."

By surveying information security professionals at a number of information security conferences the audience had already complied with the above. They were information security professionals from a wide mix of public and private sector organisations both UK and worldwide or suppliers to the same. In the main, at the NISC event software, hardware and consultancy suppliers were present as well as security professionals. These suppliers, although aware of the survey did not complete the survey unless they were also represented at the event, not just as a vendor, but where their own information security representative was present. As a result, when assessing the number of responses against those who could have responded some attendees (who were present as conference staff, organisers, product vendors etc.) were discounted, as were multiple attendees from the same organisation. In the latter case the assumption was made that one respondent from each organisation present would complete the survey. The fact that the majority provided their details in section 1 of the scoping questionnaire provided the opportunity to clarify this aspect. Upon analysis of the results 80% of those completing the survey gave their full details and there were no repeat organisations in those responses. The degree of completion would then be according to the organisational structure. A large organisation normally has a dedicated information security manager and team with a wider range of incidents and experience in their overall management with which to base their answers. Whereas in a smaller organisation a single person may well handle more of the overall process themselves.

Although this was a scoping study should the same survey be reissued to the similar respondents in the same environment it is safe to assume the responses would be the same except where any changes had taken place at their organisation which meant that a previous answer was no longer valid. For example, a change in the method of reporting incidents or an introduction of incident classification.

There is a need to ensure those responding to a questionnaire are reflective of the sector of the population as a whole. This is not easy as Robson (2011, p.276) suggests

> “carrying our real world studies can mean that the requirements for representative sampling are very difficult, if not impossible to fulfil.”

By selecting information security conferences and using the attendees as survey participants gave a degree of confidence the sample was representative of a wider group. It is recognised though that, as this was a scoping study, it may be those who responded may not have been a complete representation of those who manage incidents but the initial goal was to test an assumption. The surveys conducted in Chapter 5 and 6 had a greater emphasis on repetitiveness with an eligibility criteria as well as using recognised Communities of Interest. The next section outlines the three selected conferences and the survey participants.

4.5 Survey Participants

The Incident Reporting survey was distributed at three information security events in June 2011. This section sets out the three selected conferences. It provides a brief overview of the conference, its attendees and survey response rates.

The plan was to attend a predominantly public sector (NISC) and private sector (NG) events to enable some comparison but the actual sector representation would not be known until the event itself and then ratio of those who actually responded could influence this further. These ratios worked well by offering any likely differences in opinion between a mainly public sector group and that which was in the private sector. The other factor worth noting was the mix of seniority and nationality. NISC attendees who completed the survey could mainly be described as Information Security Officers (ISOs) who in the main are middle manager whereas those who attended the NG event were more senior being in the main Chief Information Security Officers (CISOs) who held more senior positions.

4.5.1 The National Information Security Conference (NISC) held in St Andrews Scotland on the 8th to the 10th of June 2011.

This is primarily a public sector conference attended by Information Security Officers (ISO's) and supported by a vendor exhibition. NISC is an annual event held in St Andrews, Scotland and has been running over a number of years. It has good relationships with Her Majesties Government (HMG) and agencies across the UK which gave a degree of credibility to this conference above other less well known ones. Unlike many similar events, which are more London centric, is held in Scotland to try and ensure greater participation by the Scottish information security community who may be less able to attend the more predominance of London based event. Having said that, the attendance from the rest of the UK was significant.

The attendees range from vendors, who demonstrate their Information security products, to central and local Government employees together with system integrators. Therefore not all attendees would be in a position to answer the survey.

The NISC organisers were more than happy to support the research and allowed the survey to be sent out in the pre event material as well as a printed copy being available in the delegates' packs upon arrival. This resulted in six surveys out of the overall total of responses of 20 being completed in advance of the event and sent either by e mail or by post in accordance with the instructions in the survey form. The added benefit of early completion gave the reassurance that no one identified any flaws in the flow or content of the survey. Had they done so, despite the testing, it would have enabled the researcher to consider making any changes prior to the main event.

Due to NISC's Scottish connection, the Scottish Information Assurance Forum (SIAF) also holds a session at the event and the majority of those who attend this continue to participate throughout the NISC event. The Chair of SIAF asked for a brief overview of the research to be presented to the attendees as he and others in SIAF thought it of value. This was given during a brief ten minute period to, in effect, repeat what was on the front of the surveys and answer any questions that attendees might have. It is possible that this briefing may have encouraged participation in the scoping study but the questionnaire did not have facility to see if this was the case.

Response rates for NISC (National Information Security Conference) St Andrews,

Out of a potential number of delegates who would be eligible to complete it of 70, a total of 20 completed survey forms. This represented a return rate of 29% with the Public Sector being the largest group at 75% of the respondents. Note; a considerable number of attendees were vendors who would not be in a position to answer the survey. These were removed from the total number of prospective respondents.

4.5.2 The NG Security Summit Europe held in Lisbon, Portugal between the 14th and 16th of June 2011.

This is primarily a Chief Information Security Officer (CISO) event attended by large international private sector companies with no vendor exhibition. The NG Security Summit was run on a smaller scale than NISC but with a higher level of senior attendees. This was the first information security event the organisers had run. They had significant experience in IT conferences and the main difference from NISC was the approach to vendors. Whereas NISC had a vendor village the NG event there were no vendor stands. The conference was more intense and highly focussed. This difference is possibly one of the reasons why, although overall attendee numbers at NISC were higher than at the NG conference, the actual number of information security professionals present was a smaller proportion than the NG Conference.

Response rates for NG Security Summit

At the end of the NG conference a total of 16 completed survey forms were received out of 44 who would be eligible to complete it. This represented a return rate of 36%. With 94% coming from the private sector.

At the NG event there were no vendor stands. The conference was more intense and highly focussed. As a result the proportion of attendees eligible to answer the survey was higher than NISC. Another factor of a higher return rate may have been the researcher was asked by the organisers to run a workshop on the research topic and so as an element of trust and confidence in the researcher may have encouraged completion. The workshop is outlined in section 4.

4.5.3 The Cyber Security for Oil and Gas held in London on the 22nd June 2011.

This conference was held in the Grosvenor Hotel in London. It was mainly attended by technical security and counter fraud staff from the Oil and Gas industry. The researcher was presenting on a related subject but again approached the organisers to see if they were willing for attendees to consider completing the survey. At this conference the researcher was only present for their morning presentation session up until lunchtime.

Response rate for Cyber Security Oil and Gas

Unlike the NISC and NG conferences the author was unable to stay for the whole event and not present to engage with the audience and therefore missed the opportunity for gaining their trust and to raise the profile of the subject matter. This together with the fact that the attendees were not CISO’s or ISO’s but more technical in nature, adversely affected the number completed surveys. Only two responses were received from this event. These have been included in the overall scoring of survey responses but, due to the low number, not included in comparisons in the same way as for the NISC and NG events.

4.5.4 Summary of Conference Participants

There was considerable interest in the research at both NISC and the NG conferences and by being in attendance to answer questions, the authors assurances about anonymity and confidentiality appeared to be accepted by attendees. Attendees were keen to find out when the research results would become available possibly indicating the interest in the research and its relevance to their role.

The researcher, by being part of the community, was accepted and trusted. It was believed this would result in obtaining information in a subject area that, to individuals and organisations, is sensitive and where other researchers would have experienced difficulty in eliciting the same level of detail and data.

The next section describes the results and outcomes of the survey. It highlights any differences in responses by conference group and includes examples of specific comments made by the respondent's answers

4.6 Survey Results

The results of the completed surveys make use of the ability to compare figures from the two main conferences as well as including the completed surveys from the Oil and Gas conference. Without the advance identification of the different events in the survey preamble valuable research pointers and comparisons would not have been possible. For example, the ratio of public to private sector in attendees at NISC was 75% public sector and 25% private whereas the ratio at NG Europe was reversed with 6% public sector and 94% private sector. To some extent when comparing the NISC against the NG results it is possible to infer any possible differences between the opinions of public versus private sector Information Security professionals. The next section provides a breakdown of results by section. The full table of results is reproduced at Appendix 3

4.6.1 Survey Section 1 - Details of Respondents

Based on the responses to the question that asked where their organisation was based (UK, Europe or elsewhere including if multi located) the group from NISC indicated they were primarily UK based. For NISC, 90% indicated the UK was either their sole base or they were also based there, as opposed to 25% who stated they had a European base. For NG the ratio was 44% had a base in the UK whereas some as well as a UK base indicated a larger number of bases, 75%, were in Europe and elsewhere.

Q. If your organisation is multi-based do you feel your answers given may be different according to the country where the incident occurred?

The rationale for this question is whether there were any cultural or legislative reasons that may be a factor. For NISC 25% felt that answers may be different according to the country where the incident occurred, however, no one made any additional comment.

With regards to the NG group 69% felt there may be a difference and as a result there were more comments. These included;

A company that was globally present in over 100 countries.

> *"Differing laws, regulation and cultures affect what is in place where"*.

A company based in Europe.

> "*Culture is different. Awareness level is higher in the UK than what it is in other European countries where we have operations."*

A company based outside Europe

> "*XX is a multi-based company. We can definitely see a different reporting from different sites. E.g. Less from India, China. More from US and YY"*. [sanitised home country]

A worldwide company.

> *"Need to take into account the culture."*

Another worldwide company.

"Have a globally consistent policy and processes that govern these activities. Although recognise that data breach disclosures in some jurisdictions will require localised custom responses. Especially true in the U.S."

The above responses tend to indicate that there could be differences dependent upon where the incident was reported, which in turn may have an effect on reporting rates.

4.6.2 Survey Section 2 – Incident Reporting Requirements and Methods of Reporting.

Q. Are you subject to any regulatory reporting for incidents (e.g. FSA, HMG, contractual?) If yes - please describe

For NISC the 'yes' response was 70% and NG a lower score of 50% which was interesting due to the fact that a number of attendees at NG were from organisations that would be accountable to regulatory bodies. However, the NISC figures included Government policy and Information Commissioner requirements to report incidents as a number of the comments identified. Other examples given by the NISC attendees of bodies to which they had to report incidents to included Health Departments, FSA, GovCERT and PCIDSS. In the main these reflect the Public Sector orientated group that attended. Even though there is no specific data breach notification legislation in place in the UK, it is clear from some of the comments that there are a number of avenues to report and an expectation in some sectors that they will be.

NISC comments included;

> *"ICO/FSA"*
>
> *"We report to the [country] Govt Health Department and have health specific regulations"*
>
> *"HMG and Contractual"*
>
> *"GOVCERT reporting as prescribed by [network] Code of Connection"*

Examples of NG comments included; Legal requirements such as Sarbanes Oxley (SOX). There were also examples of NG organisations that had multiple locations having to report to different standards. Examples of the responses being

> *"Reporting incidents impacting availability of systems to regulators, with slightly different rules/requirements depending on the country."*
>
> *"Local legal requirements, Central Bank of [Home country], EU legislation."*

One company referred to the need to report breaches to customers;

"Data breaches related to clients must be reported." The comments here again reflect the majority of NG attendees being from the private sector.

Q. Do you have a formal policy and procedure for reporting?

In both groups, due to the respondents being subject to various forms of regulations, it was not surprising there was a high response that there are policies and procedures in place. For NISC it was 95% and NG 88%. This still leaves a small number in both groups who have no formal policy for incident reporting.

Q. What methods are used to report incidents (tick all that apply)

	Verbal	E Mail	Form	Website/ intranet	Line manager	Specific person team	Anonymously	Other
NISC	75%	80%	50%	35%	80%	70%	35%	10%
NG	56%	88%	44%	56%	56%	75%	56%	13%
Total (inc. Oil & Gas)	68%	79%	45%	42%	66%	71%	45%	13%

Table 4-1 What Methods are used to Report Incidents

This showed a selection of reporting methods and respondents could tick all that applied to them. A wide variety of methods were listed and only a few additional ones were added by the respondents; one being 'forensic team'. The most used methods by the NISC group were to their line manager and by e mail (both 80%). For the NG group e mail was the highest (88%) followed by a specific team (75%). Although there were no comments to indicate why there was a difference, the fact the NG group had a wider distribution of locations, many worldwide, and the reporting methods in place may be different.

Q. How would you rate your current reporting system?

Bearing in mind the above scores for what methods are used to report incidents, the figures returned (see table 4-4) show for NISC attendees a split of 40% for both fit for purpose and adequate. With a fifth (20%) stating it was not fit for purpose. For the NG group the results were not so favourable with the majority (44%) stating the system was adequate and only a quarter (25%) stating it was fit for purpose. The remaining 31% feeling their reporting mechanisms were unfit.

	Fit for Purpose	Adequate	Not fit for Purpose
NISC	40%	40%	20%
NG	25%	44%	31%
Total (incl. Oil & Gas)	32%	45%	24%

Table 4-2 Rating of Current Reporting Systems

Q. If you were in charge of the incident reporting system, what changes, if any, would you make?

From the NISC Delegates 65% made comments including allowing for anonymous reporting, improve incident classification and subsequent analysis. Others thought there could be improvements in the reporting mechanism suggesting solutions such as intranet based reporting and improvements to user training. One response highlighted the need to improve the reporting of incidents by suppliers and delivery partners. There were a number of other comments including the need for incident reporting categorisation and the method of reporting i.e. forms.

Examples of comments made include

NISC;

> *"Add clarity to classification of incidents,"*
>
> *"Allow for anonymous reporting"*
>
> *"Improve reporting by suppliers and delivery partners"*
>
> *"Expand policy, training and awareness, intranet form, better definitions of an incident, lessons learnt. Investigative and audit resources."*
>
> *"Better user training"*
>
> *"More user education"*

For the NG attendees 75% made comments. Examples are shown below

> *"Formalise the process to ensure reporting, Train/educate users to report"*
>
> *"Need a better system and more awareness to end users"*
>
> *"Raise awareness"*

These were broadly similar to NISC including emphasis on better education and training for users as well as the need for incident classification. Some of the comments made here reflect the development of the Critical Success Factors through the Delphi study in chapter 5.

Q. Who investigates reported incidents?

For both NISC and NG the answer 'specific person/team' was the highest with 85% and 81% respectively. For the two Oil and Gas respondents it was 100%. Therefore it may be the case this is a standard practice across all sectors.

Q. Do you use any software tool to manage the reports/provide management information?

In both groups the majority make use of a software tool to assist - NISC 55%, NG 63% (note no software packages were mentioned)

Q. Do you use any 'incident definitions' in separating incident types?

For NISC, 50% use definitions and at NG 75%. What is clear is, even with those that use definitions, they are specific to the organisation therefore making comparisons extremely difficult. This highlights one of the potential problems of numerous Government and industry sector aims for sharing incident data to provide a greater overview of the frequency of types of incidents. Without common incident data definitions, merely sharing numbers of incidents, differently classified has the potential to complicate the overall picture. On examining the responses to this question the answers given are high level and do not contain any specific incident definitions. Two respondents said they had a more detailed list and one sent it in.

This lack of incident definition adversely affects those looking to integrate incidents reported into a bigger picture. The results indicate organisations either classify incidents or they do not. Those that do tend, from the comments provided, either to look at factors such as impact or place them in vary general criteria. It was one of the reasons to include a suggested incident definition for the Delphi and Validation study's to try and gauge responses against a common definition.

Examples of comments from those who do try to classify the incident by type are;

Some NISC attendees referred to asset type e.g.

> *“Physical, IT and Personnel.”*
>
> Others to incident type e.g.
>
> *“Theft, virus, unauthorised access."*
>
> Some referred to the value of the data;
>
> *“Personal data, non-personal data, protectively marked data.”*

Others related the incident to business impact for example;

> *“Incidents that need to be reported to the FSA (potential or actual customer impacting incidents) are rated as 1. Near miss; 2 Impact from a single dept.; 3. Operating division impact; 4. Whole company impact.”*

NG attendees’ comments included; Theft and fraud, social engineering and misuse of systems. Others tried to classify incidents according to impact for example

> *“Minor, significant, major.’”*
>
> *“By severity of business impact and confidentiality of information.”*

Q. Are other people/teams/ groups involved in the investigation of incidents or their resolution? (E.g. training, HR)

One reason for this question was to understand if incidents are just reported or actually investigated as to do this requires additional resource or capacity. True learning from incidents cannot occur if there is no analysis of cause. Equally if there is a lack of data this hinders any analysis

> “Good data is a pre-requisite to qualitative risk analysis and the lack of good data may be the main reason qualitative analysis of information security risk is not normally performed (Blakley, McDermott and Geer (202, p.99)

[It is interesting to note here that in the overwhelming number of incidents other staff from outside information security units are involved in their investigation. For NISC it was 90% of the responses and for the NG 100%. The additional resources that typically become involved are those from Human Resources (HR). This tends to suggest more emphasis on disciplinary action than root cause analysis

4.6.3 Survey Section 3 – Confidence in the Level of Reporting in your Organisation and your Opinion of Incident Reporting Levels in General.

Q. With regards to your incident reporting system, how confident are you regarding the number of incidents reported?

To some extent this question is key to the research as it gives the respondents the opportunity to comment honestly through the arrangements to ensure anonymity (although most chose to waive this) on whether the number of incidents reported represents the real picture. The breakdown of figures for confidence in the numbers of incidents reported is described and shown at tables 4-3 and 4-4.

As stated earlier the concern is that not all incidents are reported and therefore security and risk decisions are being based on flawed information

	With regards to your incident reporting system, how confident are you regarding the number of incidents reported			
Event attendees	All incidents	Majority of incidents	Some incidents	Few incidents
NISC	15%	20%	40%	25%
NG	0%	47%	47%	6%
Total (inc. Oil & Gas)	8%	30%	46%	16%

Table 4-3 Degree of Confidence in the Number of Information Security Incidents Reported

At NISC a low number scored all information security incidents were reported, where slightly more felt the majority were. The largest score being only some incidents are reported. Compare this with the findings at NG Europe where there was an equal split amongst those who either felt the majority or only some incidents were reported with a lower figure than NISC where they felt few incidents were reported. No one at NG believed all incidents were reported

.

	With regards to your incident reporting system, how confident are you regarding the number of incidents reported – aggregation of scoring	
Event attendees	Combination of All or the Majority are reported	Combination of Some or Few are reported
NISC	35%	65%
NG	47%	53%
Total (inc. Oil & Gas)	38%	62%

Table 4-4 Combination of Confidence in Number of Incidents Reported

Probably most organisations would ideally like to think that all or the majority of incidents would be reported. As can be seen for NISC attendees only 35% felt this was the case. The far larger proportion of 65% felt only some or few incidents were reported. For NG 53% of respondents felt only 'some' or 'few incidents' were reported. This clearly highlights a significant lack of incidents being reported in both groups.

When taking all the responses together the figures show a significantly smaller proportion of respondents (38%) have confidence 'all' or the 'majority' of incidents are reported as opposed to those (68%) who felt only 'some' or a 'few' are.

It is clear from this the view of the respondents was that many incidents are not reported. This supports the first goal 'to test whether the assumption that not all information security incidents are being reported is correct'.

The results in table 4-1 and 4-2 clearly show concerns re the number of incidents being reported.

Whichever way the results are looked at it seems there are likely to be barriers as all incidents are not reported. So despite having various methods available for staff to report incidents ranging from e mails, to forms or direct to line managers there is a lack of confidence that the true number of incidents are being reported.

Q. In your experience or opinion are some groups of workers more likely to report than others?

This question asked who was more likely to report and, who are least likely with an option of 'don't know'. The results may indicate where the effort and resources to improve reporting can be focussed upon. Amongst the responses there were some interesting variations. Table 4-5 below shows the responses when asked who is more likely to report an incident. Respondents could answer 'more likely', 'less likely' or 'do not know' for each staff type category. The do not know % is the remaining score but not shown in the table. Therefore, the percentage figures are showing selected preferences as opposed to distinct either/or answers.

	General Staff		Junior Managers		Middle Managers		Senior Management		Directors	
	More likely	Least likely	More likely	Least likely	More likely	Least likely	More likely	Least likely	More likely	Least likely
NISC	30%	42%	40%	32%	35%	32%	35%	26%	20%	32%
NG	33%	66%	60%	40%	87%	13%	40%	53%	47%	40%
Total (inc. Oil & Gas)	30%	55%	46%	33%	58%	38%	35%	38%	32%	46%

Table 4-5 Type of Staff Likely to Report Security Incidents

In the NISC, mainly public sector, group the result was a fairly even view spread across the board with the staff 'more likely' to report an incident being junior managers at 40%. The staff least likely to report being general staff at 42%. With the NG mainly private sector group the figures were more varied with middle managers standing out significantly being highlighted as 'more likely' to report at 87% and general staff 66% being 'least likely'. The overall scores, including the Oil and Gas, for the staff group 'more likely' to report, show Middle Managers at 58%, with general staff being 'least likely' at 55%.

The survey did not go into great detail regarding this element and it is possible that the perception middle managers are more likely to report may be affected by the method used internally by organisations for reporting incidents. It may also reflect the demographic of the respondent. It could possibly indicate the case that incidents are reported to more senior staff who then initiate the reporting process. Therefore, once aware, due to their position they had a greater degree of accountability and responsibility to report.

Q. Are security incidents reported to Board Level?

This question was inserted to gauge the involvement in the incident reporting process of Boards. The regularity was not clarified by a time scale of monthly, quarterly etc. One respondent from NG did not answer this question so the percentage scores allowed for this. Table 6 below outlines the results. For NISC respondents the highest score stated the Board were notified 'regularly' on incidents and although for the NG group this was a lower score of 27% whereas the highest score for NG was 47% for 'only if serious' when taken together including Oil and Gas the score of 'regularly' was still the highest at 41%.

	Only if Serious	Regularly	Occasionally	Rarely	Never
NISC	25%	55%	10%	5%	5%
NG	47%	27%	0%	27%	0%
Total (inc. Oil & Gas)	35%	41%	5%	16%	3%

Table 4-6 Incidents Reported to the Board

Boards appear to be kept regularly informed regarding security incidents. This might reflect the impact some incidents can have from a reputational or regulatory perspective.

Q. Is Management information on incidents created?

The majority in both groups answered yes to this NISC 75% and NG 69% with overall being 68%. The question was not asked how is this management information used. Should analysis of this information take place, bearing in mind the lower confidence in reporting, the management information will be somewhat is flawed in as much that not all of the incidents are reported. The following question asked if under reporting was a consideration in management information.

Q. Does this take into account under reporting?

The answers show 25% of NISC respondents stating 'yes' with the majority saying 'no' and one no response. For NG there were four who did not answer but the data shows a slight majority of those responding stated their figures cater for this.

Q. If subject to a serious/targeted malware or external attack do you warn/inform anyone outside of your organisation? (E.g. CPNI, WARP, CERT, GOVCERTUK etc.)

This question gave a refreshingly high number of positives in that there is a considerable amount of external reporting, albeit some is mandatory and others best practice or at least an expectation to do so. For NISC 90% stated they would report and 81% for the NG attendees with 82% overall.

Comments from NISC;

> *"Security agencies, WARPs, GovCERT, CPNI, CINRAS, Dept. of Homeland Security, FBI, Data Commissioner, colleagues in similar organisations, FSA, their Telecoms provider,"*

Comments from NG on what agencies these incidents were reported to included;

> *"ANSSI [French agency], partners and key customers, CPNI, police, central bank, clearing house, regulatory body, various agencies and regulatory bodies depending on country affected, CERT, local authorities, country specific forum for banks, industry wide information sharing network."*

The interesting point here is there is not one focal point for reporting. In some instances Computer Emergency Response Teams (CERTs) will be notified, but not by all respondents. Therefore providing overall statistics or insight of the real information security incident picture is a challenge. It is highly probable that any report that collates 'security incidents' will be missing considerable numbers of unreported incidents. This leads to an assumption that what is reported can, at best, only really be considered a snapshot. Particularly where it is clear the classification of such incidents is highly diverse.

The question continued - If no, are there any particular reasons why not?

There were no comments from NISC but comments from NG included;

"Not mandated" "company reputation", "organisation is reluctant to do so" "image".

It could be as the NG attendees were mainly private sector company image does have an influence on whether to report to another body.

Q. If certain types of incident were mandated to be reported to a central body (e.g. the ICO) what type of incidents do you think these should be?

For NISC the responses included;

> *"Malware, Distributed Denial of Service (DDOS) and other targeted attacks."*
>
> *"Personal information "*
>
> *"Where Criminal offences are involved"*

However, a note of caution was expressed with one respondent stating

> *"ICO, yes, but very reticent to do so because of reputational damage."*

For NG the responses had similar themes but also included the notion of providing the central body with;

> *"A general executive report on a regular basis."*
>
> *"Incidents that could impact on the economy."*

Comments from Oil and Gas included;

> *"Major attacks or incidents."*
>
> *"Thefts – devices, data, DNS, suspected hacking into network."*

There is a real mixture of comments here. Where most respondents recognise some types of incident should be mandated to report, there is a wide view on what these should be. This ranges from all information security incidents to the serious ones. The majority focussed on personal data loss. The wide range probably reflects on the lack of any type of universally accepted incident classification currently in existence. Again with the wide range of regulatory bodies' organisations have to report to depending on the sector they operate adding a central mandatory body with differing definitions

would no doubt cause problems in classification.

Q. Do you feel mandated reporting would increase the number of incidents reported locally?

	Mandation would increase reporting	Mandation would not increase reporting	Not sure
NISC	37%	37%	26%
NG	40%	33%	27%
Total (inc. Oil & Gas)	39%	33%	28%

Table 4-7 Would Mandated Reporting Increase Reporting

The results here are fairly even with NISC respondents showing an equal spread of 'yes' and 'no' of 37% with the remainder unsure. For NG it was 'yes' 40%, 'no' 33% with the remaining 27% unsure. Overall, with the Oil and Gas results included the proportion who said it would increase reporting was 'yes' 39% with 33% saying 'no'. The comments made regarding the mandated reporting and safeguards help to demonstrate why there is no clear winner here. For this issue to progress a great deal of work would need to be done with regards to classification and safeguards, together with issues surrounding the multiple number of bodies who already require reporting.

An attendee from NG made the additional comment; "*I do not feel it can be done."*

Q. If mandated reporting was introduced, what safeguards would you like to see in place?

Many NISC respondents commented on the need for a 'no blame culture' and protection for the reporting organisation. Other comments included:

"Mechanism for reducing blame if voluntarily reporting genuine mistakes. E.g. loss of laptop etc."

"Ability to hold off full report until investigation is complete. Any release of info on breach would need to be sanitised and as anonymous as possible."

"I would like to see incidents anonymised for press releases, I would also like to see less penalty imposed on those who report than those who do not report but are discovered to have not reported an incident – rewarding honesty."

'Cultural change issues.' (Possibly referring to response of reporting and how perceived by press, public and staff*),*

NG comments included;

"Anonymity' and *'protection of reputational risk"* was recorded several times as was,

"protecting the informer' and the data provided."

"A level of certainty of retained public anonymity."

"Protection against data leakage."

Oil and Gas comments;

"Non-disclosure and protection of data."

"Tight audience – not public."

The issues generally highlighted here are that should mandatory reporting of certain incidents be introduced, there would be concerns over who had access to the information, how it was disseminated and also the element of blame associated. There was reference to rewarding those who report and punishing those who do not.

Q. Do you read/make use of the various incident report surveys? (Verizon, Symantec, PWC etc.)

The responses were to a straight forward yes or no. The answers to this question are incorporated into table 4-8 together with the answers to the question below.

Q. Do you feel the security incident data they collect/made available to them represents; The Full Picture; Reasonable Picture; or Partial Picture

There are a few annual or bi annual incident and breaches surveys that are published – mainly by private sector organisations which try to collate and analyse security incidents, trends and costs. These include the PWC incident and breaches survey, Verizon's incident surveys and those produced by Symantec. The point of the question was to see what proportion of those who responded read such reports and to ascertain their views on whether they contained the whole picture bearing in mind earlier survey findings highlighted in this paper.

	Percentage who read incident report surveys	**What picture do they represent regarding the reporting incidents?**		
		Full Picture	Reasonable picture	Partial Picture
NISC	75%	0%	45%	35%
NG	94%	0%	81%	19%
Total (inc. Oil & Gas)	79%	0%	58%	26%

Table 4-8 Representation of Picture of Security Incidents by Incident Surveys

For NISC attendees 75 % read such surveys however none thought they reflected the full picture. The majority, 45%, felt they provided a reasonable one. For NG 94% read them but again no one thought such surveys capture everything but a higher proportion, 81%, thought the picture provided was a reasonable reflection of reality.

4.6.4 Survey Section 4 – Barriers to Learning from and Reporting Information Security Incidents.

This section of the survey was created to ascertain the views of the attendees at NISC, NG and Oil and Gas on a list of fourteen suggested barriers to learning from and therefore potentially reporting incidents from research in the Healthcare sector referred to in section 4.2. The barriers are reproduced in this section in the order they were set out in the survey. These barriers do not relate to learning from information security incidents but 'adverse patient incidents'. The value of such a comparison is to identify if the same human traits apply to both types of incident.

The respondents were asked to indicate to what degree they could apply as barriers to reporting and learning from information security incidents. Each statement included an option to select from a 5 point Likert scale of 'Strongly Agree', 'Agree', 'Neither agree/disagree', 'disagree and 'strongly disagree'. The tables highlighting the responses also include the overall agreement scores by combining 'strongly agree' and 'agree' together. Likewise the same approach is taken for generally disagreeing with the statement by combining 'disagree' and 'strongly disagree'. The middle option of neither agreeing nor disagreeing is not included in the combination scores.

Barrier 1. An undue focus on the immediate event rather than on the root causes of problems;

	Strongly Agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
NISC Combination	20%	45%	20%	15%	0%
	65%			15%	
NG Combination	25%	38%	19%	6%	13%
	63%			19%	
Total (inc. Oil & Gas) Combination	24%	40%	21%	11%	5%
	64%			16%	

Table 4-9 Barrier to Reporting - Undue Focus on Immediate Event

Both NISC and NG attendees selected ‘agree’ with 45% and 38% respectively. Overall, including Oil and Gas ‘agree’ was the most popular with 40%. ‘Strongly agree’ was the next highest. It is interesting that when looking at ‘agree’ versus ‘disagree’ and discarding ‘neither agree/disagree’, 64% of respondents ‘agree’ or ‘strongly agree’ that this is a real problem. These scores could indicate a support for a concern that if more focus is on the incident rather than the cause learning from any mistakes may be less likely to happen.

NISC respondents who indicated they agreed made comments such as;

> *“We do however have a culture of conducting RCA’s [Root Cause Analysis] post incident though not all incidents are captured. “*
>
> *“I believe one factor is fear that they have done something wrong or fear of getting someone else in trouble, combined with an ignorance of something to report”*
>
> *“It seems in these times of resource constraint many people look for expedient answers and focus on what’s ‘front of mind’ rather than cause elimination i.e. TREAT the SYMPTOM.”*

NISC respondents who disagreed made comments such as:

“*RCA always undertaken and possible improvements identified.”*

NG respondents who agreed made comments such as:

> "*Just pushing paper will not solve/prevent history being repeated, difficult to stop headless chickens leading to knee jerk reaction – I have no answer it is an observation."*
>
> *"Root cause analyses can help, - however if you manage to SLA [Service Level Agreement]why require a RCA in all cases."*

NG respondents who disagreed made comments such as;

> "*Believe that the service restoration/incident management is the necessary first step- once restored then appropriate route cause problem management should occur."*

Barrier 2. Latching onto one superficial cause or learning point to the exclusion of more fundamental but sometimes less obvious lessons

	Strongly Agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
NISC Combination	10%	30%	25%	30%	5%
	40%			35%	
NG Combination	13%	31%	44%	13%	0%
	44%			13%	
Total (inc. Oil & Gas) Combination	11%	32%	32%	24%	3%
	43%			27%	

Table 4-10 Barrier to reporting. Latching onto one Superficial Cause

For this question the responses were not so clear cut. Of the NISC respondents 30% agreed, 30% disagreed with 25% neither agreeing nor disagreeing. The NG respondents were clearer in their views with 31% agreeing against 13% disagreeing but a larger proportion 44% chose to neither agree or disagree.

NISC respondents who indicated they agreed made comments such as;

> "*Especially true if it would take resources to address the route of the problem."*

NISC respondents who disagreed made comments such as:

> *“for these incidents where an RCA is conducted, tools such as ‘5-why’ are used to avoid this”*

NG respondents who agreed made comments such as:

> *“Corporate need for closure at any cost preferably without the need for any cost.”*

NG respondents who disagreed made comments such as;

> *“Sometimes the above appears to be correct. However this is more driven by communication needs rather than waiting hours before communicating anything,”*
>
> *“Understand concern but down to style/approach of problem management. Necessary to look at in addition to root causes: 1, Trigger 2, aggravating factors 3, avoidance failures.”*

Other comments included those from NISC respondents stating neither agree nor disagree;

> “*Needs a holistic approach*.”
>
> *“Root cause analysis.”*

Barrier 3. Rigidity of core beliefs, values and assumptions, which may develop over time – learning is resisted if it contradicts these;

	Strongly Agree	**Agree**	**Neither agree nor disagree**	**Disagree**	**Strongly disagree**
NISC	10%	50%	25%	15%	0%
	60%			15%	
NG	19%	56%	13%	13%	0%
	75%			13%	
Total (inc. Oil & Gas) Combination	13%	50%	21%	16%	0%
	63%			16%	

Table 4-11 Barrier to Reporting - Rigidity of Core Beliefs

Clearer preferences emerge here with 50% of NISC respondents stating they agree and 56% of NG likewise. Only 15% and 13% respectively stating they disagree. When comparing agreeing to disagreeing NISC respondents totalled 60% with NG 75% agreeing.

NISC respondents who indicated they agreed made comments such as;

> *"This can be a danger but I would hope most people will try to understand any developing issue so avoid further problems in the future, degree of risk acceptance."*
>
> *"This is true of all science though."*
>
> *"Culture of senior management."*

NG respondents who agreed made comments such as:

> *"That is human nature – change is resisted, culture people and human nature condition a person to expect to follow rules."*

NG respondents who disagreed made comments such as;

> *"Depends upon organisational attitude – horses for courses I guess."*

Barrier 4. Lack of corporate responsibility – it may be difficult, for example, to put into practice solutions which are sufficiently far-reaching;

	Strongly Agree	**Agree**	**Neither agree nor disagree**	**Disagree**	**Strongly disagree**
NISC Combination	25%	55%	0%	20%	0%
	80%			20%	
NG Combination	19%	38%	25%	13%	6%
	57%			19%	
Total (inc. Oil & Gas) Combination	21%	47%	13%	16%	3%
	68%			19%	

Table 4-12 Barrier to Reporting - Lack of Corporate Responsibility

For this question there is again a clear leaning to agree with the statement. 55% of NISC respondents agree as does 38% of NG. Taking all who agree to some extent the scores are 80% for NISC and 57%. Interestingly the views of the NISC, who are mainly public sector (75%), felt very strongly about this. No one had a neither agree or disagree view. For NG the scores were slightly less in agreement mainly due to 25% not having a view either way.

NISC respondents who indicated they agreed made comments such as;

> *"All incident reporting should be encouraged by the head of an organisation, who should be setting an example."*

> *“Education of security with regard to ICT is particularly poor.”*

NISC respondents who disagreed made comments such as:

> “*Cost is a factor, existing regulations in the financial service industry and for any company that uses personal or payment data goes a long way to deal with service impacting events. Virus type incidents are another problem but a single piece of malware on the wrong server or workstation may be a problem. It would be difficult to report down to this level.”*

NG respondents who agreed made comments such as:

> “*Not sure if it would make a huge difference.”*

NG respondents who disagreed made comments such as*;*

> *“Not an issue in a highly regulated company.”*

Barrier 5. Ineffective communication and other information difficulties – including failure to disseminate information which is already available;

	Strongly Agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
NISC Combination	26%	47%	16%	5%	5%
	73%			10%	
NG Combination	31%	50%	19%	0%	0%
	81%			0%	
Total (inc. Oil & Gas) Combination	27%	49%	19%	3%	3%
	76%			6%	

Table 4-13 Barrier to reporting - Ineffective Communication

Again this question has resulted in a clear majority agreeing with the statement. 47% stating they agree for NISC and 50% of NG. The respondents who disagree were low in number. For NISC 10% disagreed to some extent but for NG no one disagreed with the statement in any form. Overall NISC respondents who agreed were 73% and for NG 81%.

NISC respondents who indicated they agreed made comments such as;

> *“Although there is some good communication, large organisation = SILO = generally poor communications, communication is a tricky one.”*

A valid comment from one respondent was

> *"You need to maintain confidentiality so the criminals don't know how successful they were but you also need to let staff know about malware and security threats."*

NISC respondents who disagreed made comments such as:

> "*We have disseminated much information, however this gets forgotten or ignored, and all staff get security awareness training."*

NG respondents who agreed made comments such as:

> *"The eternal problem – info leads to people not reading anything and thus missing important messages."*
>
> *"Not many tech staff have the ability to communicate the issue in business language."*

An Oil and Gas attendee who stated they agree commented

> *"Awareness is key"*

Barrier 6. An incremental approach to issues of risk – attempting to resolve problems through tinkering rather than tackling more fundamental change;

	Strongly Agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
NISC Combination	22%	33%	17%	28%	0%
	55%			28%	
NG Combination	13%	50%	31%	6%	0%
	63%			6%	
Total (inc. Oil & Gas) Combination	17%	42%	22%	19%	0%
	59%			19%	

Table 4-14 Barrier to Reporting - An Incremental Approach to Risk

Here there is an interesting difference of opinion between NISC and NG. NISC respondents although tending to agree also had a reasonable number of 28% disagreeing whereas NG only 6% disagreed and although 31% neither agreed nor disagreed 50% stated they agreed. Overall 55% of NISC agreed to some extent and 63% of NG agreed. There were no comments from NISC respondents who indicated they agreed.

NISC respondents who disagreed made comments such as:

> *“I hope this isn’t the case. With our incident management process we try to discover the root cause when we can and then feed back to a project improvement but it isn’t easy to ensure you have all the facts at the outset.”*

NG respondents who agreed made comments such as*:*

> *“Refer back – Get it fixed and move on mentality – no trend analysis means that trends are missed.”*
>
> *“Human nature drives this as well as economic and ‘fear of failure’ concerns. There is risk in grasping the nettle.”*

An Oil and Gas response from the respondent who agreed was;

The respondent who disagreed stated

> *“Not sure this poses a major barrier to reporting. “*

Barrier 7. Pride in individual and organisational expertise can lead to denial and to a disregard of external sources of warning – particularly if a bearer of bad news lacks legitimacy in the eyes of the individuals, teams or organisations in question;

	Strongly Agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
NISC	22%	26%	11%	42%	0%
Combination	48%			42%	
NG	6%	69%	6%	19%	0%
Combination	75%			19%	
Total (inc.	14%	46%	11%	30%	0%
Oil & Gas) Combination	60%			30%	

Table 4-15 Barrier to Reporting -Pride in Individual and Organisational Expertise Leading to Denial

The NISC attendees were fairly split between 26% stating they ‘agree’ and 22% ‘strongly agreeing’ totalling 48%. Whereas 42% stated they ‘disagree’. Here the NG attendees gave a large 69% response to generally agreeing with only 19% stating they disagree. This is quite a discrepancy between the two groups. The NG group clearly agreeing whereas the NISC group split. This may be a public sector v private sector issue in relation to the way that security is viewed.

NISC respondents who indicated they agreed made comments such as;

> *“Yes professional arrogance and protectionism”*

“But not sure if it is ‘pride’ or ‘assumption of trust.”

NISC respondents who disagreed made comments such as:

“Our *organisation is more likely to believe external expertise than internal”* (A local Authority respondent)

NG respondents who agreed made comments such as:

“Of course. There is always someone who will tell you that they told you so. Risk based decisions are not always 100%”

Oil and Gas attendees stated

“Perhaps too much acceptance that an incident or warning is a cost of doing business”

Barrier 8. A tendency towards scapegoating and finding individuals to blame, rather than acknowledging and addressing deep-rooted organisational problems;

	Strongly Agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
NISC	22%	11%	26%	42%	0%
Combination	33%			42%	
NG	25%	19%	31%	13%	13%
Combination	44%			26%	
Total (inc. Oil & Gas)	22%	14%	27%	30%	8%
Combination	36%			38%	

Table 4-16 Barrier to Reporting - A Tendency to Scapegoat

An interesting mix of responses. No NISC respondents stated they strongly disagreed but 42% disagreed. NG attendees had low scores for disagreement - 13% for both strongly disagree and disagree. Almost a quarter of both groups had responses of strongly agreeing

NISC respondents who indicated they agreed made comments such as;

“A belief that scapegoating and blame will occur is a major factor.”

NISC respondents who disagreed made comments such as:

“Blame culture is strongly discouraged although it persists in some locations and teams.”

“We allow staff to make anonymous reports if they wish, so I hope we do not look for a scapegoat.2

NG respondents who agreed made comments such as*:*

> *“I wish this was not true but it is.”*
>
> *“Comes with the territory in the CISO role. The higher you go the thinner the branch.”*

NISC respondents who neither agreed nor disagreed stated

> *“I’m sure this is true in some places but not prevalent in ours”*.
>
> *“Perhaps in some departmental areas but not endemic of whole organisation.”*

An Oil and Gas attendee who disagreed stated; ‘I *think we are past this.’*

Barrier 9. The difficulties faced by people in ‘making sense’ of complex events are compounded by changes among key personnel within organisations and teams;

	Strongly Agree	**Agree**	**Neither agree nor disagree**	**Disagree**	**Strongly disagree**
NISC	11%	42%	16%	32%	0%
Combination	53%			32%	
NG	13%	44%	25%	19%	0%
Combination	57%			19%	
Total (inc. Oil & Gas)	11%	41%	22%	27%	0%
Combination	52%			27%	

Table 4-17 Barrier to Reporting - Difficulty in Making Sense of Complex Events

A slight leaning towards accepting the statement. NISC and NG had 42% and 44% respectively of respondents selecting they agree with the statement. When the strongly agree selection is added this resulted in 53% and 57% respectively.

NISC respondents who indicated they agreed made comments such as*;*

> *“Especially in policing at the moment.’*
>
> *“This can be a real problem. Key staff tend to be relied on and it is easy to assume that staff will stay for ever.”*

NISC respondents who disagreed made comments such as:

> *“Locally turnover of key staff is insignificant”*

NG respondents who agreed made comments such as*:*

> *“Knowledge management is done but it is not effective due to the sheer volume of information.”*

“Relationships matter and they take time to build – especially with regard to trust.”

Barrier 10. Human alliances lead people to ‘forgive’ other team members their mistakes and act defensively against ideas from outside the team;

	Strongly Agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
NISC Combination	16%	47%	21%	16%	0%
	63%			16%	
NG Combination	31%	31%	13%	19%	6%
	62%			25%	
Total (inc. Oil & Gas) Combination	22%	38%	16%	22%	3%
	60%			25%	

Table 4-18 Barrier to Reporting – Human Alliances Tending to Forgive Within the Team

Again both groups tended to agree with this statement. 47% of NISC attendees agree with 16% strongly agreeing. 31% of NG agreed and also the same amount strongly agreed. Both respondents from Oil and Gas disagreed.

NISC respondents who indicated they agreed made comments such as*;*

“In some cases. In a council social care teams are more likely to be forgiving.’ Almost inevitable.”

Other NISC comments included*;*

“I hope this doesn’t happen as we try to have an open approach but there is always the danger that this can be the case.”

“May lead to incidents not being reported in the correct manner/at all.”

NG respondents who agreed made comments such as:

“That’s what good teams do!”

Other NG comments included;

“Depends on the incident. People and culture can be managed.”

NG respondents who disagreed made comments such as*;*

> *"Alliances are very often temporarily made. When an organisation adopts such attitude it starts an on-going process that means alliance needs to be break and /on extend in fact develops the openness."*

An Oil and Gas respondent who disagreed stated.

> *"This does not impact reporting – but we are past the blame culture"*

Barrier 11. People are often unwilling to learn from negative events, even when it would be to their advantage;

	Strongly Agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
NISC Combination	16%	26%	11%	42%	5%
	42%			47%	
NG Combination	25%	31%	19%	25%	0%
	56%			25%	
Total (inc. Oil & Gas) Combination	19%	22%	14%	38%	3%
	41%			41%	

Table 4-19 Barrier to Reporting – People Unwilling to Learn

A large proportion of NISC attendees disagreed – 42%, Where for NG the largest score went to agreeing at 31% but overall agreement versus disagreement was a percentage split for and against of 41%.

NISC respondents who indicated they agreed made comments such as;

> *"This is a danger we try to deal with."*

NISC respondents who disagreed made comments such as:

> *"Can often learn more."*

NG respondents who agreed made comments such as:

> *"Influencing and motivational activities can help. However these are many 'alphas' who all want control and influence."*
>
> *"Human nature again."*

Oil and Gas comments, both of who disagreed, included;

> *"Lessons learnt are key*."
>
> *"Not a problem for our industry*[1] *quite the opposite."*

[1] Energy Sector

Barrier 12. Contradictory imperatives – for example communication versus confidentiality;

	Strongly Agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
NISC Combination	16%	68%	0%	16%	0%
	84%			16%	
NG Combination	19%	50%	19%	6%	6%
	69%			12%	
Total (inc. Oil & Gas) Combination	16%	57%	11%	14%	3%
	73%			17%	

Table 4-20 Barrier to Reporting – Contradictory Imperatives

There was strong support for this statement with 68% of NISC selecting agree and 50% of NG doing likewise. Overall 84% and 69% agreed to some extent with the statement. NISC respondents who indicated they agreed made comments such as*;*

> *"Team v Corporate responsibilities."*
>
> *"With any attack on the infrastructure such as a hack, or DoS/DDoS it is important not to let the criminal know how close they came to succeeding."*
>
> *"People still do not believe that everything is confidential, and that if they do report something that they will not be identified as the person reporting."*

NISC respondents who disagreed made comments such as*:*

> *"Our data is confidential, it would not be shared any more than necessary but the lesson can be."*

NG respondents who agreed made comments such as:

> *"It depends on the individual and how confident they are."*
>
> *"Convenience versus security, TCO v ROI[2], You can program a system to do what it is told irrespective of external influences – not so with people."*

[2] TCO - Total Cost of Ownership versus ROI – Return On Investment

Barrier 13. High stress and low job-satisfaction can have adverse effects on quality and can also engender a resistance to change;

	Strongly Agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
NISC	32%	47%	11%	11%	0%
Combination	79%			11%	
NG	44%	38%	13%	6%	0%
Combination	82%			6%	
Total (inc. Oil & Gas)	35%	46%	11%	8%	0%
Combination	81%			8%	

Table 4-21 Barrier to Reporting – High Stress and Low Job Satisfaction

Both groups score highly in favour of this statement. For NISC 47% agree and 32% strongly agree. For NG an even greater leaning to strongly agree amongst the group with 38% agreeing and 44% strongly agreeing. Both respondents from Oil and Gas were in agreement.

NISC respondents who indicated they agreed made comments such as*;*

> *"Policy is in a state of flux, with major job insecurity and workload."*
>
> *"The human factor. Often working 8 hours or more will be more productive than working 7 but working 12 will usually be less productive. It can be hard to get the best out of people, at which point they may feel valuable but try to get that bit more and the stress builds fast."*

NG respondents who agreed made comments such as:

"High stress leads to need hide stuff – look at Nick Leeson!"

Barrier 14. Inability to recognise the financial costs of failure, thus losing a powerful incentive for organisations to change;

	Strongly Agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
NISC	26%	47%	5%	21%	0%
Combination	73%			21%	
NG	31%	44%	13%	13%	0%
Combination	75%			13%	
Total (inc. Oil & Gas)	27%	49%	8%	16%	0%
	76%			16%	

Table 4-22 Barrier to Reporting – Inability to Recognise Financial Costs of Failure

As with Question 13 another high proportion agreeing with the statement. With NISC respondents recoding 47% agree and 26% strongly agree. For NG a similar picture with 44% stating agree and 31% strongly agree. Both Oil and Gas respondents agreed.

NISC respondents who indicated they agreed made comments such as*;*

> *"We always try to cost any incident and that may be an actual cost and a potential cost, so we know how close we came to having a more serious incident."*
>
> *"Also reputational cost of failure is not understood /regarded."*

NG respondents who agreed made comments such as:

> *"Difficult to quantify cost, especially where reputational cost is evident."*
>
> *"We don't have the ability to define this very well yet."*

An Oil and Gas comment was;

> *"It is always hard to quantify value of the 'never happened'."*

4.7 Summary of Section 4 - Survey Responses

When comparing the responses of the main survey groups of NG and NISC attendees there was not a complete consensus of general agreement or disagreement across all of the barriers. In general the NG Europe attendees tended to agree with most but the differentials in levels of agreement for some questions were small.

Of the 14 barriers there were two where a difference of opinion appeared between the NG and NISC attendees. In these barriers (shown in table 4-16 and 4-19) the majority of NISC attendees tended to disagree as opposed to the NG attendees agreeing.

The barrier in table 4-16 *'A tendency towards scapegoating and finding individuals to blame, rather than acknowledging and addressing deep-rooted organisational problems'* showed for NISC an overall agreement of 33% against overall disagreement of 42% where NG attendees scored in agreement 44% against disagreement of 26%. For the barrier in table 4-19 '*People are often unwilling to learn from negative events, even when it would be to their advantage'* NISC attendees scored overall in agreement 42% against overall disagreement 47%, where NG attendees scored in agreement 56% against disagreement of 25%.

There was the risk that seeking views and degrees of comment on barriers from one sector, Healthcare, to another, Information Security, may not have worked. It may have been they were considered to be irrelevant. However, the response was good and many added comments to qualify their individual selections.

Acceptance of the Barriers - Which ones were supported most by the Information Security professionals?

Having requested the views of professional this section examines the levels of overall agreement or disagreement associated to each barrier. Of the fourteen barriers listed for comment the majority, eleven, had over 50% support from respondents as strongly agreeing or agreeing they apply to information security incidents. Only one barrier, number 8, had more not in agreement. However, the difference being only 2% with 27% neither agreeing nor disagreeing. Barrier 11 is split equally with those agreeing against those who do not.

To try and provide an indication of clear preference, any total of the scores of 'agree' or 'strongly agree' of 60% or more would arguably show support for the statement. When applied; nine of the barriers meet this suggested criteria. Were this indicator of clear preference raised to 70%, four barriers would still meet this with one close behind at 68%.

Table 4-23 below lists the barriers and shows the barrier number with an asterisk identifying those barriers whose combined 'agree' or' strongly agree' score is over 60%. Neither agree/disagree figures are discounted for this purpose. The figures represent the total responses from NISC, NG and Oil and Gas.

Note; barrier 6 is very close to the criteria with 59% agreeing and only 19% disagreeing. Due to the low number of respondents disagreeing, it could be argued that this too was generally accepted. Particularly as some of those barriers that met the 60% criteria had higher disagreement percentages. Namely barrier 7 (30%) and barrier 10 (25%) respectively.

Barriers with a score of over 60% General agreement are shown with an asterisk *

No	Barrier	General Agreement	General Disagreement
1*	An undue focus on the immediate event rather than on the root causes of problems	64%	16%
2	Latching onto one superficial cause or learning point to the exclusion of more fundamental but sometimes less obvious lessons	43%	27%
3*	Rigidity of core beliefs, values and assumptions, which may develop over time – learning is resisted if it contradicts these	63%	16%
4*	Lack of corporate responsibility – it may be difficult, for example, to put into practice solutions which are sufficiently far-reaching	68%	19%
5*	Ineffective communication and other information difficulties – including failure to disseminate information which is already available	76%	6%
6	An incremental approach to issues of risk – attempting to resolve problems through tinkering rather than tackling more fundamental change	59%	19%
7*	Pride in individual and organisational expertise can lead to denial and to a disregard of external sources of warning – particularly if a bearer of bad news lacks legitimacy in the eyes of the individuals, teams or organisations in question	60%	30%
8	A tendency towards scapegoating and finding individuals to blame, rather than acknowledging and addressing deep-rooted organisational problems	36%	38%
9	The difficulties faced by people in ‘making sense’ of complex events are compounded by changes among key personnel within organisations and teams	52%	27%

10 *	Human alliances lead people to ‘forgive’ other team members their mistakes and act defensively against ideas from outside the team	60%	25%
11	People are often unwilling to learn from negative events, even when it would be to their advantage	41%	41%
12 *	Contradictory imperatives – for example communication versus confidentiality	73%	17%
13 *	High stress and low job-satisfaction can have adverse effects on quality and can also engender a resistance to change	81%	8%
14 *	Inability to recognise the financial costs of failure, thus losing a powerful incentive for organisations to change	76%	16%

Table 4-23 Summary of Barriers

In Table 4-23 where there was a score indicating general agreement with the barrier of 60% or over this barrier is indicated by an asterisk. There were nine of the identified barriers to reporting and learning in the healthcare report that due to this score could be considered as applicable in the security reporting arena. These positive scores indicate that research in the health care sector relating to incident reporting can be considered as applicable in the information security sector, albeit for security incident reporting. It was this apparent portability of research from one sector to another sector that was further tested in the Delphi in Chapter 5.

It is worth noting that none of the surveys contained any comments in Section 5. This section did not contain any questions. It was designed to allow the person completing the survey to add any additional views or comments should there be insufficient space elsewhere.

A number of those who did respond and who gave their details, despite the offer of anonymity, showed genuine interest in being informed of the research findings. This was generally when handing in responses to the organisers and this feedback was passed back or in email responses with the questionnaire attached.

4.8 Reflection on the Survey Process

Due to using surveys in the next two stages of the research it was important to reflect early on the lessons learnt so as to avoid issues later on in the research. This section aims to identify the improvements that were needed to improve data quality. There were some problems with the methods used to complete the survey. As the respondents had identified themselves they were contacted to seek clarification, which they were more than happy to oblige. Where some answers were missing or unclear, reference to this is made in the spreadsheet used to collate all the responses and in the 'Table of Results' (See Appendix 3). Missing pages and ambiguous answers has been taken into account in any analysis.

Where there are comments from those who completed the answer they have been reproduced in italics and replicated the exact text. With some responses this does not make for good grammar or sense. It could be that this is as a result of the language of the person completing or just that the person completing was doing so in a hurry.

4.8.1 Lessons Learnt - What Worked Well?

The construct of the survey achieved its aim in eliciting honest and open views through the efforts made to ensure anonymity. Having said that, for whatever reason, the majority of respondents were more than happy to provide their full contact details. It could be assumed that this is due either to their belief in the research aims and the willingness to take part in further discussions with the author or that although provided with the opportunity to be completely anonymous they trusted the researcher in the promise to keep the identities confidential. The personal approach certainly assisted in obtaining a good response.

Bearing in mind this was not just a UK audience but a worldwide one, it was surprising that not one question was received seeking clarification in how to complete it. There were some errors in completion but these were the type of errors that could be made in completing any form. For example, missing out a section or adding information when it was not requested. As a result there were only a few where a note had to be made in the compilation of figures where a question had been missed. Interestingly there were no particular or repetitive mistakes. Therefore the error rate was small and the location of any mistake was random. However, it was noted that, despite the checking and validation, a small comments box at the end of question 2.3 had been omitted. The final selection box related to *'Other' (please describe below)* but the comments box was missing. This was annoying, however it did not affect the results as those who placed a tick against 'O*ther'* were only inserting a word or two to describe a function not covered in the choices. It is considered that this omission did not adversely affect the scoring or opportunity to comment by the responder.

It was surprising how many participants completed their contact details in full, as all good practice regarding formulating surveys point to the best results being from those who are anonymous. Despite this offering, an extremely high number provided their details and were honest in their answers (as far as one can tell).

The decision to identify the event that the person completing the survey attended by including reference to it, specifically in those distributed at the event, assisted in identifying any differences in responses that may have materialised specific to that event. Again, surprisingly the two main events were diametrically opposed regarding their type of seniority of attendees and the public/private sector mix.

It was particularly pleasing to see the number of non UK participants. This provided a wider insight into the views of security professionals who were not subject to the type of media and public attention in the UK at the time surrounding data loss incidents (HMRC, MOD).

The initial concern with regard to formatting issues was born out by some who tried to complete the word document electronically and found difficulty due to software compatibility issues. There is confidence now that the survey has been successfully deployed it is now worth the effort of creating it as an online document.

As inevitably there is a risk the survey could emerge onto the internet any use of home or work addresses could have caused potential spamming or identity issues. The choice to use the University e-mail address for contact purposes ensured that, although this risk still existed, the university address did offer some protection. In the event this concern has not manifested itself.

4.8.2 Lessons Learnt - What did not Work Well?

Surprisingly little went wrong apart from the problem with different versions of Microsoft Office resulting in the formatting of boxes being an issue. The length of the preamble was cut down following early reviews and a number of comments were received on how well the questions ran. Some comments were made regarding the wording of the barriers in Section 4 however, the wording choice was deliberate as they were taken directly from the previous research in the healthcare industry. The aim was to compare and identify if any of those barriers were relevant for Information Security. If the wording used was different this could have had the effect of nullifying any comparison.

Some interpretation of the handwriting did prove slightly challenging and this is where a typed response would have proved better. However for primary evidence of completion a personally handwritten response is far better. Also for those seeking anonymity (as it turned out most declined this) using a machine would have left a record should there be any comeback later.

Had the researcher been able to remain at the Oil and Gas cyber security event during the evening and following day more forms would have been returned. It should also be noted the event was not attended by the same type of security professional that went to NISC and NG. It was more aimed towards technical security and fraud rather than the CISO/ISO audience. In addition the maturity of the industry in regards to Infosec seemed less than others. This may only be an indication from the presentations viewed. For example one company had only just employed their first Information Security Officer.

4.9 NG Security Summit Workshop on Incident Reporting

In parallel an opportunity was provided by the NG Security Summit to delve further into some of the issues covered in the survey. Whilst it does not form the core part of the data collection it provided an opportunity to add some insights into CISO's thinking on the topic and as such is reported here for completeness. In particular, the aspect of the Department of Health (2000, p.45) research into "effective incident reporting systems".

The workshop was held as part of the NG Security Summit held between the 14th and 16th June 2011 in Lisbon, Portugal. There were approximately 35 people in the room who were either CISO's or had a similar role. The organisers ran a number of workshops and panel sessions and invited the researcher to run a 40 minute workshop on security incident reporting. This workshop could be considered as a form of focus group. A focus group is where the researcher acts as a facilitator to lead the discussion of a group to obtain an understanding of what individuals within the group, and the group as a whole, think about a particular subject (Buckingham and Saunders 2004; Yin, 2014). Although there was a slide set that was used to generate discussion, its primary intention was to get a high level view on the researches perception of a lack of security incident reporting. This was the first test of that assumption amongst a group gathered to discuss the issue as opposed to individually completing a questionnaire anonymously. As recognised by Bryman (2004) transcribing focus groups can be difficult and, at the outset, this was an opportunity for the researcher to make use of the offer of a slot at the conference as part of a series of practical workshops to discuss pertinent information security topics. This was an opportunity to gauge opinion on another element of the health care research.

This research workshop was held at the second of a series of three security professionals' conferences that the scoping study was distributed, but the only one that had a workshop. This workshop was the first of the scheduled events so at that stage, apart from the previous evening dinner, the attendees had not met as a group before which could have stifled debate. However, the subject matter appeared to be of interest to them as there was a full house of attendees.

There were approximately 35 in the room. The attendees were informed of the purpose of the research and that they were under no obligation to participate and they could withdraw at any time. They were shown some of the researcher's organisational 'in house' security incident training video clips to set the scene before introducing the subject through a set of power point slides. The workshop was entitled. 'Information Security Incidents – Are they reported?'

The second slide asked the question 'if not – why not' and followed up with 'What are the barriers?'

At NG Europe, during the workshop, the organisers also provided a member of staff to note any comments that came from any subsequent discussion on a flip chart. The workshop became quite lively and although many attendees felt that incidents were under reported there were differences of opinion on the reasons why. Interestingly a number of the reasons were closely linked to those identified in the Healthcare sector and as the comments started to come out it became easier to relate some of them to a slide entitled ‘effective incident reporting systems’. The comments were captured on a flip chart. These are shown as Appendix 1. The below is a short summary of the comments made by workshop attendees.

One attendee asked whether any research had taken into account gender. To date this had not specifically featured in identified research.

Questions were raised whether the litigatious nature of a country would affect reporting. It was felt by attendees’ that a greater influencing factor was the type of legislation and compliance regulations an organisation faced. Some organisations, which were based or operating from the US, were subject to breach notification legislation as well.

Some participants felt that one difficulty was that of employees not understanding the impact or consequences of a data loss and therefore not reacting to a situation as they did not recognise its seriousness.

There were comments that not all reporting mechanisms are effective and some work better when they reflect the organisations structure or culture. The theme of ‘blame’ and ‘repercussions’ to those who report were voiced. One comment made was the ‘Threat’ or the perception of sanctions to the person reporting must be removed somehow. This led to some participants referring to other strategies that some companies had adopted – anonymous reporting for example. One company suggested that it incident reporting had increased following the introduction of anonymous reporting. Another attendee commented that if staff report and there is no feedback they do not see the point. Others suggested that low levels of reporting are due to complex reporting mechanisms which meant employees could not see the benefit of reporting, particularly if their contribution or diligence was nor recognised. Some commented that more use should be made of technology (e.g. DLP- Data Loss Prevention) to improve reporting. Others felt that to just solely rely on technology was flawed in its own right.

Following the discussion the researcher then introduced the slides in their presentation (see figure 4-1 below) that reproduced findings from the Department of Health: An Organisation with a Memory (2000, p.45) report suggesting how incident reporting systems can be improved. These were compiled from the report's researchers experience in the safety industry and that of research in the aviation industry.

Effective Incident Reporting systems

- **Separate collection and analysis from disciplinary or regulatory bodies**
- **Collate information on near misses**
- **Feedback to those who report**
- **Make it easy to report in the first place**
- **Standardise reporting in your organisation**
- **Individuals should be thanked for reporting incidents, rather than automatically blamed for what has gone wrong**
- **Make reporting mandatory**
- **Standardise the impact and risk of reported incidents.**
- **Consider the potential for confidential or sanitised reporting**

Figure 4-1 Slide 9 from the NG Europe Workshop Presentation. An Extract from Department of Health: An Organisation with a Memory (2000, p.45)

Many of the earlier comments from workshop discussion were easily linked to some of the recommended bullets the presentation slide contained. For example; reporting mechanisms, anonymous reporting, removing blame and not receiving feedback. Although the slide list was taken from the Department of Health Report, the report itself had not specifically identified the link between the perceived barriers to learning and reporting and the need for effective reporting systems. The workshop attendees, having been exposed to the barriers then during a discussion on those barriers, and prior to the slide identifying the effective reporting systems identified in the report, began to identify methods of overcoming them that were similar to the effective reporting systems also contained in the report. This unrehearsed linkage appeared to demonstrate that the Department of Health report's findings had the capability of being further exploited in other sectors.

4.10 Substantive Contribution to Research in this Area

There are three areas where it can be demonstrated this research has provided a substantive contribution to the body of knowledge in the subject of Information Security Incidents. Firstly, the scoping study shows amongst the participants there is a lack of confidence that all or most information security incidents are reported. A range of views from information security professionals from both the public and private sector has validated the researcher's assumption that the true number of information security incidents is not known due to under reporting**.** This is despite 58% being subject to regulatory reporting. With only 38% believing all or the majority of incidents are reported as opposed to 62% only believing that some or few are reported.

Secondly the study has demonstrated that findings from research in a different sector, Healthcare, into a similar problem of incident reporting and learning from incidents has the potential to be used in the information security sector. As the barriers are human or organisational (or a mixture of both) it could be concluded that any strategies or methods developed to overcome these barriers in one sector could have the potential bring a degree of acceptance and success in that of another. To some extent the workshop held in Lisbon demonstrated this where the discussion over ways to improve incident reporting led to very similar comments to those contained in a summary slide of findings from the Healthcare sector.

Thirdly the methods used to elicit sensitive information from potentially reticent participants proved successful and could be imitated by others conducting similar sensitive research.

4.11 Conclusion

This scoping study has shown that following recognised methods for the construct of surveys can bring about valid and honest responses and where the responder feels confident in the handling of their information and comments. This in turn has provided a strong view that incident reporting in itself can be complex as can the reasons why they are, or are not, reported. The mix of quantitative and qualitative answers has provided interesting responses and views that a simple quantitative survey would be unlikely to elicit.

It is also apparent that barriers to reporting do exist, as the consensus is that not all incidents that occur are reported. Therefore, the current trust placed in the outcome of risk assessments needs to be carefully considered as an element of any risk assessment is based on likelihood of the occurrence of a threat or vulnerability.

The findings of this survey furthers the knowledge regarding the reporting of information security incidents by clearly identifying, though validation from a wide range of information security professionals, that not all incidents are reported. By saying not all, this in fact relates to a considerable number that do not come to official notice. Thus potentially putting into jeopardy assumptions made by a range of risk assessment calculations, where security incidents form part of that analysis.

Most organisations have considerable avenues open for staff to report incidents including forms, e mail, by phone, to line managers etc. but despite this only 32% have confidence these systems are fit for purpose.

There appear to be issues regarding incident definitions. From the responses, those who did describe how they classified incidents did so mainly from internal definitions. There is at present no national or internationally accepted definition of a security incident. The recently introduced BS ISO/IEC 27035 Information Security Incident Management standard (2011) may lead to this. This is an area that will need further research. This lack of incident definition adversely affects those looking to integrate incidents reported into a bigger picture. The results indicate organisations either classify incidents or they do not. Those that do tend, from the comments provided, either to look at factors such as impact or place them in various general criteria.

The barriers to reporting and learning identified in the healthcare research drew a mixed response of agreement. This is described in more detail in the report but there are some aspects where certain barriers appear to be well recognised and agreed as relevant in the domain of information security.

The issue of the introduction of legislation or regulation wider than the current measures to mandate the reporting of certain types of incidents drew a mixed response with 39% feeling this would result in an increase in reporting. It is interesting that, even if the mandatory reporting of information security incidents was introduced, the view was there would not be a significant increase in reporting.

Referring back to the goals that this scoping study was intended to tackle these were

> (1)To test whether the assumption that not all information security incidents are being reported is correct.

This was achieved as there was a clear margin of respondents that believed there was under reporting.

> (2) To examine whether research on incident reporting conducted in other sectors, such as healthcare, can be applied to the information security sector.

This too was achieved as there were nine of the barriers to learning from incidents scoring over 60% agreement that they were relevant in information security. The workshop also indicated that other research from the Department of Health report (2000) into "effective incident reporting systems" appeared to have a linkage between those reporting systems and the barriers and could equally be applicable in the information security sector.

This scoping study leads to the need for further consideration into how the issue of incident reporting can be improved. The issue of a lack of a common incident definition will also need to be resolved particularly to ensure future studies can at least ensure when respondents answer questions relating to incidents there can reference a specific definition. Chapter 5 investigates the Critical Success Factors to improve security incident reporting.

Chapter 5 Obtaining the Consensus of Information Security Professionals through a Delphi Study

5.1 Introduction

Chapter 4 set out the findings from the scoping study and how it achieved two of the research goals. These being confirming the assumption that information security incidents were under reported and that there is a potential to re-use research on barriers to learning from incident reporting from other sectors. This chapter sets out the methodology and reasons for the selection of a Delphi study to which invited information security professionals to contribute to, and arrive at, a consensus as to what constitutes the Critical Success Factors to improve the reporting of security incidents. This would provide further assurance with regards to goal 2 and address goal 3.

It sets out what a Critical Success Factor is and how the Delphi study was used to identify those CSF's required to improve security incident reporting. The chapter also includes the construction process and distribution of the Delphi survey form, the rounds, together with the outcome and findings. This Delphi study was developed from the research obtained from the literature review (Chapter 2) and the scoping study (Chapter 4). The Delphi outcome; a consensus as to the Critical Success Factors required to improve security incident reporting, would then need to be communicated. The use of a Maturity Model was identified for this purpose and this is referred to in this chapter, but dealt with in more detail in Chapter 6.

It can be the case that when an enquiry or report publishes its findings, whether it is the result of a disaster, significant event or one commissioned to resolve a problem, the valuable content is not always taken up as organisational cultures are resistant to and or difficult to change (Perrow, 2007; Schein, 1992). This research investigates the potential to make use of recommendations from such reports and academic research in other disciplines for the potential reuse and benefit of the information security sector. The common elements relating to the reporting of incidents, particularly the perceived barriers to such reporting, identified from research elsewhere could influence and potentially improve security incident reporting. The scoping study in Chapter 4 identified that these elements had the potential to be reused. A method of extracting the benefit from the findings and putting them to practical application was required.

As this research already suggested there is a perceived problem with the reporting of security incidents in general. Simply publishing a list of what elements could improve the situation neither has the contextual application of those findings in the information security sector, nor any validity on what could actually work. Refining the elements to identify which ones could make a real difference would need further research. Chapter 3 set out the methodology that identified the use of Critical Success Factors as a recognised method (Caralli, 2004) for identifying the important elements for success. It was considered such an approach would take security incident reporting forward, this chapter expands on that.

5.2 What is a Critical Success Factor?

There are a number of definitions of Critical Success Factors. Bullen and Rockart (1981, p.7) define them as; "the limited numbers of areas in which satisfactory results will ensure successful competitive performance for the individual, department or organisation. CSF's are the few key areas where "things must go right for the business to flourish and for the manager's goals to be attained". Elsewhere the software Engineering Institute describe them as;

> "The handful of key areas where an organisation must perform well on a consistent basis to achieve its mission. CSF's can be derived through a document review and analysis of the goals and objectives of key management personnel, as well as interviews with those individuals about their specific domain and the barriers they encounter in achieving their goals and objectives". (Gates, 2010, p.xi)

Bullen and Rockart (1981) continue in describing what Critical success Factors are not. They should not be used as a standard set of measures. They are areas of major importance for a particular group at a particular time. Whilst CSF's are in use in industry, retail for example, they have not been commonly used in government although there are reports on their use in healthcare (Eni, 1984; Gates, 2010). The use of Critical Success Factors in this research is to attempt to set out what is really important to set in train or achieve to bring about an improvement in the process for identifying and reporting of information security incidents thereby enabling better informed judgment for risk management and increasing the amount of data that can be effectively shared, analysed and acted upon within organisations and further outside to relevant sectors and even nationally and internationally. CSF's provide the tool to prioritise issues already identified as a priority. Their use can enable appropriate levels of focus on what must be done particularly where concentrated attention from management is required (Eni, 1989)

CSF's to be successful must not be large in number otherwise the focus is lost. Freund (1988) identified from research common problems associated with identifying and implementing CSF's

Symptom	**Probable Cause(s)**
Too Many CSF's	**Defined at too low a level** • **Confusing CSF's with performance indicators**
Incorrect CSF's	• **Unrealistic view of marketplace** • **Solving "political" problems** • **Strategies defined before CSF's are identified become self-fulfilling prophecies**
Weak Performance Indicators	• **Improper linkage to CSF** • **Boss sees data, but subordinate doesn't**
Management Frustration	• **Insufficient front-end training for participants** • **Insufficient time allowed** • **Planning process overly complex**

Table 5-1 What Can Go Wrong. Freund (1988, p.23)

Similar issues are reported by Poon and Wagner (2000) where a number of organisations who had set CSF's were studied. They suggest that CSF's are "the conditions that need to be met to assure success of the system" (Poon and Wagner, 2001, p.395). Either they were a success or a complete failure. Their research led to some valuable key elements required for any CSF's to be successful. These were referred to as "Meta success factors" (Poon and Wagner, 2001, p.393);

> "Championship" - someone has to lead the effort and
>
> "Availability of resources" - without this the process will struggle and finally "link to organisations objectives" – an organisation will struggle to make any progress on CSF's that are not really deemed critical for that business.

If these were not in place the CSF's were likely to fail whereas when the above are in place the CSF's are successful in achieving the overall aims set across a number of organisations. Mendoza et al (2007) utilised CSF's across a number of disciplines; processes, human factors and technology. It is clear that CSF's can be utilised in differing scenarios and with different approaches. The key is to gather information from the right sources; hence the proposed Delphi to identify the CSF's is asking a group of information security professions from differing communities of interest.

Leidecker and Bruno (1984) state that the identification of Critical Success Factors is an important element in developing an organisation strategy. Rockart and Bullmer (1984) suggest a two stage approach to identify the CSF's through an interview based discussion of the goals followed by identification and development of the CSF measures. Whereas Caralli (2004) suggests a five stage approach, which commences with the scope then data collection followed by analysis before the CSF's are devised, then finally they are analysed. Indeed Caralli has reported on the use of CSF's in an Enterprise security environment in which he describes the use of CSF's as a simple and powerful concept. Boynton and Smud (1984) propose that although recognised as being applicable in developing and organisations strategic plans CSF's can also be equally applicable to be used to identify critical issues associated with implementing a plan. They also state CSF's can be flexible and do not require a rigorous format and therefore offer advantages in their applicability to different uses. They do however identify a risk that flexibility can also lead to 'an overly casual approach to their application.' (Boynton and Smud, 1984, p.26) Whilst the use of CSF's in this research is not focussing on one organisation but a generic issue the intended outcome is the same. The description by Freund below and the intended outcome for this research use of CSF's are similar, he describes Critical Success Factors as:

> "Important to achieving overall corporate goals and objectives,
>
> Measurable and controllable by the organisation to which they apply,
>
> Relatively few in number – not everything can be critical,
>
> Expressed as things that must be done not the end point of the process,
>
> Applicable to all companies in the industry with similar objectives and strategies and are hierarchical in nature." Freund (1988, p.20)

In this research the overall goals and objectives are to provide a method by which organisations can improve their incident reporting. The factors are measurable through the use of the Maturity Model and the outcome of increased reporting which feeds into risk management locally and further afield.   The number of CSF's is determined by use of a Delphi survey of information security professionals, using a Likert scale to identify the CSF's importance. The aim being to identify from the Delphi respondents whether the suggested elements are achievable as outcomes and they are applicable to the information security sector. The use of security professionals to identify the CSF's is endorsed by Boynton and Smud (1984) who state that the factors should be elicited from those who represent a cross section of the major functional areas. As Gates (2010) points out although CSF's cannot guarantee an outcome they are a useful technique for managing commitments. It is this development of CSF's that is appealing in the research.

The aim is not to impose CSF's and a Maturity Model on organisations, but suggest through research and professional opinion what could be used to achieve improvement. It may be that the timing of any introduction of the outcome of this research may mean it is not adopted but on the other hand for some organisations that see the need (and with increasing concern regarding Cyber security and data breach legislation) this is in fact a very good time to implement the findings of this research.

To ascertain the validity of the proposed Critical Success Factors and whether they could be incorporated into a Maturity Model the use of a Delphi study was considered. The next section explores the rationale for the Delphi.

The use of a case study was initially considered but due to the results of the Delphi study set out in Chapter 5 it was instead decided to use the police service security professionals who had not been part of the original Delphi, either as they were new in post or as a result of other organisational changes to act as a control group to in the validation study (Chapter 6) as an assurance to the Delphi study outcomes.

The reason for considering the UK police service was in earlier research into the police service and incident reporting Humphrey (2004); it was identified there were concerns regarding the level of confidence in the number of incidents being reported.   Since that research the police service appears to have has improved its incident reporting capability and the central collation of incidents has enabled an improving interpretation of the figures.

5.2.1 Critical Success Factors in Security Incident Reporting

The use of Critical Success Factors in this research aims to identify what is really important to potentially improve the identification and reporting of information security incidents. An increase in empirical security incident data should enable better informed analysis and judgments for risk management decisions and tackle those the under-reporting concerns of Gordon, Loeb and Sohali, (2003), Hagen (2009) and Parker (2010). Should the reporting of security incidents increase this in turn should improve the volume of empirical incident reporting data for analysis and assessment. See figure 5-2 below.

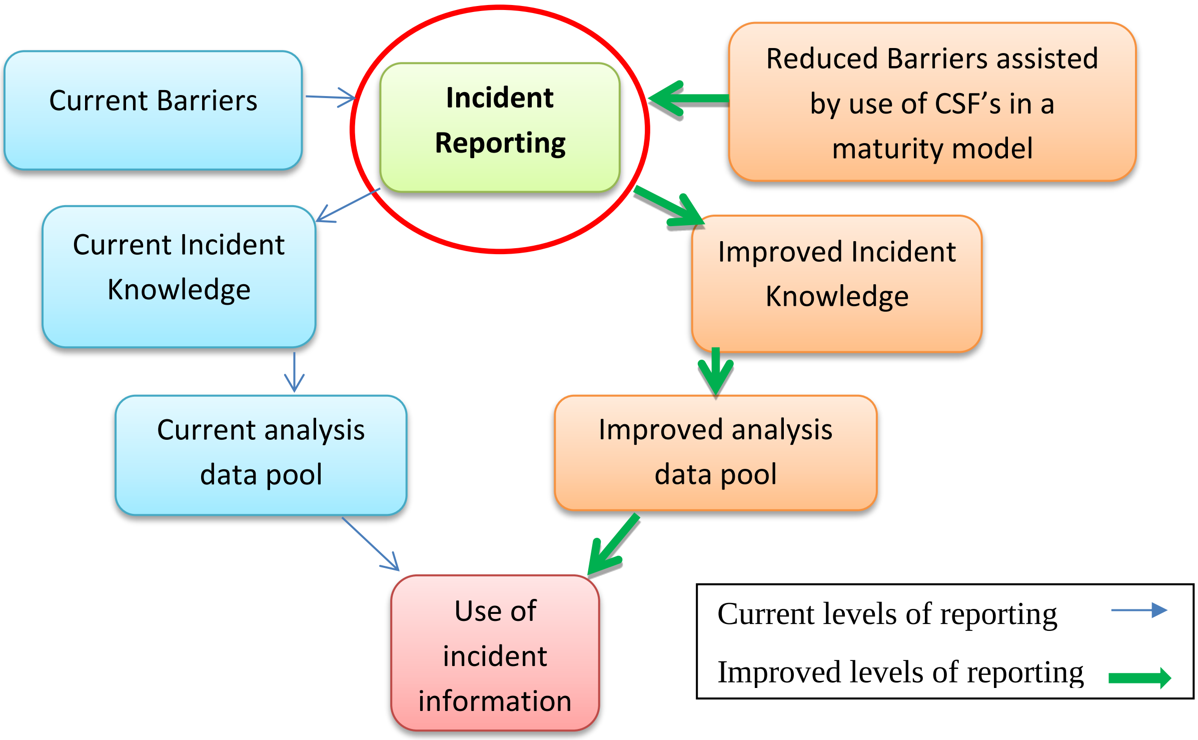
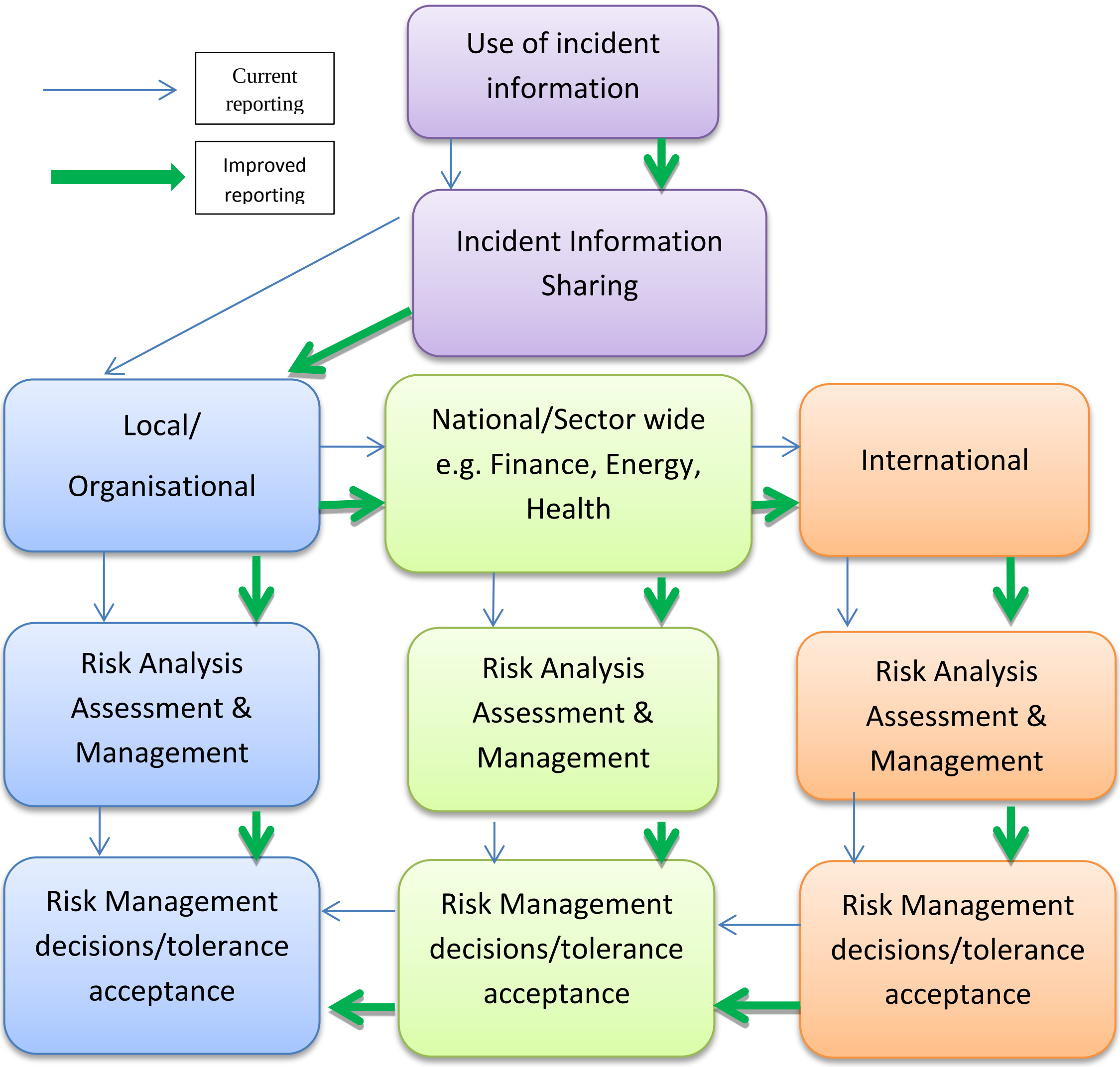

Current Barriers
Incident Reporting
Reduced Barriers assisted by use of CSF's in a maturity model
Current Incident Knowledge
Improved Incident Knowledge
Current analysis data pool
Improved analysis data pool
Use of incident information
Current levels of reporting
Improved levels of reporting

Figure 5-1 Authors Suggested Current Restricted Flow of Reported Incidents and the Potential Improvement using the CSF's and the proposed IRMM

This increase in available incident data can be shared, analysed and acted upon internally within organisations with increased confidence as it is likely to better reflect reality than previously.

Where necessary this data can be utilised further afield in relevant sectors locally, nationally and internationally as demonstrated by the below figure.



Current reporting
Improved reporting
Use of incident information
Incident Information Sharing
Local/ Organisational
National/Sector wide e.g. Finance, Energy, Health
International
Risk Analysis Assessment & Management
Risk Analysis Assessment & Management
Risk Analysis Assessment & Management
Risk Management decisions/tolerance acceptance
Risk Management decisions/tolerance acceptance
Risk Management decisions/tolerance acceptance

Figure 5-2 Authors Design of the Potential Relationship Between Local, Regional/Sector and National use of Improved Security Incident Reporting Data.

Through the identification of the potential Critical Success Factors (CSF's) required to improve security incident reporting, organisations could use these to focus on what activity was essential to improve the reporting of those security incidents. An appropriate research method to refine what elements of security incident reporting could be classed as CSF's with the aim to seek consensus from a wide community of information security professionals. Based on the report Dept of Health Report (2000) a number of identified perceived barriers to incident reporting were initially tested in the scoping study (Chapter 4). The outcome of that study gave a degree of confidence as to what were the more relevant to information security. However, it should be pointed out that the intention of the scoping study was to identify if the perceived problems relating to the reporting of security incidents did exist and whether other research into incident reporting could have the potential for reuse. As that study it was not intended at the time to test what methods could improve security incident reporting, and could be considered as CSF's, a more in depth study was needed to achieve this.

5.2.2 How were the Critical Success Factors Developed

The potential CSF's to improve security incident reporting to be included in the Delphi were developed from the literature review in Chapter 2. The main sources for these being The Dept. of Health: An Organisation with a Memory (2000, p.45) list of "characteristics of effective reporting systems" and from Barach and Small (2000) both of which had researched adverse incident reporting across health, safety and aviation. The remaining elements were based on feedback and suggestions from participants who took part in the scoping study and workshop in Chapter 4, and at information security conferences held in 2011 and 2012 where the initial findings of the research and scoping study was socialised through a number of presentations to security professionals to seek views and challenges on the assumptions regarding security incident reporting. The scoping study confirmed, through the survey of security professionals, the assumption security incidents were under reported and that there was potential to re-use research from the healthcare sector as shown from the results of the applicability of the barriers to learning. It followed that as this research on barriers to learning could be re used and, now that the scoping study had confirmed the assumption that incidents were being under reported, that same healthcare research that identified "effective incident reporting systems" could be reused to identify the Critical Success Factors.

The intention was to use the first rounds of the Delphi to identify which of the thirteen elements to improve incident reporting could be considered as CSF's. These elements would at least provide a stimulus for responses.

The thirteen elements used were:

1. Separation of collection, and analysis from any discipline or regulatory process
2. Collection of reports of ‘near misses’ as well as actual incidents
3. Rapid, useful, accessible and intelligible feedback to the reporting community
4. Ease of making a report
5. Standardised reporting systems within organisations
6. A working assumption that individuals should be thanked for reporting incidents rather than being automatically blamed for what has gone wrong
7. Mandatory reporting
8. Standardised risk assessment (to determine the impact of the incident)
9. A common understanding of what factors are important in determining risk
10. A mechanism or process for confidential reporting
11. A recognition by senior management that incidents will happen
12. Incidents reporting systems that are designed appropriately to ensure learning is possible
13. Incident analysis that considers root cause analysis and wider systems/processes and not just the initial impact assessment

The first ten were taken from Dept. for Health an Organisation with a Memory (2000, p.45) which listed “characteristics of effective reporting systems” as derived from the research into the reporting of adverse incidents. The remaining three elements were derived from the feedback and comments from the participants of the Scoping study and other presentations.

5.3 What Method is Most Appropriate for Identifying the Critical Success Factors

This section examines the potential methods that could be used to identify the Critical Success Factors as well as the reasons for discarding some of those options.

5.3.1 The Case Study

One approach that could be considered is that of a case study. A case study is a methodology that is used to “explore a single phenomenon (the Case) in a natural setting”. (Collis and Hussey, 2009, p.82). Bryman (2004) refers to case studies normally being associated with a location, such as a community or organisation and continues that often case studies are associated with qualitative research but often utilise both quantitative and qualitative research. This stance is supported by Yin (1981, p.58) who continues that their supportive evidence can take many forms “fieldwork, archival records, verbal reports observations or any combination of these”. There are risks that a case study can presume a finding in one community can be replicated in another (Bryman, 2004) however, the possible use of multiple case studies could alleviate this. The aim of this research was, if possible, to obtain consensus across a wide representation of the information security community, not just from one or a number of groups. The disadvantage of a case study is that if based on one community, although having some validity, it may not be considered as truly representative of a wider group. In particular, one of the sectors may be subject to specific regulatory controls or community security policies relating to incident reporting. This could result in any extrapolation of the findings from such singular groups not necessarily reflecting the true situation of the wider security community. However, any findings from a singular group may provide useful indicators of potential success factors that could be applied across the wider information security sector. This, in itself, would require a further study to validate such indicators. To achieve a consensus would require a greater number of case studies and as the intended participants were information security professionals a large number of organisations and companies would need to be involved to obtain a reasonable number of responses as many may only employ person who met the eligibility criteria. A case study approach was therefore discounted.

5.3.2 Focus Groups

A focus group is where the researcher acts as a facilitator to lead the discussion of a group to obtain an understanding of what individuals within the group, and the group as a whole, think about a particular subject (Buckingham and Saunders 2004; Yin, 2014). The use of focus groups is a recognised research approach however; there are also concerns that, within a focus group, social pressures can take effect, such as undue influence by some participants through their domination of responses which may affect the views of others (Collis and Hussey, 2009). There is also a view from Rowe, Wright and Bolger ((1991) that with some groups may due to the groups motives instigate premature closure of the group discussion in order to simply reaching agreement or where agreeing to the firsts solution rather than offending anyone. (1991, p. 236). In a similar vein, obtaining the views of all participants can be a challenge. Some members of a focus group may be uncomfortable in presenting their views in an open forum (Easterby-Smith, Thorpe and Lowe, 2003) and, as recognised by Bryman (2004), transcribing focus groups can be difficult but not impossible.

Focus groups can be a useful way of finding out what the main issues and concerns of any group are. The outcome of a focus group or case study can help in questionnaire design or to develop a future interview strategy (University of Bradford, 2005, p.23). It could be argued that the scoping study in Chapter 4 had already made use of the conference attendees as a focus group, particularly the presentation session at the NG Lisbon conference, where participants discussed the initial findings of the academic research. As the intention was to obtain consensus from a wide representation of the information security sector the use of a focus group was discounted.

If the use of a case study or focus group is discounted, then a different process of gaining consensus from a wider community would be required. Whatever the selected method some type of interview process to ensure consistency in the questions asked would be needed.

5.3.3 Interviews and Questionnaires

There are several types of interviews that can form a study (Bryman, 2004 and Buckingham and Saunders, 2004) and the main types are set out below;

i. Structured

These involve using a questionnaire based on previously identified and set questions which are provided to all participants (Buckingham and Saunders, 2004). They can be read out or printed.   The key element is to avoid any bias or leading of responses including intonation or emphasis in voice or tone. Being structured does not constrain the researcher from noting further comments outside of the interview boundaries. However, there are other types of interview that could be considered.

ii. Semi-Structured

These interviews have some structure and standard questions but the researcher may not include all or may add others depending on how the interview is progressing. With such interviews the interviewee “has a great deal of leeway in how to reply” (Bryman, 2004, p.321). This leads to a potential difficulty when comparing results or views against a single topic.

iii. Unstructured

This is where the interview is more likely to be unstructured or where a printed questionnaire asking broad and wide ranging questions that may not elicit a specific response to the area of research in question. The researcher could be using a set of topics as an aide memoir or even just one question and the respondent can answer freely (Bryman, 2004, p.320). These types of interviews can often be spontaneous in both question and response. These can be time consuming and difficult to record the answers (Collis and Hussey, 2009). However, this can often engage the respondent in a conversational style that may be appropriate for the type of study particularly where there is no fixed agenda (Buckingham and Saunders, 2004, p.131)

Semi structured and unstructured interviews, although challenging, are appropriate in some circumstances (Collis and Hussey, 2009). For example, where the interviewer wishes to understand the respondent's world or where the interviewee is uncomfortable about answering specific questions. The issue that will arise with any form of interviewing is the process of interpretation (Buckingham and Saunders, 2004), as the real challenge is to ensure the planning of the interviews recognises that the interpretation of a question by an interviewee can be different to the understanding of the response by the interviewer.

The general view is that other research methods such as questionnaires or interviews should be considered by those undertaking research against the practicalities, logistics and the research questions themselves. "Attention must be given to other data collection methods," (Hasson, Keeney and McKenna, 2000, p.1009).

The use of a distributed questionnaire was considered which could alleviate the discussed concerns. To identify an agreed set of CSF's a degree of validated consensus would be required. As the CSF's had not yet been identified the limits to case studies, focus groups and interviews in this research would be time consuming and labour intensive, particularly if a wide group of security professionals needs to be involved to achieve a more relevant and acceptable consensus. The scope of the subject is narrow and will rely upon participants with subject matter expertise. The use of a Delphi in this research to assist in identifying CSF's that has ultimately lead to a Maturity Model drew on the research from De Bruin, Freeze, Kulkani and Rosemann (2005) who used the Delphi to identify Maturity Models and suggest the Delphi could be used as a two-stage approach. In this case, it may be used in the first stage to achieve consensus on the CSF's required and, then be used to validate a subsequent Information Security Incident Reporting Maturity Model. Becker, Knackstedt and Poppelbub (2009) suggest the use of literature analysis to identify the assessment criteria required to formulate material for Maturity Models based on the identified success factors. They continue by suggesting the use of explorative research methods citing Delphi methods as suitable to achieve this aim. Therefore, an alternative research method, the Delphi was considered as the most appropriate method for this research.

5.4 The Delphi Study

The technique known as a Delphi originated from research conducted by the RAND group in the 1950's to identify the impact of technology on warfare. Rand (2017). The research used a group of expert opinions to obtain consensus through an iterative process (Erffmeyer, Erffmeyer and Lane, 1986). Since then the method has become popular as a research method. It is described by the originator of the Delphi, Norman Dalkey, as "a rapid and relatively efficient way to 'cream the top of the heads' of a group of knowledgeable people" (Dalkey 1969, p.16). Participants in a Delphi do not assemble, nor do they know the identity of others participating in the study. The Delphi

> "allows all group members equal participation and influence even when geographically separate" (Moga, Guo, Schopflocher and Harstall, 2012, p.5).

Dalkey (1969, p.v) states there are three features of a Delphi;

i, Anonymous response – where a questionnaire is used to obtain a groups opinion.

ii, Iteration and controlled feedback - is the examination of those responses with carefully controlled feedback to enable further iterations from the group.

iii, Statistical group response - where the opinions of every member of the group are defined as an aggregate of those responses, following the final round of iterations.

The main aims of these three elements are to minimise any bias from dominant participants, irrelevant communication and group or peer pressure.

The Delphi process works by circulating a question or issue to a selected group who in turn respond. Their views are collated and then returned, including any views of the collective group allowing each respondent to review their opinion and return the response again. This process continues until either, there is a consensus, or a point of diminishing return is reached.

> “The Delphi is only appropriate to investigate certain research problems; so careful consideration must be given to the nature of the problem before selecting this approach.” (Hasson, Keeney and McKenna 2000, p.1009).

This Delphi was not specifically looking for “generation” of ideas but “evaluation” and “extension” (Day and Bobeva, 2005, p.106) of those already put forward following earlier research identified in the literature review. In this research, the aim is to gather the views of professionals from a wide range of security related disciplines with a focus on a perceived real-world problem – security incident reporting. The intention is to improve the understanding of that particular sector which has been termed by Robson (2011, p.365), as ‘research integration’ and that the Delphi method has been used for this purpose.

If poorly undertaken a Delphi can be considered an alternative method of data collection, as opposed to consensus forming. However, it can be much more than this due to the iterative process and can provide a real understanding of the research subject (Day and Bobeva, 2005). A Delphi can also be used as a method of obtaining qualitative results. One attractive element of using a Delphi is, apart from asking for respondents to provide quantitative responses for analysis, to include a facility for comments by the respondent. This free text qualitative response from a questionnaire can be utilised to add contextual analysis. As identified by Hasson, Keeney and McKenna (2000) respondents may use this facility to qualify their selection or justify the inclusion of a new process which may result in additional quantitative responses to analyse in the subsequent iterations. In the case of this research the view of Hasson, Keeney and McKenna (2000) was considered as an important opportunity to provide the Delphi participants with a capability to suggest alternative, and not formally identified through other research, CSF’s that could be put forward. It also offers the capability to refine the wording of those potential CSF’s already identified.

Other benefits of a Delphi study include that it offers considerable anonymity between respondents though an iterative process, whilst allowing a form of conferring but without the social pressures to conform to the views as expressed by others (Skulmosky, Hartman and Krahn, 2007, p.2). The advantage of using a Delphi questionnaire is that (Goodman, 1987, cited in Hasson, Keeney and McKenna, 2000, p. 1012) the true ethical anonymity is easier to evidence. Although in a Delphi the participants can present and react to ideas unbiased by the identities and pressures of others, they do not see other participants individual responses - only the outcomes of the consensus forming. This has been referred to as "quazi-anonymity" (McKenna, 2004. Cited in Hasson, Keeney and McKenna, 2000, p. 2012).

The Delphi can seem to be a simple concept but, as Linstone and Turoff (1975) observe this can result in it being used without carefully considering the potential problems and many have failed in their aims. Linstone and Turoff (1975) offer a number of reasons for the failure of a Delphi and these include;

- " the person managing the Delphi imposing their views and over specifying its structure; assuming it is the 'surrogate' for all other communications;
- poor techniques of summarising and presenting the responses; ignoring or not disagreements resulting in some participants dropping out
- underestimating the demands that a Delphi and appreciating the time respondents put into the process." Linstone and Turoff (1975, p.6)

There are detractors of the Delphi as a research method, particularly with reference to the selection of experts. One such is Sackman (1974) in their Delphi Critique which in turn was evaluated by Rowe, Wright and Bolger (1991) where they considered many of Sackman's criticisms were based on Delphi's that had not been executed well .

Rowe, Wright and Bolger suggest four necessary characteristics a Delphi should demonstrate in order to be considered valid (Rowe, Wright and Bolger (1991, p. 237)

1. “Anonymity. Allowing group members to make their responses privately and avoid undue social pressure

2. Iteration. Presenting the questionnaire over a number of rounds allowing participants to change their opinions

3. Controlled Feedback. Informing group members of the opinions of other group members. Often provided by a summary of the group response

4. Statistical group response. Where the group’s judgement is normally expressed as a median and the spread of opinions may be used as an indication of the consensus.”

Although the researcher may identify the respondent, each respondent in turn will not know the details of others. They may assume fellow professionals may be taking part but any such individual’s details are not confirmed. The feedback is controlled through a questionnaire and the iterative stages allow for responses to develop. Finally, it offers a statistical and analytical measure of the Delphi responses received at each iteration. The iterative stages also allow the respondent to review and revise their own response, considering the information from the summarised response of the previous iteration. The below figure illustrates Rowe, Wrights and Bolger’s (1991, p.243) view that the Delphi is a two stage process where the first stage seeks to reduce any individual bias and the second stage equally weighs responses and averages them.

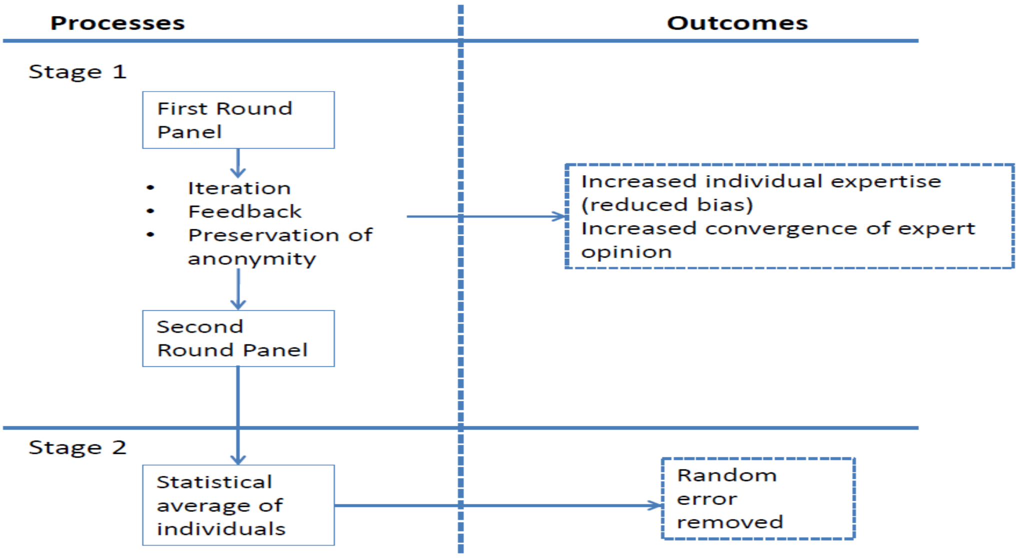

Processes
Outcomes
Stage 1
First Round Panel
• Iteration
• Feedback
• Preservation of anonymity
Second Round Panel
Increased individual expertise (reduced bias)
Increased convergence of expert opinion
Stage 2
Statistical average of individuals
Random error removed

Figure 5-3 Delphi as a Two-Stage Process (Rowe, Wright and Bolger (1991, p.243)

5.4.1 How Many Rounds are Required to Achieve Consensus?

The number of Delphi rounds required can be a challenge in that there needs to be sufficient opportunity for consensus before fatigue and lack of time or interest on behalf of the respondents is reached. Determining the design and number of iterations likely to be required used research from other Delphi studies such as Skulmoski, Hartman and Krahn (2007) who set out a model for a three round Delphi process and as does Day and Bobeva (2005). The number of rounds can also affect the response rate. An important part of the planning is to recognise when to cease the Delphi, either due to a growing obvious consensus and or a diminishing number of returns potentially indicating 'survey fatigue' as highlighted by Hasson, Keeney and McKenna (2000) and Day and Bobeva (2000).

Skulmoski, Hartman and Krahn (2007) reported in their Delphi comparison study that the number of rounds did not exceed three, indeed with some only taking one round. Rowe, Wright and Bolger (1991) report that most commonly although the number of rounds is variable they seldom go past two iterations (1991, p.237). In separate research Erffmeyer R, Erffmeyer E and Lane (1986) also sought the optimum number of rounds to a point where stability in the consensus could be reached. Their research used a group of students to reach consensus for a hypothetical problem; the NASA Moon Survival Problem. Individuals were asked to rank 15 items of equipment in terms of their importance for the survival of the crew of a crashed spaceship. In this study, it found that the group reached stability after the 4th round. The criticism that could be laid at this study was the participants were not experts and therefore it is likely to take longer to achieve consensus. The number of items (15) had to be ranked and without specific survival skills and there was likely to be a greater difference in the early rounds than if a panel of survival experts were used.

The amount of time required to the post Delphi round analysis to keep up the momentum is also a deciding factor. To some extent there is an element of being a 'hostage to fortune' as, despite diligent planning, there may be a very low, or conversely, an exceptionally high response. It is recognised that dropout rates in Delphi panels can be quite high and some studies have resulted in findings based on Delphi panels in very small numbers (Moga, Guo, Schopflocher and Harstall, 2012). This was also identified by Skulmoski, Hartman and Krahn (2007) where sample size can be affected by the number of ‘experts’ available, accepting they may be few in number, but still be representative to achieve an accepted consensus. However, Skulmoski, Hartman and Krahn (2007) urge caution in small sample size Delphi’s. Therefore, any Delphi questionnaire return dates or commitment to further rounds must factor these variables in, otherwise potentially good Delphi candidates could lose interest waiting for the second or subsequent rounds.

Skulmoski, Hartman and Krahn (2007) identified in their sample of several Delphi studies the sample sizes (panellists) varied considerably from as low as 3 to 171. Day and Bobeva (2005) refer to the largest sample size being one in Japan which involved several thousand people but most study’s (citing Gordon, 1994) involving between 15 and 35 people. These lower sample sizes need to be considered when considering whether a response rate is valid. Determining what a good response rate is can be a challenge. It was accepted that paper based surveys often returned greater responses than online ones (Nulty, 2008) although as more confidence grows in on line surveys this could change.

> “As a general rule a response rate of 30% or greater for a postal or externally sent questionnaire is generally regarded as reasonable. A goal of 50% or more responses should be attempted in any questionnaire that involved face to face interviews.” (Neville, 2005, p.33).

One potential limiting factor surrounding a Delphi is in achieving a good response rate recognising the Delphi requires continuing ‘audience participation’ potentially from a narrower field of experts than a more general questionnaire. As with any study or questionnaire the response rate can be poor. Asking respondents to persevere, not once but potentially several times, to achieve consensus can result in a dropout rate and ultimately limit the number of rounds that are likely to achieve any meaningful response. Erffmeyer, Erffmeyer and Lane (1986, p.7) suggest that whilst the Delphi has limitations these can be overcome if the Delphi is implemented “according to the guidelines of those who devised it” referring to (Dalkey, 2009) who as one of the RAND employees involved in the first use of the technique, produced a paper on how the technique could be improved following earlier use.

Having identified the Delphi as a method for finalising the CSF's and to assist in the forming of the Maturity Model the next section examines who should be invited to participate.

5.4.2 Identifying the Respondents

The respondents to a Delphi should have good knowledge of the subject matter in hand otherwise criticism that the validity of the Delphi would be levelled at the outcome. In their critique of the Delphi process, Rowe, Wright and Bolger (1991, p.240) refer to the differing views of academics on the selection of expert's to take part. As this can be time-consuming some Delphi's suffered from poor execution or sloppy execution

Therefore, it was important that any participants in this survey could be evidenced as being expert in the subject examined.

There is currently no singularly recognised information security profession or community of interest (CoI) in the UK. However, there are a number of established information security CoI's in the UK whose members could be harnessed to achieve a degree of consensus based on their knowledge and broad sector experiences. These include the Institute of Information Security Professionals and the Information Assurance Advisory Council – IAAC. There are other communities of shared I.T. infrastructures, such as the Police National Network (PNN) which is primarily a criminal justice network supporting police and criminal justice organisations and the UK HMG Government Secure Intranet (GSI) where the codes of connection (the rules to comply with for using that infrastructure) stipulate the reporting of security incidents is required. Having identified potential CoI's, approval of those responsible for such groups was sought and obtained as part of the ethical approach. This was achieved by contacting the relevant governing bodies of those groups and seeking formal approval to use their members, having outlined the research subject. It was also important to recognise that as the recipients were security professionals they are likely to be suspicious of unsolicited requests for information regarding the security of their organisation. Such professionals are also often bound by the needs to protect their organisation and therefore may be reticent to provide full and complete answers. Kotulic and Clark (2004. p.603) identified this difficulty when trying to obtain responses to security questionnaires sent to organisations and their experience was a very low response rate of 0.61%. Others such as Flores, Antonsen and Ekstedt (2014, p.100) obtained a higher response in their survey managing a 15.2% response. This was put this down to the sensitive domain of security and the unwillingness to give out information and possibly survey fatigue.

It was therefore important to ensure the respondents were informed of the fact that any professional or security body they belonged to also supported the Delphi.

5.4.3 Eligibility to Participate

Simply identifying security professionals would not enable the focus on security incident reporting. The Delphi was designed for use by experts making meaningful judgements or forecasts Rowe, Wright and Bolger (1991, p.241). Amongst those professionals the target audience for participants were those who have been directly or indirectly involved with security incident reporting. A respondent eligibility criteria was drawn up to make clear in any correspondence to potential Delphi participants this was not a general information security survey, but one focussed on a specific subject - security incident reporting. To demonstrate the responses were from those who had relevant experience or expertise the invitation to respond needed to make it clear what type of experience and expertise was being sought. Otherwise the validity of the response and the 'expertise' or 'experience' of the subject matter could be diluted to a general interest response. This too was important to counter any challenge regarding the relevance of the expertise of the participants. The below criteria were included in the invitation to participate letter (Appendix 4)

> *Eligibility criteria for completion of the questionnaire.*
>
> *Through your experience in information security many of you will meet the requirements. I am particularly looking for those of you who at some point have been involved or provided advice and guidance on one or more of the following;*
>
> *i) the reporting of, investigation or management of security incidents,*
>
> *ii) risk analysis, risk assessment and/or risk management,*
>
> *iii) any policy, regulatory or legal role that covered incident reporting*
>
> *However, even if you do not meet the above but feel you have a valuable contribution to make your involvement in this research will definitely be most welcome.*

There was a risk this may severely reduce the volume of responses, but it was important to encourage those involved in the subject matter to contribute, as opposed to those who were a member of the CoI but their experience and expertise lay elsewhere. There was still the ability to allow others who may not have met the exact criteria but felt in their role or experience they had a valuable contribution to make.

Having identified the potential participants and the eligibility criteria it is important, as with any questionnaire based research, that the Delphi can stand up to any challenge that it lacked methodological rigour. Sackman, (1975, cited by Hasson, Keeney and McKenna 2010, p.1009) suggest the planning and construction must be carefully thought through to avoid this risk. The next section describes the Delphi construction process.

5.5 The Delphi Study Approach

Having identified a number of relevant groups to distribute the study to an appropriate design of a Delphi questionnaire and accompanying instructions were set out. The provision of clear instructions is key to ensuring respondents understand what is required of them (Buckingham and Saunders, 2004). The research survey processes of best practice outlined in Chapter 4 for the Scoping study appeared to be successful, thus the same approach was planned for the Delphi, subject to the lessons learnt outlined in section 4.8.

This Delphi will focus on CoI's in the information security domain to provide participants to the survey who meet the eligibility criteria and to provide a degree of confidence in any potential respondent that the research and survey is supported by their particular CoI. As the invite to participate was sent to several communities of interest it is likely that some would know who else is participating. The critical element is to ensure any responses are kept confidential.

This aspect was catered for in the distribution of the Delphi material either by sending a common message by blind copying (bcc) respondents and where appropriate sending individually addressed messages. Once participants had responded, subsequent rounds were sent direct to individuals. Any general reminder messages were sent as 'bcc'. Should any respondent not wish it to be known to their employer they are participating, their responses could be returned by them by post as opposed to e-mail, or by a third-party proxy using a different e-mail address. The challenge being if the respondent, having completed round one of the Delphi, wished to remain completely anonymous, there is no way of knowing who to send the 'round two' iteration to without sending it to everyone, irrespective whether they responded in the first place. The option, as described in the instructions, to post the response would at least cater for any concerns of a respondent relating to the use of a company email system. In the end some respondents did return round 1 by post but all gave their full details enabling round 2 to be sent direct to them by email.

5.6 Delphi Questionnaire Construction and Design

There are three critical stages to consider in a Delphi study (Day and Bobeva, 2005) the design, implementation and evaluation. Associated with these are;

i, the Delphi approach

ii, the constitution of the Delphi panel members, and,

iii, managing responses.

In conjunction with the above stages the method by which the use of the Delphi to encourage participation is equally important. The below sections describe the approach to constructing the Delphi. Getting this right is imperative as a poorly designed and constructed survey can put respondents off (Robson, 2011). The intention is for those surveyed to understand what is being asked of them, they need to be willing to do so and provide their response to enable valid interpretation.

There is considerable guidance on survey design. Linstone and Turoff (1975, p.65) believe that the person managing the Delphi will be more productive if they see their role as "producing results, not on surveying what is already there". They also offer tips on design that range from Creating Panels, Stimulating Response, Orchestrating interaction, interpretation and summation of responses and finally communication of the results.

As in Chapter 4 the design stages suggested by Collis and Hussey (2009, p.192) were followed and again including the stage missing of representativeness.

> "Design the questions and Instructions
> Determine order of presentation

Write accompanying letter/request letter
Test questionnaire with a small sample
Choose method for distribution and return
Plan strategy for dealing with non-responses
Conduct rests for validity and reliability"

5.6.1 Design the Questions and Instructions

The list of potential CSF's contained a number of closed yes/no questions ranging from is it relevant to information security incidents, to selections ranking the importance of an element to improve incident reporting using a Likert scale. Each potential CSF question section also had the facility to provide an open response thereby enabling both quantitative and qualitative responses. The facility for free text comments against each of the identified elements allowed for a qualitative response from participants in a broader fashion (Collis and Hussey, 2009) and not just respond to the question, thereby providing added value from their personal and sector experience. In the main, those that are closed are of the tick box style and therefore quick to answer and easier to codify the response. The survey contained instructions for its completion and return, as well as an overview of the research and how the respondent could contribute.

This approach was successful in that in round one of the Delphi study 57% of those who responded provided additional comments and in round two 56% did. Even with the subsequent validation survey, reported in Chapter 6, over 80% of respondents provided comments, which was significantly above expectations.

5.6.2 Determine the Order of Presentation:

The Delphi study questionnaire was set out in two sections to ease the flow of requested information.

Section One - Identification of respondent and relevant business sector

This section was mainly used to identify information about the person completing the survey and outlined the arrangements for completion. It also provided an explanation relating to the Delphi process, the potential number of Delphi rounds and the various options for returning the responses. Emphasis was also made that respondents could 'withdraw from the survey at any time and after the completion of the survey' and importantly reiterating

> '*all responses will be treated with strict confidentiality and the final analysis and any reporting will not identify individuals or companies'*

The questions enabled, if required, sufficient information to place respondents in the public or private sector, business area and gauge the size of organisation as well as what community of interest they belonged to, recognising that many could belong to more than one of those communities. The instructions for Section 2 also included Freund's (1988, p.20) description of a Critical Success Factor to ensure consistency in interpretation.

Section Two -The potential Critical Success Factors –

Thirteen elements that could be considered as potential Critical Success Factors were identified from the literature review and scoping study research. These are listed below.

1. Separation of collection, and analysis from any discipline or regulatory process
2. Collection of reports of 'near misses' as well as actual incidents
3. Rapid, useful, accessible and intelligible feedback to the reporting community
4. Ease of making a report
5. Standardised reporting systems within organisations
6. A working assumption that individuals should be thanked for reporting incidents rather than being automatically blamed for what has gone wrong
7. Mandatory reporting
8. Standardised risk assessment (to determine the impact of the incident)
9. A common understanding of what factors are important in determining risk
10. A mechanism or process for confidential reporting
11. A recognition by senior management that incidents will happen
12. Incident reporting systems that are designed appropriately to ensure learning is possible
13. Incident analysis that considers root causes and wider systems/processes and not just the initial impact assessment

As these elements were formed outside of the Delphi group, rather than just accept these are the only potential Critical Success Factors, the identification of any other potential elements considered by participants as relevant to the information security sector, was needed. The Delphi round one questionnaire provided a facility for the respondents to suggest any other elements they believe should be considered.

> *You can add any factor that you think has not been considered and feel worthy of inclusion. It may be included in the next round for your fellow professionals to consider.’*

These may be incorporated in subsequent iterations if sufficient support for a new element was evidenced from those taking part.

In the Delphi first round respondents were asked to provide answers against each of the elements shown above. (Table 5-2) below shows the questions section of the survey.

Element Description	**Is it relevant to information security incidents**	**Is this a possible Critical Success Factor**	**Rank the importance of the element to improve incident reporting by selecting or circling as appropriate one of the below numbers as applicable to the key below;**	**Comments (if any)**
(each of the thirteen elements were described individually here.) *E.g.* Ease of making a report	Select as appropriate or Circle the Yes or No	Select as appropriate or Circle the Yes or No	1. Highly important 2. Important 3. Neither Important/unimportant 4. Unimportant 5. Highly unimportant	

Table 5-2 Extract Example of the Delphi Round 1 Questionnaire

The purpose of the first question *‘Is it [the element] relevant to information security incidents*’ is key because if a significant number of respondents answered no, it immediately rules the element out from being considered a Critical Success Factor.

The second question ‘Is *this a possible Critical Success Factor’* is an obvious one that requires the respondent to make an initial decision as to their views on this point. Having been provided with Freund’s (1988) description of a CSF, the aim was to start focussing the respondent’s opinion on this point.

The third and final question was intended to assist in the ranking of those elements identified as possible CSF's then drill down into the respondent's views as to how important the element is to incident reporting. The intention being to separate out those elements not considered as relevant. This allowed for focus on those identified as possible CSF's and analyse their Likert ranking.

At the end of each potential CSF set of questions was a space for free text comments. These text boxes were optional to complete but do provide an insight into the rationale for the choice of answer. The additional benefit being these comments allowed for an analysis of the original wording of the elements based on the observations of respondents as part of the process to achieving consensus. This analysis led to a rewording of the main element descriptions and the addition of further descriptors to these elements. This supported the view by Hasson, Keeney and McKenna (2000, p.1000) that the outcome from the initial survey may produce qualitative information that can be turned into a quantitative form for the second round. To allow for comments may only draw a limited response as with regards to self-completed questionnaires "most people do not like writing" Buckingham and Saunders (2004, p.71). Allowing for comments also mitigates against the criticism of Delphi's that the validity can be weakened by not allowing participants to discuss the issues raised as suggested by Hasson, Keeney and McKenna (2000, p.1013). They continue that a Delphi consensus does not necessarily mean the right answer has been found, but the results may be useful in identifying issues for further debate.

5.6.3 Write Accompanying Letter/Request Letter

The introductory letter and support from any sponsor to encourage participation is equally important to get right. It must not show any bias towards any of the elements and needs to be clear on who is eligible to take part. The explanatory invitation to participate letter headed 'Information Security Incidents Reporting Delphi Study December 2015'(Appendix 4) was sent out to the various CoI's which set out the purpose, eligibility criteria and the way confidentiality was being approached. It also included further options for those wishing a higher degree of anonymity, returning by post for example.

The letter contains an explanation of the nature of the Delphi and its purpose. Complete anonymity can be difficult in a Delphi as the identity of the respondent should be known by the researcher to ensure they receive subsequent stage iterations to enable further responses.

The intention of the letter was to accompany the actual questionnaire, setting out a brief background and experience of the researcher, the subject, and the rational for the research. The letter explained why they had been sent the questionnaire and that the research was supported by their relevant CoI to provide assurance to the potential participant that the researcher was genuine and had relevancy to their profession. This was felt important as many questionnaires are often sent out in an unsolicited manner and by gaining approval of the relevant CoI body it may encourage the respondents to participate if they met the criteria. As many security professionals do not just belong to one community of interest and therefore could receive the questionnaire via more than one of them, there was a real risk this could be both annoying and be considered as a type of 'spam'. This was anticipated as the letter included in the second paragraph an advanced apology.

> '*It may be you have also received this through other CoI's that you belong to and, if this is the case, may I apologise if it appears that you are being spammed. One response would be really appreciated'.*

This was indeed the case and to some extent helped to further publicise the support of a number of CoI's and potentially further encourage completion. The letter also explained the eligibility criteria and questionnaire format. It also pointed out that the respondent could add any unlisted elements they felt should be considered.

An expectation of the demands of the time of the potential respondents was included. Testing had indicated it would take approximately 15 minutes to complete. These timings were based on experience of the volunteers whilst it was being tested. Finally, explaining the Delphi process and the intention to seek consensus and again time management that normally such studies do not go further than three rounds. It was felt important that as the respondents may wonder how much time their participation would involve and that the subsequent rounds were likely to take less time to complete.

A definition of a security incident to be used for the purposes of this research was included. This definition was included as one of the outcomes of the scoping study in Chapter 4 clearly demonstrated that no commonly agreed definition of a security incident was used by the respondents to that study. To avoid any misunderstanding of what was meant by a security incident a definition to be used for this survey was included.

This definition was developed in the absence of a universally accepted security incident definition and its development is described in more detail in Chapter 2.

> *An information security incident is either, an actual or potential event that has, or is likely to, cause harm to the confidentiality, integrity and/or availability of data, assets, systems or infrastructure whether caused by people, processes or technology.*

Recognising that not all professionals belong to a CoI there was always the potential for some respondents to forward on the introductory letter and questionnaire to those they felt may also be eligible. The introductory letter included this point by stating after the eligibility criteria

> '*If you know of someone else who is equally eligible, but may not have received this, please forward them a copy of this letter and questionnaire.'*

This in fact appeared to take place as some other CoI's and individuals did respond as a direct result of the request being sent out. These included members of the Europol Security Committee who then passed the Delphi out to relevant EU government organisations. In the UK the questionnaire was subsequently re distributed by the UK National Technical authority, the UK MOD the Government DSO forum and other groups who upon seeing it forwarded to others in the Information Security Profession. It should be noted that this snowball approach means that it is not possible to calculate the response rate to the survey.

5.6.4 Test the Questionnaire with a Small Sample

It is considered good practice to test a survey prior to its distribution (Bryman, 2004; Buckingham and Saunders, 2004). The draft survey form was reviewed, refined and then tested to ascertain any issues with its design, flow and clarity. Hasson, Keeney and

McKenna (2000) and Collis, Hussey (2009) consider it is best practice that a small scoping should be conducted to test for these possible issues.

These drafts, as well as the instructions and introductory letter, were initially tested on a small group of volunteers who met the eligibility criteria. Attention was paid to the language, logical flow and any potential misunderstanding of words or phrasing that could affect the response. Draft versions were also sent to university colleagues for comments. Having made amendments identified from the initial testing, a different group of users tested the questionnaire as if they were completing it for real. They were requested to test the documents from work, home and other machines. The main intention was not only to test the content but also to test Microsoft word and pdf version compatibility. As it was likely a number of different operating systems and software versions would be used, combined with individual and corporate sets ups and defaults for common office products, this variety of set ups could cause issues if not identified at an early stage. For example, some corporate email defences may strip out macro commands and the survey did incorporate the opportunity to use drop down lists. This aspect was catered for in the design that if drop downs did not work the question and selections for answers were still visible in the text. This testing did identify a couple of minor errors in the drop downs. However, a decision to still include drop downs was based on comments from testers relating to the ease of completion offered using drop-down selections. Testing also identified issues such as wordiness of the letter and questions. This resulted in a reduction in the size of the survey form, greater clarity in the instructions and identified ambiguities reworded. Following a final set of testing using a mixture of other eligible volunteers, including some from academia, the final questionnaire was ready.

The formulation of the questionnaire and letter took considerable time in wording and testing. The fact that it was completed by a worldwide audience, without any questions regarding its completion does demonstrate the importance of testing. The number of human errors in the completion of responses was low. These errors included missing out some answers. These errors were factored into the analysis of responses for each section to ensure the appropriate statistical validity was obtained.

5.6.5 Choose Method for Distribution and Return

It is important to identify a method for distribution, decide upon a time to respond, any cut-off date for non-responses including managing the expectations of participants when the next round(s) will be distributed. The survey was emailed to the CoI's that had agreed their support. A form of words to base their research support message to the membership was included as it was felt it would assist the process and ensure key consistent messaging was maintained. Some organisations simply mailed out to their membership, others posted it as a link to their website to download. The survey was designed to be completed either as a word document, a pdf form or printed and completed by hand and then scanned and e-mailed back or even posted if required.

5.6.6 Plan Strategy for Dealing with Non-Responses

At the outset, it was decided to personally respond to every completed response by thanking the sender, although this was not made clear in the introductory letter. This later proved beneficial where anyone who had responded and returned a completed survey, but not received an acknowledgement would know their answers had not been received. This made a subsequent chase up group 'bcc' message easier by stating that had a respondent replied but their response blocked at any of the mail gateways then they would not have received a thank you message. If they had not received a thank you please contact the researcher.

5.6.7 Conduct Tests for Validity and Reliability and Representativeness

As outlined in the scoping study in Chapter 4 where McNeill (1992) introduces his concept of three key areas regarding research; reliability, validity and 'representativeness'. This was considered as part of the Delphi process as well.

Reliability. By ensuring the process and method of collecting evidence is reliable any future use of this method should result in similar findings. (McNeill, 1992, p.14).

The only difference regarding future surveys obtaining similar findings is if the context in which the survey was re-issued had changed. For example, any changes that had occurred at their place of work regarding reporting processes because of regulatory change. In general the facts should be the same, but some of the perceptions of the person filling the survey may have changed slightly. It very much depends on the time difference between when the first survey was sent out and if it were to be re- issued.

Validity: This relates to being confident the data collective reflects reality and is a true picture of what is being studied. (McNeill, 1992, p.15)

There is an accepted risk of misinterpretation of a question. Undertaking trial runs with different people before deploying the survey reduced the likelihood of this occurring to a low level. The fact that a Delphi was used, which returns the findings to respondents for reconsideration to obtain consensus, adds to the validity of the process as any unusual interpretation may be further challenged by respondents. The fact that the Delphi was supported by the various CoI's and that the responses were from numerous sectors and country from the public sector, private sector and some academia, as well as being iterative and obtained consensus demonstrates it can be considered to reflect reality. This also assists in evidencing the sample representativeness of the Delphi respondents which is discussed further below.

Representativeness: Using the views already set out for representativeness in Chapter 4 and reiterating that McNeill (1992, p.15) suggests it is important to ensure the sample population that are being studied are a true reflection of others in that group and Buckingham and Saunders (2004, p.70) also refer to the importance of the "people you interview need to be representative of the wider population from which they have been sampled.

The range of participants that made up the Delphi respondents gives confidence that the selected group or the subject matter is typical of others. Surveying information security professionals from a number of recognised CoI's adds weight to the sample representativeness. Whilst recognising as stated earlier, no singular representative group as yet exists, by using bodies such as the Institute of Information Security Professionals to assist in identifying the participants and that other CoI's provided their support coupled with an eligibility criteria to ensure those who were completing the Delphi had knowledge and experience of incident reporting and the use to which such information could be put when assessing information security risk were involved. The participants were from a wide mix of public and private sector organisations and academia from the UK and worldwide.

5.7 Summary of Approach to the Delphi Study

The Delphi process was designed to follow identified best practice. It was conducted through a number of stages which are summarised below.

- A review of literature on Delphi study's to understand both the potential benefits and concerns of this study method and to design out where possible any potential challenges to the process.
- Making use of the general approach and lessons learnt from previously conducted questionnaires where the need to ensure respondents were content with the confidentiality arrangements.
- Testing of the initial Delphi construction through;
  - Use of academics and volunteers for ambiguities and errors
  - Dry runs to test the survey for any further errors
  - Inclusion in the testing the identification of potential issues due to multiple methods of submission. In particular, the potential adverse effects of differing versions of Microsoft and adobe software as well as printing on potential participant's systems. Also factored in were the possible security controls at corporate mail gateways that may affect any macros used for drop-down menus in the questionnaires.
  - The viability and instructions for alternative methods of return such as printing hand completion and scanning and returning of responses.
- Ensuring clear, unambiguous, concise communication separate to the questionnaire
- Canvassing the level of support and interest for the subject matter and Delphi approach from appropriate relevant professional bodies and Communities of Interest.
- Obtaining formal approval from these groups to use their membership as a form of distribution.
- Identifying points of contact to distribute the questionnaire
- Thank each respondent individually so they know their questionnaire has been received.
- Keep interest high through updates to professional bodies.

- Send appropriate messages to all respondents giving update on progress without appearing to apply pressure to respond.

The introductory letter, Email text sent to CoI's, and final version of the round one survey are shown as appendices 4, 5 and 6 respectively.

5.8 The Delphi Questionnaire - Results of Round One.

The Delphi round 1 was launched at the beginning of December 2015 and was distributed through a number of recognised CoI's during December 2015 and January 2016. Responses were then received during the months following. This section provides the results and analysis of the Delphi questionnaire responses. The first consideration is whether the return rate is sufficient to be valid and that the level of representation from respondents reflects the wider information security community. Section 1 of the questionnaire asked respondents for details that assisted in the demographics for example to identify the sector they worked in (public, private or Academia) and the size of their organisation.

Overall the range of representation was encouraging. A total of 115 responses were received from the UK, Europe and further afield including Australia, India, America and South Korea. Against the findings of Skulmoski, Hartman and Krahn (2007) referred to earlier in the chapter where they reviewed Delphi's that had numbers of respondents ranging from 3 to 171, this was a favourable response. The types of organisations represented by the respondents included law enforcement, central government, local government, finance, energy, retail, health, telecommunications, military, managed service providers, pharmaceutical, service industry, food, academia and others.

5.8.1 Breakdown of Responses to Round One of the Delphi

Public Sector	Private Sector	Academia
59%	37%	4%

Table 5-3 Overall Response by Sector

The distribution of public and private sector was 59% public sector 37% private sector with a smaller amount, 4% from academia. This lower level of academic response was expected as less academics are likely to be involved in the management of security incidents but clearly some, based on the eligibility criteria, felt they had valuable contributions to make .

5.8.2 Breakdown of Response by Size of Organisation

Number of employees	0-500	501-1000	1001-5000	5001-10000	10000+	Self employed
All groups	15%	6%	25%	14%	37%	3%

Table 5-4 Response by Size of Organisation

Each employee size group is represented in the returns. 15% of the responses came from security professionals employed by organisations employing less than 500 staff, 25% from those employing between 1000 and 5000 and interestingly a larger percentage of respondents, 37%, who worked in major companies or organisations of over 10,000 employees. This range of size of organisations is a good indication of the validity of the response. Self-employed professionals represented 4% of the total received.

Number of employees	0-500	501-1000	1001-5000	5001-10000	10000+	Self employed
Public Sector	0%	1%	43%	21%	35%	1%
Private Sector	35%	0%	5%	5%	54%	1%

Table 5-5 Response by size of organisation by sector

The breakdown of size of organisations between the largest two groups, the public and private sector shows the public sector had no representation from the smallest size and only 1% from the next size up. Their responses were more representative of the medium to large employee groups with 45% from 1001-5000 21% from 5001-1000 and 35% in the 10000 plus range. In contrast the private sector were more representative of the smallest and largest employee groups with the largest representation, just over half, from the biggest employee base (10,000+), and just over a third from the smallest employee group (0-500). The size of organisation groupings were set out originally to give an overview of the responses by size of company. If regrouped as small, 0 to 1000, medium 1001 to 10000 and large being over 10000 this shows the response from the public sector mainly representing medium and large organisations and the private sector representing as small and large organisations. This could possibly reflecting a tendency for public sector organisations are not normally found to be small in number and private sector organisations do have many small companies. With such a wide range of responses from different sectors and countries this was not possible to confirm with official statistics on organisational size.

A considerable number who responded did indicate which the community of interest body they had been made aware of the survey by. Although in some cases the respondent indicated more than one body, which vindicated earlier planning to apologise for potential spamming and the belief that some professionals belong to more than one security body. The biggest response group was the Institute of Information Security Professionals (IISP) which accounted for just fewer than 50% of the responses. This also provided a degree of validity relating to the professionalism of respondents as these members must demonstrate information security competencies in the information security sector to be eligible to be members.

5.8.3 Section Two of Round One of the Delphi

This section was aimed at the views of professional on the 13 elements identified from previous research. Respondents were asked to answer against a list of processes considered to be effective for the overall reporting process of reporting incidents. Against each process they could state ‘yes’ or ‘no’ if they believed it is relevant to information security incident reporting. Then the same again whether they believe the process could be considered a Critical Success Factor (CSF). They were informed a process can be very important but not necessarily a Critical Success Factor. The Delphi questionnaire set out that CSF’s have been described as:

> “Important to achieving overall corporate goals and objectives,
>
> Measurable and controllable by the organisation to which they apply,
>
> Relatively few in number – not everything can be critical,
>
> Expressed as things that must be done not the end point of the process,
>
> Applicable to all companies in the industry with similar objectives and strategies and hierarchical in nature.” (Freund, Y, 1988, p.20)

Although different groups had slightly differing scores, overall the consensus on what was a Critical Success Factor was very similar. It may be that differing bodies will consider some types of element more relevant than others in their sector. For the purposes of the next round of the Delphi the overall consensus was used. Therefore, there is a degree of confidence that the overall response is representative of a wide information security community.

	Is it relevant to security incidents?		**Is this a possible CSF?**	
	Yes	No	Yes	No
1. Separation of collection, and analysis from any discipline or regulatory process	87%	13%	58%	42%
2.Collection of reports of 'near misses' as well as actual incidents	97%	3%	61%	39%
3.Rapid, useful, accessible and intelligible feedback to the reporting community	96%	4%	73%	33%
4. Ease of making a report	98%	2%	71%	29%
5. Standardised reporting systems within organisations	94%	6%	58%	42%
6. Working assumption that individuals should be thanked for reporting incidents rather than being automatically blamed for what has gone wrong	95%	5%	58%	42%
7. Mandatory reporting	88%	12%	64%	36%
8. Standardised risk assessment (to determine the impact of the incident)	90%	10%	63%	37%
9. A common understanding of what factors are important in determining risk	89%	11%	60%	40%
10. A mechanism or process for confidential reporting	89%	11%	61%	39%
11. A recognition by senior management that incidents will happen	90%	10%	67%	33%
12. Incident reporting systems that are designed appropriately to ensure learning is possible	93%	7%	61%	39%
13. Incident analysis that considers root causes and wider systems/processes and not just the initial impact assessment	99%	1%	82%	18%

Table 5-6 Response to Questionnaire by Element Relevance and is it a CSF?

The above responses are the results of the questions to each of the listed elements.

Is the element relevant to information security incidents?

The responses clearly show the respondents feel that the elements identified in research elsewhere are relevant to the information security sector. This reinforces the findings from the scoping study that research elsewhere into incident reporting has the potential to be reused in the information security sector. The lowest score agreeing the element is relevant being 87% and the highest 99%.

The next question is important. Is the element a possible Critical Success Factor?

Here the responses were more discerning with the lowest score as a possible CSF being 58% for three of the elements and the highest element scoring 82%.

These scores produced quantitative data that required further breakdown to enable a judgement to be made in the consensus forming process. The questionnaire then asked respondents to rank the importance of the elements to improve incident reporting based on a five point ‘Likert’ Scale ranging from 1 Highly important to 5 Highly unimportant. The facility for respondents to add comments after each answered element was also provided.

These figures show that many of the elements are considered important and that to identify which ones may be potential critical success factors would require examining a combination of the two quantitative yes/no questions and the Likert responses together with analysis of the comments that were provided.

On initial examination of the question to ‘rank the importance of the element to improve security incident reporting’ elements 11 and 13 had over 50% scores at the highest ranking. Others, although popular also had higher mid-range to negative scores. For example element 10 scored relatively well , 7 and 8 had relatively high scores but the mid-range and negative scores showed that consensus might not be as easy to achieve.

Rank the importance of the element to improve security incident reporting	Highly Important	Important	Neither important/ unimportant	Unimportant	Highly unimportant
1. Separation of collection, and analysis from any discipline or regulatory process	27%	46%	15%	11%	1%
2.Collection of reports of ‘near misses’ as well as actual incidents	32%	54%	11%	3%	0%
3.Rapid, useful, accessible and intelligible feedback to the reporting community	40%	46%	11%	3%	0%
4. Ease of making a report	46%	43%	11%	0%	0%
5. Standardised reporting systems within organisations	32%	47%	14%	6%	1%
6. A working assumption that individuals should be thanked for reporting incidents rather than being automatically blamed for what has gone wrong.	35%	47%	17%	1%	0%
7. Mandatory reporting	45%	32%	14%	9%	0%
8. Standardised risk assessment (to determine the impact of the incident)	43%	35%	16%	6%	0%
9. A common understanding of what factors are important in determining risk	25%	50%	15%	7%	2%
10. A mechanism or process for confidential reporting	35%	41%	19%	4%	1%
11. A recognition by senior management that incidents will happen	51%	33%	7%	7%	2%
12. Incident reporting systems that are designed appropriately to ensure learning is possible	29%	52%	15%	3%	1%
13. Incident analysis that considers root causes and wider systems/processes and not just the initial impact assessment	58%	36%	1%	0%	0%

Table 5-7 Importance of Element in Reporting Incidents using a Likert Scale

A number of the comments were received suggested some combination or changes to the initial wording of the potential CSF's to make them more relevant to security. This could make it easier to better judge their potential as a CSF going into round two. Others comments suggested changes to a potential CSF's wording that incorporated parts of the less popular elements.

5.9 How the Potential CSF's were Selected for Round Two

Having collated scores relating to the elements relevance, it potential for becoming a possible Critical Success Factor and its importance in improving security incident reporting, the next stage was to identify which of the elements could go forward to the Delphi round two as potential CSF's. As stated earlier, Fruend's, (1988, p.20) view is CSF's they should be "relatively few in number – not everything can be critical,"

Firstly, by identifying if any of the original 13 elements were not considered as relevant to security. In the first round of the Delphi all scored highly enough to be considered as relevant. The highest scoring element was number 13 'Incident analysis that considers root causes and wider systems/processes and not just the initial impact assessment' with 99% and the lowest element 1 'separation of collection and analysis from any disciplinary or regulatory process, with a score of 87%.

Then by examining the Yes/No question is the element a possible CSF. As stated earlier three of the elements (4, 12 and 13) scored well in the 'highly important' Likert scale. The next choice 'Important' Likert scale scores were taken into consideration. Some scored highly overall when the 'Highly important' and 'important scores were taken together.

As can be seen in Table 5-7 a number of the elements consistently score the highest although their position varies slightly, therefore the differences in each column would need to have some other review to ensure the most popular were consistent.

As the aim was to focus on the CSF's and improve security incident reporting this resulted in some weightings being applied to the importance of the element to improve security incident reporting. . The yes no CSF score was used as it stood. However the next question which asked for a Likert scale scoring was had weightings applied to the Highly Important and Important scores as Highly Importance was considered a higher value than important but simply taking each score from the Likert range did not differentiate this importance. This process was validated within the academic supervision of this research.

As it was judged using a Likert scale, the highest importance received a weighting of 2 then the importance answer a lower weighting of 1.5. A combination of scores of the potential of the element being a CSF and the importance to improve security incident reporting showed 7 elements scoring over 200% once the weighting had been applied. The top 4 elements were then selected as the potential CSF's and three elements that scored less than the top four but were clear of the remaining elements were included as possible CSF's.

Element number	**Critical Success Factor Yes**	**Highly Important**	**Highly Important score weighted x2**	**Important**	**Important score weighted x1.5**	**Total of CSF Yes score and weighted Highly Important and Important scores**
1	58	27	54	46	69	**181**
2	61	32	64	54	81	**206**
3	73	40	80	46	69	**222**
4	71	46	92	43	64.5	**227.5**
5	58	32	64	47	70.5	**192.5**
6	58	35	70	47	70.5	**198.5**
7	64	45	90	32	48	**202**
8	63	43	86	35	52.5	**201.5**
9	60	25	50	50	75	**185**
10	61	35	70	41	61.5	**192.5**
11	67	51	102	33	49.5	**218.5**
12	61	29	58	52	78	**197**
13	82	58	116	36	54	**252**

🟧	Highest Scoring elements considered as potential CSF's
🟦	Middle scoring elements that may be Possible CSFs

Note: All figures are percentages

Table 5-8 Summary Chart of how most popular elements that could be CSF's were identified

Examination of the comments provided suggestions as to the wording of each of the higher scoring elements in preparation for round 2. For example, 'near misses' was a popular answer in some responses but others felt they should not be separated out from normal incidents. Therefore reference to near misses was included in the amended description of element 4 ‘ease of making a report’ to reflect the relative popularity of near misses into an already high scoring element. The near miss element which was scored as a possible element was also amended to reflect the comments made.

Some examples of comments from respondents to the ‘near miss’ element were

> *“The more data the easier it is to identify a pattern”*
>
> *“If anything this should be considered as more important that actual incidents. This is the opportunity to take action to avoid future incidents and real damage”*
>
> *It is vital to collect this information as it could help prevent any potential future major incident occurring”*

There were some comments that were not as supportive

> *“important but not a CSF as not vital. How do you capture this information and can you justify the effort”*
>
> *“Near misses are difficult to determine. They go unnoticed by the outside. It needs tremendous trust to report them, as there will be consequences”*

For the element ‘ease of making a report’ when finally issued in round 2 the wording had changed from

> ***Ease of making a report***

to

> ***2a. Amended wording:***
>
> ***Ease of making a report, recognising if incident reporting is difficult individuals will be less likely to submit them. This may particularly affect the reporting of near misses. The reporting process should:***

- *Include a sufficiently clear level of education and awareness to all staff in how the reporting process works.*
- *Describes what an incident is.*
- *Describes how to report it and what escalation needs to take place.*
- *Sets out levels of expected feedback.*
- *Be clearly set out as part of any governance process.*

This re wording had taken into account comments from round one participants to improve on the bland initial element to a more focussed one *"the system must be user friendly"*

"*if it's not easy to make a report then will discourage from making future reports*"

"This is extremely important, if it isn't easy for users to report incidents and events then they will probably not be bothered to do so"

"the most important factor is knowing who to communicate with and how"

"It is important to make reporting straightforward and simple"

The inclusion of the education and governance wording came from some of the suggestions for other CSF's.

"Education and awareness re incident reporting"

"clarity of reporting systems (who do I tell)

"Reporting lines"

"Staff Awareness re reporting"

"Establishment of governance"

The next section explains the manner in which some aspects of the suggested additional CSF's were incorporated.

5.10 Other Suggested CSF's

To ensure the respondents did have an opportunity to put forward a different view on the elements identified through research elsewhere, they could make suggestions for other potential elements to be considered. The response to this was encouraging. Of the 67 public sector respondents 34 (51%) made a total of 45 suggestions, of the 43 private sector 10 (23%) made a total of 18 suggestions. The space for these suggestions was set out in such a way those respondents could also score them against the same criteria as the 13 listed ones. This enabled a similar ability to identify those that may be considered as Critical Success Factors. These were collated and compared with those that already existed as well as looking to identify if any suggested element had sufficient support that it could be included in round 2 of the Delphi. The list of these suggestions is shown at Appendix 9.

It became apparent that the majority that were suggested were very similar to those already set out and this, as well as other comments made by respondents, was one of the reasons for adding additional descriptions to the initial wording of the most popular elements before sending them out in round 2. The additional elements suggested were in effect sub descriptions that gave more clarity to the original elements meaning. Of the suggestions ‘education’ and ‘governance’ regularly featured in some form or another. As a result no new elements were introduced but the original wording of the most supported elements was amended to take into account of the comments made.

Again using the example of developing the element relating to ‘Ease of making a report’; the Delphi round 2 included the original CSF wording, then showed an amended wording to take into account some of the comments and the suggestions for possible other elements. Education was weaved into this element as a result. An example is set out below;

Original wording (Element 4)

Ease of making a report

Amended wording:

Ease of making a report, recognising if incident reporting is difficult individuals will be less likely to submit them. This may particularly affect the reporting of near misses. The reporting process should:

- Include a sufficiently clear level of *education and awareness* to all staff in how the reporting process works.
- Describes what an incident is.
- Describes how to report it and what escalation needs to take place.
- Sets out levels of expected feedback.
- Be clearly set out as part of any *governance* process.

The above amendment included elements of the suggestions including ‘education’ and ‘governance’.

The next section describes the process of the 2nd Round of the Delphi and how the four most popular elements plus the three that were supported as possible CSF’s were amended to reflect the suggestions and comments into more rounded elements for the 2nd round participants to consider.

In fact all of the elements included in round 2 included the original wording together with a suggested re wording based on the comments received in round one.

5.11 Delphi Round Two

Having identified the top 4 scoring elements and the next three possible CSF's the task was to engage the participants in round 2 of the Delphi. The methodology of the survey design and testing for round 2 followed the approach for round 1. As there were identifiable respondents this time the round 2 survey was directed at only those who had responded to round one on a more personal basis. The main difference being the survey questions design.

As there was now a potential 115 respondents in the Delphi panel it and their responses to round 1 had been numbered, it was easier to send and track the responses to round 2.

The Round 2 Delphi was divided into three sections
Section 1 was primarily instructions to the participants and they were informed they could withdraw at any time.

Section 2 explained the emerging consensus around the top 4 elements. It continued by stating

> *"The CSF descriptions have been added to, based on the responses and comments provided in round one. This section asks your views on whether you feel the additional description affects the element as a Critical Success Factor.*
> *There are again five choices available for you to indicate your preference. This time the options ask your opinion whether the amended wording of the element either; significantly improves its value as a CSF, improves its value as a CSF, neither improves or reduces its value as a CSF, reduces its value as a CSF and finally significantly reduces its value as a CSF. In addition, please indicate whether this amended element remains a CSF - Yes or No? There is also space for any comments you may wish to make."*

Section Three informed the participants about those elements that did not score the highest but could be considered as CSF's as a result of the amendment to the wording based on comments made in round one.

> *Section 3 set out the three elements that due to their positioning in the scoring could still be considered as a CSF. This section contains those elements that scored well, but not as well as the above four elements, but were scored higher than the rest. As in Section 2, the descriptions have been added to, based on the responses and comments provided in round one. This section asks your views on whether or not you feel the additional description affects the element and improves it to such an extent that it can be considered eligible to be included as a Critical Success Factor amongst the four already identified in Section 2. There are three of them (again not in any order of preference).*
>
> Element 2. Collection of reports of near misses as well as actual incidents
>
> Element 7. Mandatory Reporting
>
> Element 8. Standardised risk assessment (to determine the impact of the incident)
>
> *Again, there are five choices available for you to indicate your preference. The options are that the amended wording either; significantly improves the element such that it should now be included as a Critical Success Factor with the four CSF elements above, improves the element such that it should now be included as a Critical Success Factor with the four CSF elements above, neither improves or diminishes the element such that it should remain where it is, it diminishes the element such that it should not be included as a Critical Success Factor with the four CSF elements above and finally it significantly diminishes the element such that it should not be included as a Critical Success Factor with the four CSF elements above. There is also space for any comments you may wish to make.*

The 2nd Round Delphi was made up of a 5 point Likert and a yes no question that was slightly different in wording for the top 4 elements to the next three 'possibles' to reflect the opportunity for participants now that the elements wording had been amended to reflect the various comments made.

In essence the top 4 Likert scale was asking

How do you feel the amendments impact on the value of the element as a Critical Success Factor**?**

1. Significantly improves the value of the element as a Critical Success Factor
2. Improves the value of the element as a Critical Success Factor
3. Neither improves or reduces the value of the element as a Critical Success Factor
4. Reduces the value of the element as a Critical Success Factor
5. Significantly reduces the value of the element as a Critical Success Factor

Finally they were asked to confirm or not whether they felt as a result of the changes did the element remain a CSF.

In view of the above, does this element remain a Critical Success Factor? YES or NO

With regards to the three possible elements the question was different where it was asking for the participant to reconsider the positioning of them as a potential CSF. The instructions being

The below elements scored well, but not as well as the above four elements but were scored higher than the rest. Further descriptions of the element have been added as a result of comments made by respondents in Round One. The original element number is shown in brackets. Please place your view against each of the three elements that the emerging consensus scored well, but not as well as the above four elements in Section 2 by selecting or circling, as appropriate, one of the five numbered choices.

Do you feel the amendments impact on the value of the element and its potential to join the four Critical Success Factors in Section 2

1. Significantly improves the element such that it should now be included as a Critical Success Factor.
2. Improves the element such that it should now be included as a Critical Success Factor.
3. Neither improves or diminishes the element and that it should remain where it is.
4. Diminishes the element such that it should not be included as a Critical Success Factor.

5. Significantly diminishes the element such that it should not be included as a Critical Success Factor.

Again there was a 5 level Likert selection. See table 5-8 for the full wording and results.

To reduce the burden on respondents and lessen the completion time, instead of requesting their details again, each was allocated a reference number used collating their round 1 response. The round 2 Delphi questionnaires were then numbered accordingly so each respondent received their allocated numbered questionnaire. To overcome the potential issues which were in part experienced in round 1 each respondent was sent two emails, one with a word version of the round 2 and the other with a pdf version.

The Delphi round 2 was sent out by email at the end of April 2016. It was sent to the original 115. Initially found some respondents had left the organisation they belonged to for round one. This was identified by out of office messages that were returned; none had forwarding addresses. This reduced possible number of respondents to round 2 to 111.

A Subsequent e mail was sent out thanking those who had responded stating that those who had would have received confirmation and if others had sent a response but not received a response to make contact as it was possible their response had been blocked. This achieved an additional burst of activity and likely acted as a prompt to those who had not done so to now complete it.

Some responses were unclear and due to the reference number approach the respondents were able to be contacted by email for clarification. The reason appeared mainly due to some boxes responses being stripped out as they were macros.

After assessing the results there appeared to be a consensus on the elements considered to be Critical Success Factors. The results indicated no significant changes or disagreements in respondent's views. There were still some suggestions re minor re wording of the descriptions of the CSF's. There was some support for promoting one or possibly 2 elements as CSFs but this needed to be balanced against. Whilst an element may be important it does not necessarily make it a CSF (Freund, 1988). In the end 82 respondents completed round 2 giving a 74% return. The below table sets out the summary of responses to the elements identified as Critical success Factors from round one.

Do you feel the amendments impact on the value of the element as a Critical Success Factor?	**1. Original wording (Element 3)** ***Rapid, useful, accessible and intelligible feedback to the reporting community***		**2. Original wording (Element 4)** ***Ease of making a report***		**3. Original wording (Element 11)** ***A recognition by senior management that incidents will happen.***		**4. Original wording (Element 13)** ***Incident analysis that considers root causes and wider systems/ processes, not just the initial impact assessment.***	
1. Significantly improves the value of the element as a CSF	27		33		52		30	
2. Improves the value of the element as a CSF	61		45		37		44	
3. Neither improves or reduces the value of the element as a CSF	6		13		10		20	
4. Reduces the value of the element as a CSF	5		9		1		6	
5. Significantly reduces the value of the element as a CSF	0		0		0		0	
In view of the above, does this element remain a CSF?	Yes	No	Yes	No	Yes	No	Yes	No
	100	0	98	2	95	5	95	0

Table 5-9 Do Amendments to Wording Improve the Highest Scoring CSF?

Looking at the results for each element in turn.

Element 3 *Rapid, useful, accessible and intelligible feedback to the reporting community*

The results appear to indicate that the amended wording has improved the view of the respondents with 88% stating it either significantly improves or improves the value of the element as a CSF. When asked is it still a CSF there 100% support for it. This indicated the amendments had made a difference and there was solid support that it remained a CSF.

Element 4 Ease *of making a report*

This too appears to show the amended wording has improved the view of respondents. 78% thought the wording significantly or improved the wording and there was a 95% score that it is still a CSF. Although there was some dissention regarding it remaining a CSF the overall score of 95% showed convincing support

Element 11 *A recognition by senior management that incidents will happen.*

Again the results appear to show the amended wording has improved the view of respondents. 89% thought the wording significantly or improved the wording and there was a 95% score that it is still a CSF. This element had the highest score for an improvement of the CSF wording and like element 4 had a 95% support for it to remain a CSF.

Element 13 *Incident analysis that considers root causes and wider systems/ processes, not just the initial impact assessment.*

Likewise to the other results shows an indication of an improvement in the wording.77% thought the wording significantly or improved the wording and there was a 95% score that it is still a CSF. In a similar vein to element 4 and 11 an improvement in wording.

Overall none of the elements had a score that the wording significantly reduced its value as a CSF. The highest score of a reduction in the value was 9% for element 4.

In summary it appears that the amendments to the original wording were well received and that the top four elements are still considered to be CSF's. This clearly indicates a consensus from the Delphi participants.

5.12 Section 3 Possible Critical Success Factors.

The next section focusses on those elements that did not score highly enough in round one to be considered as a Critical Success Factor but still had scored sufficient to be included in round 2 as a possible CSF following amendments to the wording. The rewording that had taken place following the comments made in round one may have been sufficient to change the respondent's views. Therefore in round 2 the participants were also asked to consider three possible elements that could be elevated as Critical Success Factors and if support for one or more of the top three diminished significantly could replace one or more of them.

These were;

Element 2. Collection of reports of near misses as well as actual incidents
Element 7. Mandatory Reporting

Element 8. Standardised risk assessment (to determine the impact of the incident)

Many of the comments that were received were supportive of the element and the revised wording but opinion whether it they should now be considered as CSF was divided.

The below table provides the results for the three possible CSF's

Do you feel the amendments impact on the value of the element and its potential to join the four CSFs in Section 2?	**Original wording (Element 2)** ***Collection of reports of near misses as well as actual incidents***	**Original wording (Element 7)** ***Mandatory Reporting***	**Original wording (Element 8)** ***Standardised risk assessment (to determine the impact of the incident)***
1. Significantly improves the element such that it should now be included as a CSF.	16	29	16
2. Improves the element such that it should now be included as a CSF.	46	44	28
3. Neither improves or diminishes the element and that it should remain where it is.	35	20	50
4. Diminishes the element such that it should not be included as a CSF.	2	7	5
5. Significantly diminishes the element such that it should not be included as a CSF.	0	0	1

Table 5-10 Do Amendment's Improve the Possible CSF Elements?

Element 2. Collection of reports of near misses as well as actual incidents

The scores for this element showed a 16% support that the wording had significantly improved that it should now be considered as a CSF. However, 35% of the scoring was that it neither improved or diminished the element and should stay where it is and not be a CSF. A useful element but not a CSF. There was little concern that the wording had diminished the element

Element 7. *Mandatory Reporting*

This potential CSF had a higher level of scoring in support of it being considered as a CSF. 29% feeling it significantly improved the element. There were supportive comments but the areas of concern related to what is mandated to be reported and whether internally or externally. Some linked the wording to ease of making a report rather than making reporting mandatory.

Comments such as

> "*mandatory reporting can give a negative perception – how can it be enforced' "[Referring to ease of making a report] 'it appears duplicative to raise the issue again here'. 'I struggle whether this is a CSF. An organisation should have a culture of reporting'.*

On balance although there was greater support for it to be considered there was sufficient concern from respondents that it was not considered as strong enough to become a CSF.

Element 8. *Standardised risk assessment (to determine the impact of the incident)*
This element had the highest score (50%) that it should remain where it is. Although like other possible elements there was support for it to be considered.

5.13 Review of Additional Comments Provided in the Delphi 2 Response.

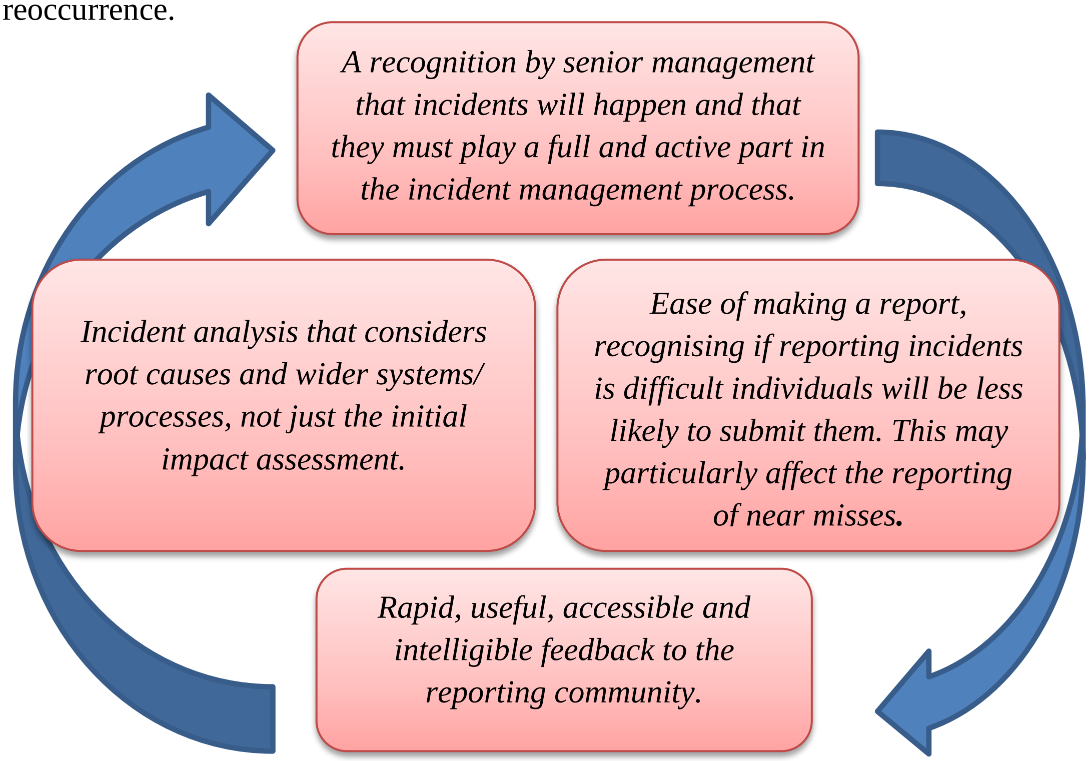
There were many positive comments regarding an improvement of their description but also some criticism. As the respondents came from a wide range of sectors and sizes of organisations and some were overseas respondents, it may be difficult to achieve 100% agreement as to the to exact wording but the Delphi 2 outcome gives a high degree of confidence in the wording that was sent out.

The approach taken was to only amend further where there is common agreement. In essence recognising, although it appears that the Delphi 2 had reached acceptable consensus, there was still room for further minor tidying up of the wording in preparation for the Incident Reporting Maturity Model validation study.

5.14 Summary

In summary the four identified CSF's were still considered to be so by clear high scoring. Of the possible CSF's, Mandated reporting, scored the best. However, in view of the comments and the fact that clarity as to what should be mandated to report and it is difficult to measure if incidents were reported of not, meant it was not considered as a CSF. To be included in a Maturity Model it would also be harder to judge as an organisation would either have mandated reporting or not and the maturity would be on the confident that incident were being reported against that mandating. In addition organisations may be subject to external regulatory or policy reporting requirements. With the soon to be introduced General Data Protection Regulation (Regulation (EU) 2016/679) which relates to personal data incidents as opposed to other types of incidents this could make the 'mandation of reporting' if it were a CSF more complex.

The findings show a group of four CSF's that could run in a natural sequence. Starting from a recognition that incidents will occur to then having a process that makes it easy to report incidents, then provide feedback to reporters (to encourage future reporting) and finally making use of the reports to understand the root causes to prevent or reduce reoccurrence.


A recognition by senior management that incidents will happen and that they must play a full and active part in the incident management process.

Ease of making a report, recognising if reporting incidents is difficult individuals will be less likely to submit them. This may particularly affect the reporting of near misses.

Rapid, useful, accessible and intelligible feedback to the reporting community.

Incident analysis that considers root causes and wider systems/ processes, not just the initial impact assessment.

Figure 5-4 The Four CSF's in a Cyclical Process

Chapter 6 sets out the Validation study to test the original findings of the Delphi and introduce an Incident Reporting Maturity Model.

Chapter 6 Validation of the Delphi Study Findings. The Creation and Testing of an Information Security Incident Reporting Maturity Model

6.1 Introduction

Chapter 5 set out the four main Critical Success Factors identified through a Delphi study that have the potential to improve information security incident reporting. Once the CSF's had been identified, the next stage was to conduct a validation study which aimed to;

i) Provide an opportunity to that the final CSF selection findings from the Delphi study did not cause any concern from the Delphi participants. This may identify any significant differences of interpretation which could call into question the researchers interpretation.

ii) Test the potential of an Incident Reporting Maturity Model (IRMM) as a tool in which to place the four CSF's and to see if it can be used to evaluate an organisations maturity level against those CSF's.

iii) To further test the IRMM and CSFs a control group, who had not previously participated in the formation of the CSF's but met the eligibility criteria, was identified.

The purpose of the use of a control group as well as the original Delphi participants was to enable a comparison of their scoring against that of the Delphi participants to identify if there are any significant differences between the two. This has two benefits. Firstly to test whether the identified CSF's wording is understandable as the control group had not previously been exposed to their development. Secondly, to identify any significant differences of opinion that would warrant further investigation or research.

This Chapter aims to validate the findings from the Delphi and proposes a method to communicate them to the information security community using an Incident Reporting Maturity Model. This is in support research goals three and four which, for convenience, are reproduced below.

> (3) To identify the Critical Success Factors that may be applicable to information security incident reporting.

(4) To propose an information security Incident Reporting Maturity Model that could be applied by organisations and may improve the flow of incidents that are reported.

Research goal 3 was primarily dealt with in Chapter 5 but the validation study would also provide assurances particularly with the involvement of the control group. The main goal that the validation study is seeking to address is no 4.

Having identified the four CSF’s through the Delphi study there needed to be a method to make practical use of the research in a real world environment rather than simply providing a list of them. To assist in the uptake of the use of these CSF’s a method that would enable businesses and organisations to evaluate where they were positioned in relation to these CSF’s was considered a more practical and beneficial approach. The four identified Critical Success Factors could be placed within an Incident Reporting Maturity Model (IRMM). This could be used as a tool that could potentially assist in the identification of the level of maturity an organisation has in relation to these CSF’s and whether or not there is an appetite to take them further. However, although the Delphi study had been conducted and a consensus reached, it would be diligent to conduct a form of validation against the final wording of the CSF’s and to test the Delphi findings with a selection of security professionals who, although eligible to take part in the Delphi study, did not. The validation study therefore gave the opportunity of the original Delphi participants for any further comments on the CSF wording as well as testing whether the CSF’s could be placed in a IRMM to enable organisation to judge their level of maturity against those factors. In addition it introduced a control group who were not exposed to the previous stages of research to judge how well the CSF’s and the IRMM would be accepted by those not being involved in their development.

6.2 Validation

With any research there is always a concern that, despite rigour in design and approach, doubts could exist regarding the accuracy of the data analysis and interpretations of the findings. There is a risk the researcher may have been “‘fooled’ as to be mistaken about them” (Robson, 2011, p.85). There is considerable debate amongst researchers over what constitutes validity. Scheurich (1997) in his criticism of interpretations of what is meant by validity argues that when differing research views describe varying types of validity they often are dealing with the same problem. As previously discussed in Chapters 4 and 5 the issues of Validity, Reliability and Representativeness are important to demonstrate the rigour of the research and assurances the findings are based on reality. This research is based on a pragmatic approach recognising that both positivist and interpretative methods and approaches have been adopted. The mix of types of quantitative and qualitative questions in the surveys is a good example. The table offered by Easterby-Smith Thorpe and Lowe (2003) who instead of the terms validity, reliability and representativeness refer to the term generalizability. This generalization test is partly undertaken by the validation study. The author has added comments in italics to reflect how this study addresses the challenges asked in the table. For example under generalization the research did not intend to validate the research findings in the healthcare sector and elsewhere regarding incident reporting but to test whether they could be reused.

	Positivist	Relativist	Constructionist
Validity	Do the measures correspond closely to reality**?(**_**as far as possible based on following best practice and use of security professionals)**_	Have sufficient number of perspectives been included*?* ***(in terms of the range of professionals taking part in the studies it is believed so)***	Does the study clearly gain access to the experiences of those in the research setting**?** ***(Yes, based on the professionals responding)***
Reliability	Will the measures yield the same results on other **occasions (**_**There will be variables as organisations and views may change over time. The control group and validation study helped to assure reliability)**_	Will similar observations be reached by other observers ***(Yes, but there is the risk regarding interpretation of comments However, those interpretations of the CSF wording changes were included in subsequent Delphi rounds and validation so some of this concern can be dismissed)***	Is there transparency in how sense was made from the raw data ***(The Delphi process gives an opportunity to challenge the authors interpretations if there was concern. The raw data is in the appendices)***

Generalizability *(others such as McNeill (1992); Buckingham and Saunders(2004) refer to representativeness*)	To what extent does the study confirm or contradict existing findings in the same field **(*There does not appear to have been any similar research in the information security sector but confirmation research in other disciplines can be reused***	What is the probability that patterns observed in the sample will be repeated in the general population ***(if referring to the security community this is likely based on the similarity of findings between the Delphi participants and Control group but if referring to the public it would not be applicable)***	Do the concepts and constructs derived from this study have any relevance to other settings? **(*Yes, as shown reuse into information security. The findings have the potential to be re-used back into the original research findings from healthcare)***

Table 6-1 Perspectives on Validity, Reliability and Generalizability (with Author's added context in italics) Easterby-Smith Thorpe and Lowe (2003, P.53)

Others such as Yin (2014, p.45) refer to four tests of the quality of research designs 'Construct validity, internal validity, external validity and reliability'. Yin (2014) refers to construct validity as an issue where researchers make subjective judgements whereby their pre-conceived views can influence the data gathering and, in the case of a survey, its construction. Internal validity does not apply always to studies but the element where Yin (2014) suggests it does is where inferences from the collective data are made. External validity relates to how far the results can be considered a true representation of a wider group which links into the views of Easterby-Smith Thorpe and Lowe (2003) in table 6-1 above. Finally Yin (2014) refers to reliability, if another researcher followed the same path would the same results be obtained. Buckingham and Saunders (2004, p.296) also refer to a number of types of validity; face validity, content validity, construct validity and external validity. Despite considerable rigour in the approach to the Delphi study; the ability to question or challenge the findings arguing the construct was biased or that the external validity was not met still exists.

To demonstrate reliability in that should the Delphi be rerun and analysed by a different researcher the quantitative answers of the Delphi study rounds should result with the same percentage scores against the relevant elements to increase reporting (assuming respondents answer the same as they did before). Internal validity or inference is harder to validate. The quantitative answers provide clear views but a combination of qualitative free text comments provided by the respondents, when used to clarify their answer or place a different view or suggestion, could result in some variation of their interpretation by a different researcher. Validation is important to ensure the findings of research can be considered as sound or accurately reflect the phenomena under study (Collis and Hussey, 2009, p.64). Scheurich (1997, p.81) describes validation as separating research than can be considered acceptable from that which is not. Yin (2014) advocates that following recognised research procedures is important in preventing threats to validity. The use of the Delphi process in its self is a partial guard against the risk of researcher inference as the participants may well voice views on a researcher's interpretation during the iterative stages. The use of a validation survey will try to alleviate these concerns, particularly by making use of a control group where the group's answers can be compared with those who have already been involved in the Delphi study.

To add to the validation a control group, made up of professionals who were considered as meeting the original criteria to be part of the Delphi study, but have not as yet been involved, were also sent the IRMM. This was intended to achieve the three aims set out in 6.1.

The outcome of the IRMM and comparison of findings should provide the assurances that the original interpretation of the researcher met the challenge of Easterby-Smith Thorpe and Lowe (2003, P.53) as set out in their table (Table 6-1).

6.3 What is a Maturity Model?

A Maturity Model is a method used to judge or gauge an organisations level of maturity against particular criteria. In this research that being the reporting of incidents. The level of maturity is set against a scale. Maturity "combines notions of evolution with levels of process formality." (Fraser, Moultrie and Gregory, 2002, p.248). They continue by suggesting that to avoid complexity "they propose a definition of maturity that encompasses effectiveness and repeatability" (2002, p.248)

6.4 Why a Maturity Model?

Can a Maturity Model make a valid contribution to the incident reporting problem. Referring to the conceptual framework, the perceived gap was the need for more information on reported incidents. Having identified the CSF's that have the potential to increase the reporting of security incidents how would an organisation judge its current position, identify the gaps and move towards improvement.

It has been suggested that "companies demonstrate behaviors (sic) that reflect their maturity levels" Dinsmore (1998, p.24 cited by Jugdev and Thomas 2002, p.6). Jugdev and Thomas (2002, p.6) also argue that Maturity Models do have their critics in that they can be inflexible, are typically geared towards identifying, but not solving, problems and do not consider the rapid pace of change. A Maturity Model will contain a scaled of a number of levels of maturity. The typical 5 levels of maturity do not offer sufficient granularity, they can be impractical and focus on process rather than the resources required. Having surfaced these concerns Jugdev and Thomas (2002) do recognise the benefits of Maturity Models that raise awareness of issues. It is this raising of awareness that could be a prime benefit and the understanding of what could improve reporting and where an organisation is placed relative to the identified factors against the Maturity Model levels is an attractive proposition.

To assist organisations in understanding how far they are progressing towards attainment of a goal, the notion of measuring an organisations maturity have become more popular. This popularity has spawned many different models; in 2005 a study by De Bruin (2005) identified over a hundred different models. Not only are they large in number but also in style. Fraser, Moultrie and Gregory (2002) provided a table setting out a sample range eighteen Maturity Models and their differing numbers of levels and approach. Although large in number and of differing approaches they also have degrees of commonality with varying levels of granularity. For example, they all describe a number of maturity levels, descriptors (although they can differ or vary in name) and descriptions of activities against each level. One potential reason for the large number is the problem definition and approach can vary according to the industry or sector and Becker, Knackstedt and PoppelBub (2009) suggest the continuing development of Maturity Models can often result in model owners reviewing their own to compare its suitability and potentially providing incentives to consider change.

Due to the large variation of model types, no one model appeared to be used more than another. Jugdev and Thomas (2002, p.6) suggest that the Maturity Model field is relatively young and that no model has achieved worldwide acceptance. In this research the proposed use and area being researched was compared against a synopsis of designs laid out by Becker, Knackstedt and Poppelbub (2009, p.217). Their structure for a business process Maturity Model includes the iterative procedure, evaluation and methodological approach used in this research. Becker, Knackstedt and PoppelBub (2009) also make the valid point that consideration should be given to whether there is in fact a need for a Maturity Model in the first place.

In the UK, to measure or benchmark government departments and agencies standing relating to information security, an Information Assurance Maturity Model was first introduced in 2008 and formed part of the UK Information Assurance Maturity Model and Assessment Framework (Great Britain, CESG, 2015) as one measure to monitor the recommendations following the 2008 UK Government Data Handling Review (Great Britain, Cabinet Office, 2008). The purpose being to support the drive to embed information risk management processes within organisations. This was aimed at providing greater levels of assurance when departments and agencies wished to share information with the knowledge there are comparable and, to some extent, consistent approaches being adopted. This Information Assurance Maturity Model was introduced to enable individual government organisations to assess at what stage of maturity they sit and this was subject to external audit. Thereby providing a process that would potentially allow for benchmarking across like-minded groups, as well as provide a minimum level of maturity to aspire to. Over time this can be raised as the lowest common denominator of maturity is reached by all and then the bar can be raised, if it is deemed important to do so. The use of Maturity Models for information security and cyber security are not new, other work such as research by the US Department for Homeland Security in its Electricity Subsector Cyber Security Capability Maturity Model (ES-C2M2) (2014, p.15) which has a different number of levels - 0 to 3, where 0 means that even the initial practices at 1 have not been achieved.

The IRMM could have the potential to not only be used to assess the internal maturity of an organisation regarding incident reporting but also for the IRMM to support information sharing. It could be used to assess the maturity of third party organisations. Having confidence that, if something went wrong within the organisation that data was being shared with, it would be reported could provide additional assurance. This potential additional use of a Maturity Model supports the view of Becker, Knackstedt and PoppelBub (2009) that there is a need for a Maturity Model in the first place. To examine its potential use to be extended to external third party verification of incident reporting maturity the following question was included in the Validation survey questionnaire.

Q. "If other organisations used the same model would this assist when determining the ability of that organisation to handle incidents? (for example, if exchanging data with them or contracting them as a third-party supplier)"

The responses that it was valuable or extremely valuable from the viewpoint of the original Delphi respondents was 80% and even higher at 92% from the control group.

Whilst Maturity Models may not suit all organisations, they are a recognised approach to consider as they can identify any gaps between where an organisation is against where it would like to be. However, many models do not make it clear how to achieve the closing of the gap (Mettler and Rohner, 2009). None the less the main purpose of a Maturity Model is to identify a gap that can be closed after following improvement actions (Fraser, Moultrie and Gregory, 2002,). However they continue by stating it is recognised, that the "'knowing -doing- gap' can be very difficult to close." (Fraser, Moultrie and Gregory, 2002, p.248) This is despite organisations knowing what needs to be achieved.

6.5 Levels of Maturity

Within most Maturity Models there is a common approach to depict maturity against stages of levels. There are variations on the titles but in the main they are broadly similar. Five levels of maturity are common, although they can range from three to six (Mettler and Rohner, 2009) with the highest level being a notional ideal. Other Maturity Models such as that posed by De Bruin and, Rosemann (2005) use a five-level scale, as shown in the table below.

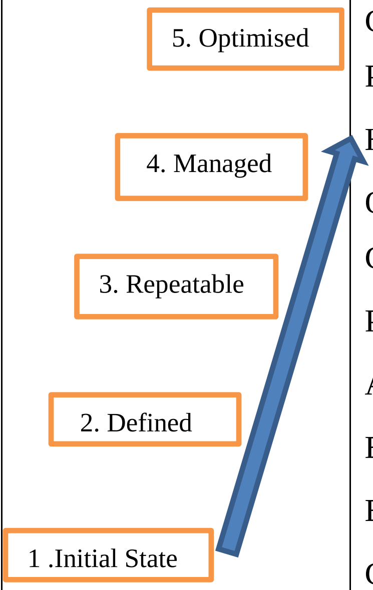
Low Maturity		**High Maturity**
Un-coordinated, isolated projects Low BPM skill Key Personnel Reactive Manual (Meaningful) Internally Focused Low Resourcing Naive Static	 5. Optimised 4. Managed 3. Repeatable 2. Defined 1 .Initial State	Co-ordinated Business Process Mapping Activities High BPM Expertise Organisational Wide Coverage Proactive Automation Extended Organisation Efficient Resourcing Comprehensive Understanding Innovative

Table 6-2 Levels of Maturity Taken from De Bruin and Rosemann (2005, p.4)

6.6 Is a Maturity Model Suitable for all?

Suitability relating to the desired outcome should be considered. Several Maturity Models have a linear approach - a progression through from a low standpoint to final maturity (Shackleton, Fisher and Dawson, 2004). However, this may stifle improvement or at least not recognise it fully. It may well be the organisation going through the maturity process has more maturity in some areas as opposed to others and improvement is not simply linear or iterative but more in line with the standpoint of Shackleton, Fisher and Dawson (2004) that other approaches other than linear should be considered. They refer to research by Quirk (2000) who identifies spaces for improvement rather than a simple linear approach. Such an approach of a non-iterative model could fit the IRMM incident reporting maturity levels. One organisation may have a good security culture but a poorly implemented reporting system. It is the reporting system that holds them back whereas another organisation may have a good reporting system, but a poor security and safety culture. If the levels of maturity placed such items as culture or reporting systems on a linear path this may be misleading in demonstrating where the improvements in both the Critical Success Factors for the organisation and the ultimate measurement of maturity lay.

6.7 Maturity Models - A Good or Bad Approach?

There is always a danger that once a system is introduced the maintenance and checking of its validity and continuing use can be forgotten and the model is then left to exist on its own. It is inevitable that any process introduced will need re-evaluation against the original requirements. With this in mind Becker, Knackstedt and PoppelBub (2009) suggest that Maturity Models need to be regularly evaluated.

The term Maturity implies that a function or process is understood and commonplace in its application in the workplace. The key goal is to ensure that once this is achieved it is sustainable and the actual need for the model has declined or disappeared. (Fraser, Moultrie and Gregory, 2002, p. 248). Refer to this as sustainability In other words, the activities required to achieve the highest levels of maturity are now institutionalised.

Some of the criticisms aimed at Maturity Models are well documented. As already referred to the view of Jugdev and Thomas (2002) that Maturity Models do not solve the real issues and they do not consider the pace of change and they focus on process not people. Skulmoski (2001) suggests that as the area of Maturity Models is relatively young there is a lack of empirical evidence on what models competencies support success. Despite this, it is claimed by Jugdev and Thomas (2002) that Maturity Models have contributed to identifying the competencies required to bring about success in the area of focus applied. Fraser, Moultrie and Gregory (2002, p.244) describe the potential comparison between a maturity level descriptions and the use of "'Likert' scales questionnaires with anchor phrases," to which to place a decision against. The notion being there is the high and low end of a maturity level and the same with a Likert scale which are viewed as very good to the low end as very poor. The respondent to such Likert scale questionnaires is simply to place their score against the one they feel appropriate without further guidance whereas with Maturity Models there is more of an evaluation of the positioning against the level There is also a risk that maturity level grids or matrices, which describe the level activity as often trading the resolution in brief terms as opposed to a deeper description of what is required. Fraser, Moultrie and Gregory (2002, p.244) who suggest it is a challenge to ensure the maturity grid is fit for purpose and that compromise is often required to ensure the aim of the Maturity Model is realised in the "interests of producing a useful and usable tool"

Fraser, Moultrie and Gregory (2002) propose there could be a pairing of Maturity Models. In what they describe as management maturity and process maturity grids. For this research that could translate into an incident reporting matrix that dealt with improving the reporting of incidents and a process grid that then handled the levels of maturity for making use of them.

The initial management stage diagram proposed by Fraser, Moultrie and Gregory (2002, p.244) has been reproduced below. The italicised text reflects suggested replacement words that relate to incident reporting to show how it could be relevant in this research. The first matrix is the management maturity element.

Stage V Certainty	We know why we do not have a problem with quality *(incident reporting*)
Stage IV Wisdom	Defect prevention (*incident reporting*) is a routine part of our operation
Stage III Enlightenment	Through management commitment and quality improvement *(improvement in incident reporting)* we are identifying and resolving our problems
Stage II Awakening	Is it absolutely necessary to always have problems with quality (*incident reporting*)
Stage I Uncertainty	We don't know why we have problems with quality *(incident reporting*)

Table 6-3 Maturity Model Matrix Adapted from Fraser, Moultrie and Gregory (2002, p.244)

The proposed IRMM is primarily based at the management maturity element, as this needs to be tested as part of the validity study. At this stage of the research the IRMM is based on a reasonable assumption of the 5 levels of maturity, rather than being more prescriptive as to the process to bring about change. This could be a candidate for further research should an organisation decide to adopt the IRMM.

One of the challenges to Maturity Models is they only differentiate between maturity and immaturity, albeit at various levels and the term immature, although not explicitly used in such models can have a detrimental effect. Andersen and Henriksen (2006) propose that there should be more emphasis on activities that are focussed on the 'customer'. In the case of security incident reporting there could be a number of 'customers'; the organisation itself; various teams; like-minded organisations or parts of wider groups affected by the data produced. If this approach were to be taken, as opposed to the traditional linear or iterative Maturity Model, would it make any difference for this research.

The conceptual framework from Chapter 1 answers this to some extent by including the outcomes of improved reporting which would be to the benefit of all the customers involved. Never the less to achieve outcomes it is easy to argue some basic activity and level of maturity will be required. As there is 'no one size fits all' Maturity Model then the test of the model to be used should be to examine if there are opportunities for its improvement.

This research has considered the some of those 'customers' (the Information Security Professionals) by asking them in the first place, as part of the Delphi study, to identify what are the Critical Success Factors required to improve security incident reporting. The challenge is to turn the consensus for the CSF's into a meaningful and useable Maturity Model. The fact that the CSF's have been identified through a research study should add to the value in including them in the Maturity Model. Fraser, Moultrie and Gregory (2002) argue that it is this challenge of identifying success factors makes it difficult to ensure the Maturity Model approach. Some models are experienced based (Fraser, Moultrie and Gregory 2002, p.248) whereas the proposed Maturity Model in this research is based on research that has identified the success factors.

The model this research intends to develop is one where not all elements of a particular stage of maturity need to be completed before activity at the next level can commence. Stages often indirectly lead to the belief that one stage higher is better than the lower stage, however often activity in each of the iterative stages can and will occur. Anderson and Henriksen (2006, p.239) argue that

> "the triggers for moving to one stage rather than to another stage are more rewarding to focus on rather than observing whether government is at stage I or IV",

where they refer to digitalisation of e government and in their four-stage model moving from publishing intention stage I to delivery phase IV.

The question of whether a Maturity Model is the right approach was considered in this research and in the IRMM survey there were specific questions to test whether respondents had used them before, had any views on their use as well as how relevant they could be to this research. If none of the respondents had either used or disliked Maturity Models it could have influenced the outcomes of their responses or they probably would not have opted to complete the survey at all. The survey respondents possibly do not represent that view. It transpired that the research identified that most respondents had used Maturity Models previously (70% of the Delphi respondents and a lower number 62%, but still majority, of the control group). There were equivalent responses regarding the usefulness of Maturity Models as tools to assess a particular situation (88% against 69%). Therefore it could be considered that the respondents answers were not going to be unduly affected by their lack of or poor experience in the of Maturity Models.

6.8 The Incident Reporting Maturity Model – IRMM

The IRMM construct was based on the methodology and outcome of the two rounds of the Delphi study outlined in Chapters 4 and 5 and the design stages suggested by Collis and Hussey (2009, p.192) were followed and again including the missing stage of representativeness.

- “Design the questions and Instructions
- Determine order of presentation
- Write accompanying letter/request letter
- Test questionnaire with a small sample
- Choose method for distribution and return
- Plan strategy for dealing with non-responses
- Conduct rests for validity and reliability”

The intention in this validation stage is to provide a vehicle for the four identified Critical Success Factors to be part of an Incident Reporting Maturity Model that organisation could potentially use to bring about and improvement in the number of incidents being reported.

6.8.1 Design the Questions and Instructions

The four CSF’s identified as a result of the Delphi were placed in a proposed IRMM. The intention being to understand the participants views on its potential use as a tool that organisations can use to adopt the four CSF’s.

6.8.2 Determine the Order of Presentation

The IRMM contained instructions, the four identified CSF's set in a proposed Maturity Model format. See Appendix 14 which is the Delphi group version and Appendix 15 which is the Control group version. This took up the first five pages and the following pages contained the questionnaire which again like the other surveys contained a mix of quantitive and qualitative questions.

The survey included the wording of the four identified Critical Success Factors which had been further refined based on the comments from participants from round 2 of the Delphi study. The validation survey would also seek to identify if any further suggested wording changes came from either the original Delphi participants and importantly from any of the control group who would not have seen this wording before.

The purpose of the validation was not only to present the final version of the CSF wording but also request the Delphi participant's views on whether the use of an IRMM would be of benefit to their organisation. The questions also sought to understand the use of Maturity Models within their organisations as it was possible that any responses may be influenced by previous experiences and usage of such models.

The intention was to use a 5 point Likert scale against each of the 4 CSFs. The first asking

"Based on the Critical Success Factor and the level description how easy was it for you to interpret the maturity position of your/another organisation?

The intention being that by looking at the description of the CSF would its description make it easy to understand or deduce what is meant by the CSF in relation to their organisation? This was aimed more at the wording of the CSF to see if then the level of maturity against it can be judged.

The second question

Based on the Critical Success Factor and the level description how easy would it be to use to judge your or another organisations position in the Maturity Model?

The second question is asking if the wording enabled respondents to interpret the CSF and how easy is it to rank or evaluate their organisations position. The difference between the two questions being the understanding of the wording of the CSF and, having understood it, how easy an exercise to judge the organisations position.

This was followed by general questions on Maturity Models to gauge the participants experience of them and possible any bias towards or against them from that experience. The reason for this was if the respondent did not feel Maturity Models were of use this may have had a negative impact on the IRMM survey response.

> Q. Do you use Maturity Models in your organisation or one for which you have reviewed or assessed. The choices were yes or no
>
> Q. Do you personally feel Maturity Models are useful tools to assist an organisation understand where they sit regarding to a particular situation. The choices were yes no or no strong view
>
> Q. Some Maturity Models set out a larger number of elements to measure against. Is just listing the critical elements a better approach. The choices were yes no or no strong view

The final contained specific questions on the IRMM.

> Q. Overall would you consider this Maturity Model to be of value to your organisation to assess how security incident reporting is handled and managed against the identified Critical Success Factors. The choice was a Likert scale of 5
>
> Q. If other organisations used the same model would this assist when determining the ability of that organisation to handle incidents? (For example if exchanging data with them or contracting them as a third party supplier) The choice was a Likert scale of 5
>
> Q. Once refined would you consider using this Maturity Model in your organisation or one you would be assessing. The choice was Yes Possibly or No
>
> Q. Would just knowing what the Critical Success Factors are and using an internal method of ensuring a gradual move to ensure they were embedded be a better approach for your organisation The choice was Yes Possibly or No

There was a final section which allowed for any other comments. They may wish to make. All of the questions allowed for free text comments

The IRMM was sent out to all those who had responded to round two of the Delphi (82 in total). In addition, a control group was used to add a test of the validity of the CSF the external validity of the interpretation of the Delphi findings and to ascertain how well the IRMM would be understood by those who had not been involved in its iterative construction through the Delphi process. Of all the responses, only one respondent sought clarification on the question and, when explained, had no difficulty in then providing their answers.

6.8.3 Write Accompanying Letter/Request Letter

The IRMM had two versions one for original Delphi group and the other the control group. The Chair of the National Policing service Information Board and Commissioner of the City of London Police (who had already supported the Delphi) was approached again. He agreed to support a request for those who were newly in post as security professional in the UK Police Service who, if eligible under the agreed criteria, may wish to become part of a control group. He wrote an introductory letter (appendix 11) which accompanied the email that was sent to potential control group participants.

The Delphi group received an email which (appendix 13) which was in effect the introductory letter. The email contained the rational for the IRMM and in particular explained that it contained the four CSF's that incorporated the amended descriptions taken from their comments. It asked they view the IRMM to see whether it was understandable, usable and considered to be of value to their organisation regarding the deployment of those CSF's.

6.8.4 Test Questionnaire with a Small Sample

As in previous studies the IRMM underwent testing to ensure the flow, instructions and questions did not cause any confusion or ambiguity. Again testing of the differing formats of word and pdf and whether the questionnaire would be blocked by IT security took place

6.8.5 Choose the Method of Distribution and Return

As in the Delphi study the IRMM was emailed to those who had participated in the Delphi and to the potential members of the Control Group. The emails were different as the control group email had the accompanying letter from the commissioner of the City of London police as well as the IRMM. The method of return was also the same and instructions on how to do this were included.

6.8.6 Plan Strategy for Dealing with Non Responses

Again, as in Chapter 5, it was decided to personally respond to every completed response by thanking the sender. This again later proved beneficial where anyone who had responded and returned a completed survey, but not received an acknowledgement would know their answers had not been received. After the initial deadline date had passed a chase up email was sent to those who had not appeared to have responded. This resulted in further responses from those who had not yet responded received a thank you message.

6.8.7 Conduct Tests for Validity and Reliability and Representativeness

This followed the same rationale as for Chapter 5

Validity.

This study was based on the findings of the Delphi study and in itself was a test of the validity of findings that approach. By selecting the original Delphi participants ensured a degree of consistency as they had already been involved in the previous Delphi study and were aware of the research. The addition of a control group was intended as a test of that validity by introducing participants who met the eligibility criteria but had not been involved. Should any noticeable discrepancies in the results of the two groups be realised this could challenge the reliability and validity of this and the Delphi study.

Reliability

Using the same methods and controls outlined in chapter 5 for the Delphi should this IRMM be reissued later then the results should be similar apart from any changes in policy or perceptions and experiences of the participants since their last involvement.

Representativeness

One of the two groups participating was those who had already taken part in the Delphi study and the representativeness of this group has already been set out in chapter 5. The control group was a new introduction and the next section describes the approach to make sure the representativeness challenge could be countered.

6.9 Identifying a Control Group - Representativeness

A control group is a method that assists in understanding the phenomenon we are interested in better when we compare it with something else which is similar (Bryman, 2004, p.41). For this research a Control Group was considered as part of a validation exercise to understand whether a security professional, not involved in the Delphi process, would;

a. understand what was asked of them,

b. understand the potential use of the IRMM in relation to the wording and meaning of the CSF's to improve reporting as sufficient to as they would not have seen the CSF's before.

c. provide an opportunity to compare their responses with those professionals who had been involved in the Delphi to see if any differences of opinion occur.

The possible challenge with the control group being that it was not a wide representation of the overall Delphi group. The practicalities of finding a control group outside of the security professionals who had already taken part in the Delphi survey were significant. The approach taken was to identify a group of security professionals from within one of the sectors that provided a response to the Delphi. In fact, the first round of the Delphi 26% of the respondents came from Law Enforcement so a control group from that sector would at least represent a significant proportion of those who responded in the earlier rounds. In the end, there were 13 control group respondents 2 of which were outside of law enforcement.

Identifying potential control group respondents was not easy. As has been described earlier considerable length to invite security professionals to take part in the Delphi rounds one and two had taken place over a period of approximately 14 months. To identify through professional bodies another yet unused number who met the criteria and were willing to participate may have proved difficult. In the end it was identified that one particular group of respondents that came from the law enforcement sector had experienced considerable churn in their security staff and that may provide a small number of volunteers to take part who were relatively new to that sector and may have worked in other security sectors.

If the IRMM is to be considered as a useful tool it needs to be of practical use, not just that it works with those who had been directly involved in its iterative construction. To use a previously unsighted group to take part in the IRMM at the same time using the same format may identify weaknesses in approach or indicate that the consensus achieved for the CSF may not be able to continue through into the IRMM.

6.10 Summary of findings from the IRMM Validation Study

There were 59 respondents from the Delphi group (response rate out of 101 = 58%) of which 50 made comments (84%). There were a possible 101 responses due to attrition from previous Delphi rounds (left organisation, dropped out etc.). This is a minimum response rate as the IRMM questionnaires were sent to all Delphi participants including those who did complete round 1 but did not participate in round 2 and may also have left their organisations but no indication of this (e.g.in the bounced e mail.) Of the 59 respondents 58 had completed round 2. Only one respondent who did not complete round 2 but did complete round 1 responded.

For the Control group there were 13 responses of which 11 made comments. The potential response rate for the Control group was difficult to assess. The UK police service security contacts held by the National Policing Information Risk Management Team recognised that there had been some reduction in security staff and due to this and other changes 35 UK police forces were contacted. Most with personal email addresses. Some bounce backs indicating a leaver were received but this does not mean all the addresses related to an employee still in post. The response of 11 completed forms from law enforcement represents a minimum return of 31%. Two other control group forms were received who were not in the targeted law enforcement group. One as a result of it being forwarded by a respondent to the Delphi study to a person in their organisation who was new and would be responsible for such monitoring and measurement. The other was from an organisation that had responded to round 1 of the Delphi but due to staff changes had not responded to round 2 or the initial IRMM. This respondent worked for that organisation and became aware of the Delphi and IRMM and volunteered to respond. It was decided to use them as a Control group response as they had not personally responded to the initial Delphi.

6.11 The Validation Survey Results

The below table sets out as comparison of the findings from the validations survey and compares the results from the Delphi participants against the Control Group.

Question	Delphi Respondents		Control Group	
CSF 1 A recognition by senior management that incidents will happen and that they must play a full and active part in the incident management process (A 5 point Likert Scale was used)	Easy or very easy to understand/interpret an organisations position	91%	Easy or very easy to understand /interpret an organisations position	84%
	Easy or very easy to use to judge an organisations position against the maturity levels	76%	Easy or very easy to use to judge an organisations position against the maturity levels	69%
CSF 2 Ease of making a report, recognising if reporting incidents is difficult individuals will be less likely to submit them. (A 5 point Likert Scale was used)	Easy or very easy to understand/interpret an organisations position	90%	Easy or very easy to understand/interpret an organisations position	77%
	Easy or very easy to use to judge an organisations position against the maturity levels	79%	Easy or very easy to use to judge an organisations position against the maturity levels	69%
CSF 3 Rapid, useful, accessible and intelligible feedback to the reporting community (A 5 point Likert Scale was used)	Easy or very easy to understand/interpret an organisations position	83%	Easy or very easy to understand/interpret an organisations position	85%
	Easy or very easy to use to judge an organisations position against the maturity levels	75%	Easy or very easy to use to judge an organisations position against the maturity levels	85%
CSF 4 Incident analysis that considers root causes and wider systems/processes, not just the initial impact assessment. (A 5 point Likert Scale was used)	Easy or very easy to understand/interpret an organisations position	87%	Easy or very easy to understand/interpret an organisations position	84%
	Easy or very easy to use to judge an organisations position against the maturity levels	73%	Easy or very easy to use to judge an organisations position against the maturity levels	62%
Do you use Maturity Models in your organisation or one for which you have reviewed or assessed (Yes or No)	Yes 70%		Yes 62%	

Question	Delphi Respondents		Control Group	
Do you personally feel Maturity Models are useful tools to assist an organisation understand where they sit regarding to a particular situation. (Yes/No /No Strong View)	Yes 88% No 2 % No Strong view 10%		Yes 69% No 8% No Strong view 23%	
Some Maturity Models set out a larger number of elements to measure against. Is just listing the critical elements a better approach. (Yes/No /No Strong View)	Yes 52% No 12% No Strong view 36%		Yes 69% No 0% No Strong view 31%	
Overall would you consider this Maturity Model to be of value to your organisation to assess how security incident reporting is handled and managed against the identified Critical Success Factors	Said it was valuable or extremely valuable	88%	Said it was valuable or extremely valuable	85%
If other organisations used the same model would this assist when determining the ability of that organisation to handle incidents? (for example if exchanging data with them or contracting them as a third party supplier)	Said it was valuable or extremely valuable	80%	Said it was valuable or extremely valuable	92%
Once refined would you consider using this Maturity Model in your organisation or one you would be assessing (Yes/Possibly/No)	Yes 59% Possibly 40% No 2%		Yes 62% Possibly 38% No 0%	
Would just knowing what the Critical Success Factors are and using an internal method of ensuring a gradual move to ensure they were embedded be a better approach for your organisation (Yes/Possibly/No)	Yes 34% Possibly 49% No 17%		Yes 46% Possibly 31% No 23%	

Table 6-4 Validation Survey Results

In general, with regards to the four identified Critical Success Factors the answers relating to whether the CSF is considered very or easy to interpret the scores were high. Although still high there appeared to be less confidence in using the Maturity Model to judge the position of their organisation. This was understandable as the tool had not actual been used to assess the organisation merely as to its potential to do so. It is likely that this confidence may result from actually using the tool but even so the scores across all four CSF’s showed the lowest to be from the control group for CSF number four at 62%. This is still an encouraging score.

Except for CSF number 3, the Delphi group scored higher but only by a small amount. What was particularly encouraging were the responses to the questions relating to the use of the IRMM as a tool to deploy the CSF's.

With regards to the use of Maturity Models The Control group appeared to use Maturity Models less. This may be of no significance or could reflect on the majority of the control group being from the one public sector group and possibly less likely to use a Maturity Model. A similar difference regarding the view on the usefulness of Maturity Models. If the control group had used Maturity Models less they are less likely to have been able to comment on their usefulness.

With regards to the IRMM being of value to their organisation the scores were encouragingly high where 88% of the Delphi group considered it to be either valuable or extremely valuable and even amongst the control group this score was 85%.

The specific question that asked whether the IRMM could be used to assess third party organisations with whom their share information was also high. Particularly with the control group. Interestingly the respondents gave even higher scores for other organisations using it so they could be judged than they were to use it to judge themselves. Having said that, once refined, most would use the IRMM.

When asked if just having a list of the CSF’s as opposed to using the IRMM would be better for their organisation this gave the lowest of positive scores across the whole questionnaire which again indicates a favourable stance for the IRMM and even if not used the CSF’s could be used as a standalone entity.

The overall results were encouraging on two main counts. Firstly there were only minor differences between the Delphi group and control group findings. Broadly speaking the control group was not at odds with the Delphi group results. There was support for the Delphi even to deploy it. This indicates the potential for the IRMM to be further researched as to the outcome of its use and any potential increase in reporting that results which is one of the recommendations for future research.

Although when the validation Maturity Model was sent out there was no request to use it to judge the respondents organisation a couple did. There were also favourable comments from some of the respondents that they would actually use or consider using the IRMM once further refined and finalised to conduct an assessment against their current reporting. A selection of some of the comments relating to the potential use of the IRMM are summarised below.

> *Yes: I’ve used this table to match against an internal scoring mechanism we used last year to compare ourselves at different points along our road to implementing an internal/[redacted]-partnered SOC*

> *I have already started to apply some of the knowledge that I have learned through the review of this model*

These two comments appear to indicate the IRMM has started to be used in one form or another. The below comments relate to its usability.

> *I like the straightforward nature of this MM, in which it describes the key elements of incident management that can be easily understood by non-technical management and can be evaluated in real-world terms. It is concise which can give a quick look overview that would be applicable to most sizes of organisation.*

> *It clearly and simply defines what success factors are relevant and why and how they are to be scored.*

The following are examples of its future use either now or once refined.

> *Please let me know if this hard work of yours gains acceptance. I would be happy to use it to bench mark our 'as is' maturity and then use it further to improve the standards in an attempt to achieve 'optimised' in all CSFs*

> *Where I would find this model and the 4 CSFs particularly helpful would be in highlighting to the SIRO where I see vulnerabilities in our current incident reporting mechanisms*
>
> *I would definitely consider using a version of this MM as part of any wider evaluation as I like the concise nature, simplicity of use and the focus on the key requirements of the capability.*
>
> *When can I start using it?*

There were of course others who would not consider using it. In the specific question relating to once refined would you consider using it there were eighteen responses one said no, six said yes and the rest, ten, said possibly. One response was unclear. The no response was below

> *Not my role to do this sort of thing ……*

6.12 Summary

The validation survey had three main aims;

To check that the final CSF selection findings;

To test the potential of an Incident Reporting Maturity Model (IRMM) as a tool;

and

To further test the IRMM and CSFs using a control group.

In relation to the first aim;

CSF 1. There were two comments from one respondent from the Delphi group stating the first two of the bullet points did not read well. There were no other adverse comments from the Delphi or control group for this CSF so no amendment was considered.

CSF 2. There were no comments from any of the respondents.

CSF 3. There was one observation about the investigative process, not the wording of the CSF. One comment about informing the community from the same respondent who made the comments regarding CSF 1. This was not a wording challenge. There was another comment that they were not sure about one of the bullet statements being quite correct and referred to anonymity needed in some cases. As a result no change considered.

CSF 4. There was one comment from a Delphi participant suggesting the removal of the word ‘just’ from the third bullet point. This could be amended but no other comments were made, so again no change to the wording of this bullet point was made.

Therefore, overall no CSF wording was challenged to an extent there would be cause for concern for either the wording or author’s interpretation of comments through the Delphi rounds. Three of the comments made came from the same respondent. The low number and nature of the comments made was viewed as a majority endorsement of the CSFs wording

With regards to the second aim 88% of respondents from the Delphi and 82% from the control group felt the IRMM would be valuable for their organisation to use and when asked if they would use it for their organisation a good majority of the Delphi said yes with 40% saying possibly. This was similar to the control group. This gives a strong sense that the CSF’s combined with the IRMM have a real potential to be used to improve security incident reporting. These figures also answer the aim as the control group scores were broadly similar to that of the Delphi group. In summary, the four identified CSF’s were still considered to be so by clear high scoring.

The four CSF’s could be viewed as sequential. Starting from a recognition that incidents will occur to then having a process that makes it easy to report incidents, then provide feedback to reporters (to encourage future reporting) and finally making use of the reports to understand the root causes to prevent or reduce reoccurrence.

Should an organisation wish to use the ISO/IEC 27035 standard the CSF’s and IRMM appears to have the potential to assist in this. When the four CSF’s are placed in an order of approach and then compared with the ISO/IEC 27035 stages there does appear to be a synergy.

Using the four identified Critical Success Factors they could be placed in a circular fashion as previously described in Chapter 5.

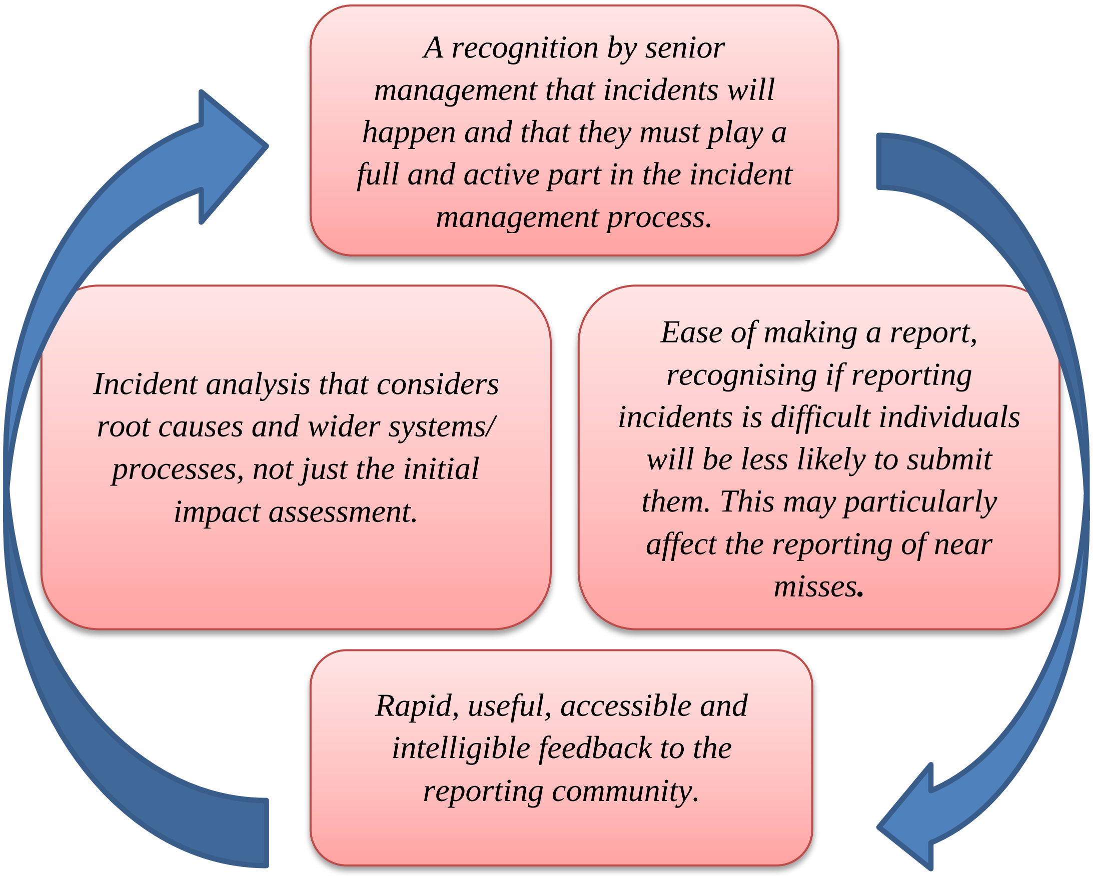

A recognition by senior management that incidents will happen and that they must play a full and active part in the incident management process.
Incident analysis that considers root causes and wider systems/ processes, not just the initial impact assessment.
Ease of making a report, recognising if reporting incidents is difficult individuals will be less likely to submit them. This may particularly affect the reporting of near misses.
Rapid, useful, accessible and intelligible feedback to the reporting community.

Figure 6-1 The Four CSF's in a Cyclical Process

This cyclical process can be compared to the British Standard ISO/IEC 27035 approach to managing incidents as described by Tondel, Line and Jaatun (2014, p.44) in their figure below.

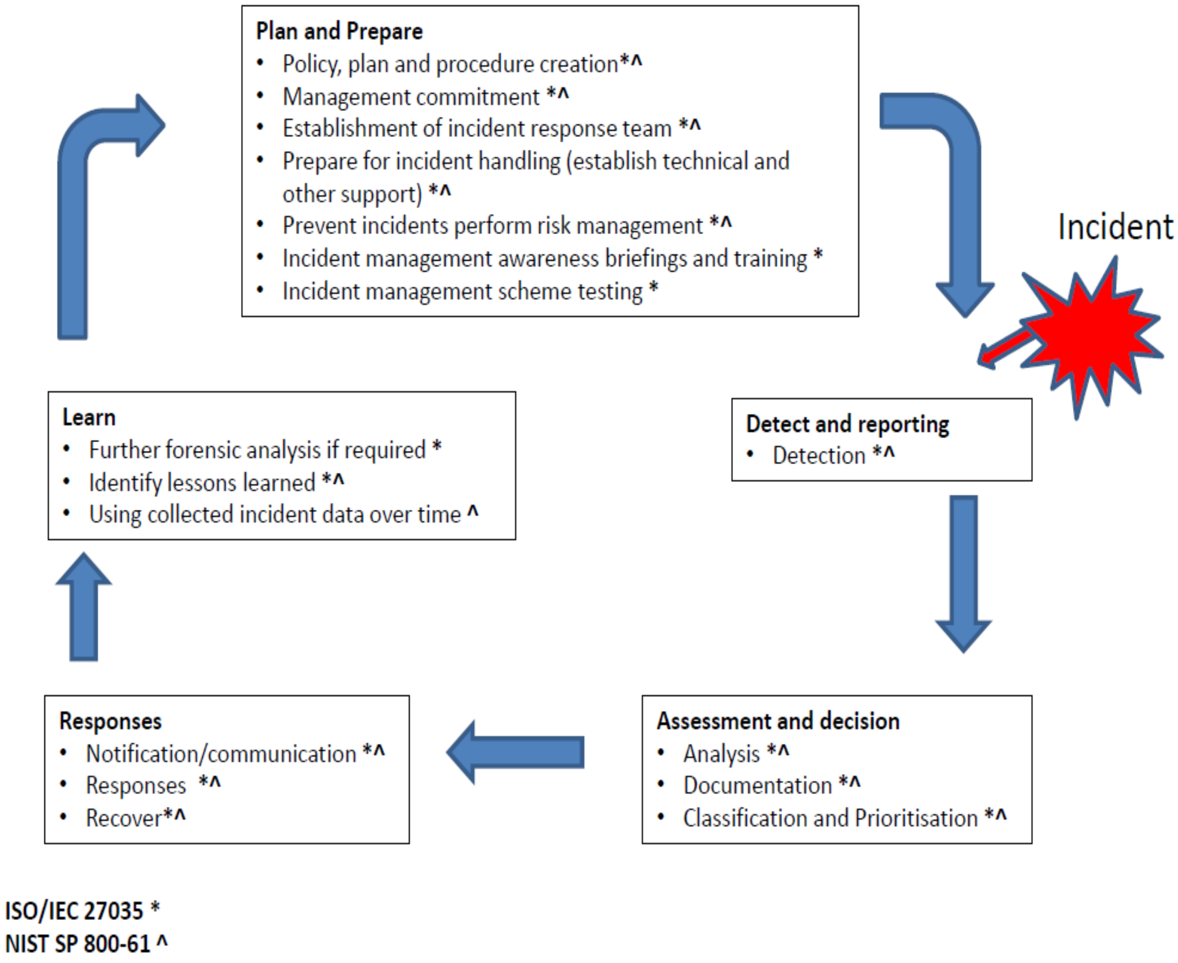

Plan and Prepare
Policy, plan and procedure creation*^
Management commitment *^
Establishment of incident response team *^
Prepare for incident handling (establish technical and other support) *^
Prevent incidents perform risk management *^
Incident management awareness briefings and training *
Incident management scheme testing *
Incident
Detect and reporting
Detection *^
Assessment and decision
Analysis *^
Documentation *^
Classification and Prioritisation *^
Responses
Notification/communication *^
Responses *^
Recover*^
Learn
Further forensic analysis if required *
Identify lessons learned *^
Using collected incident data over time ^
ISO/IEC 27035 *
NIST SP 800-61 ^

Figure 6-2 Adaption of The Incident Management Process. Tondel, Line and Jaatun (2014, p.44)

A comparison of the 5 ISO/IEC 27035 stages against the 4 CSF's identified in the Delphi outlines where the CSF's compliment the standard's stages and should assist in adopting the standard in practice. For example stage 1, to 'plan and prepare' for incident management, those plans will be tested this may not be taken as seriously unless there is 'an acceptance that incidents will occur' (CSF 1) and Stage 2 'Detect and report' requires staff to know how to what and how to report so CSF 2 'ease of reporting' will provide valuable assistance. Assess and decide relies on the incident being reported in the first place so this stage has a reliance on CSF 1 and 2. Stage 4 'Responses' does have an element of communication and may include updating the person who reported. This stage should include CSF 3 'feedback to the reporter'. Finally stage 5 'learn' is complimented by ‘CSF 4 ‘root cause analysis’. The below table sets out the comparison and relationship between the incident management stages and the CSF’s.

ISO/IEC 27035 stages	**CSF’s applicable to the stages**	**Comment**
1.Plan and prepare	1. A recognition by senior management that incidents will happen and that they must play a full and active part in the incident management process	To plan there needs to be an acceptance that something will happen
2.Detect and Report	2. Ease of making a report, recognising if reporting incidents is difficult individuals will be less likely to submit them. This may particularly affect the reporting of near misses.	If it is not detected or reporting is difficult then under-reporting will occur. The CSF ‘Ease of reporting’ should help to alleviate this
3.Assess and Decide		Not part of the CSF process
	3. Rapid, useful, accessible and intelligible feedback to the reporting community	An important part of the process not shown in the ISI/IEC stages
4.Responses		Actions on reporting can only occur if the incident is reported. One response could be notification to the reporter of what has happened to the report
5. Learn	4. Incident analysis that considers root causes and wider systems/ processes, not just the initial impact assessment	A synergy of approach – both deal with learning from the incident

Table 6-5 Authors Comparison of the CSF’s Against the ISO/IEC 27035 Incident Management Process Stages set out by Tondel, Line and Jaatun in Figure 6-2

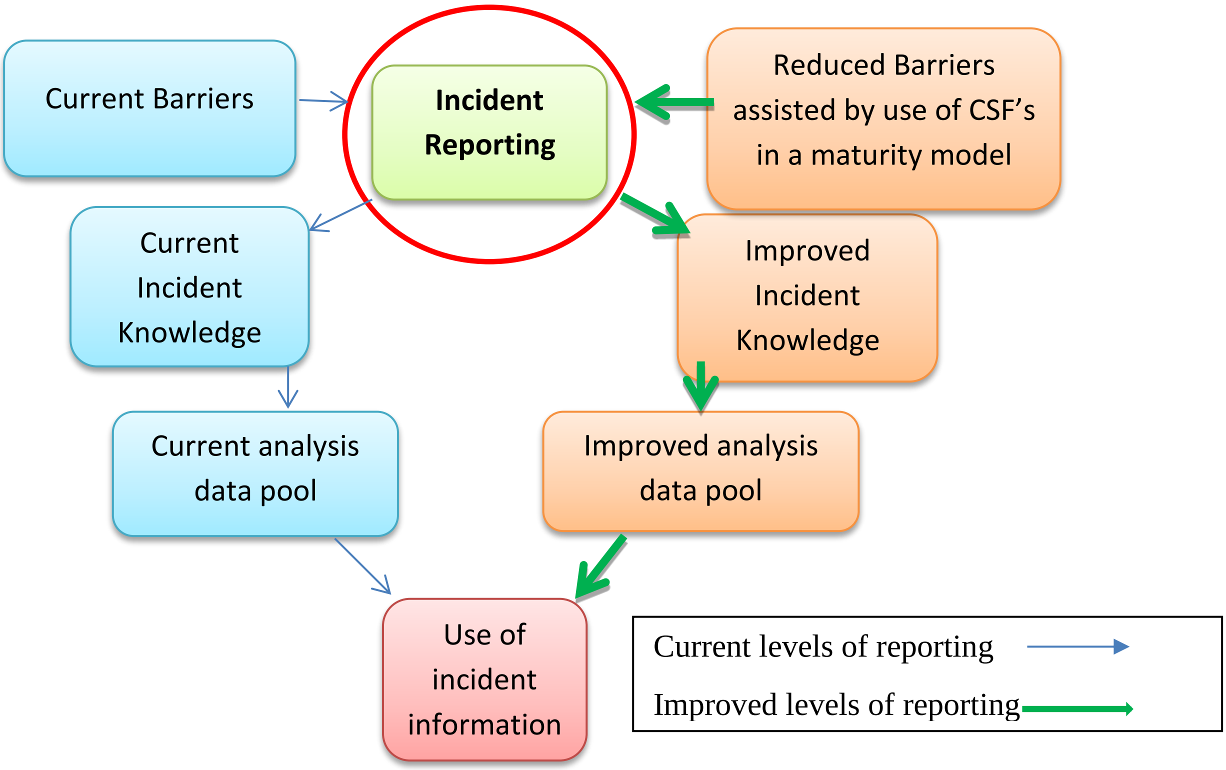

Current Barriers
Incident Reporting
Reduced Barriers assisted by use of CSF's in a maturity model
Current Incident Knowledge
Improved Incident Knowledge
Current analysis data pool
Improved analysis data pool
Use of incident information
Current levels of reporting
Improved levels of reporting

Figure 6-3 Authors Suggested Current Restricted Flow of Reported Incidents and the Potential Improvement using the IRMM.

Figure 6-3 demonstrates the potential impact that barriers to reporting currently have and the result should an organisation adopt the proposed CSF's and IRMM. This in turn may release the flow of security incident data to enable more informed decisions on risk management. If this is achieved at a local organisation level the following figure 6-4 outlines how this could have the potential to improve the information flow to enable the sharing of information security incident knowledge. This in turn could potentially support the risk management process locally, regionally (or by commercial sector) and then at national level; with a further potential to become international. Initiatives in the UK such as CiSP (CERT UK, 2015) aim to improve the sharing of cyber security incident information at a national level. However, this research will explore the view that due to under-reporting initiatives national incident sharing initiatives, such as CiSP can be viewed as an aspirational approach. To be more effective at the national level the reporting of incidents at the lower level has to be improved.

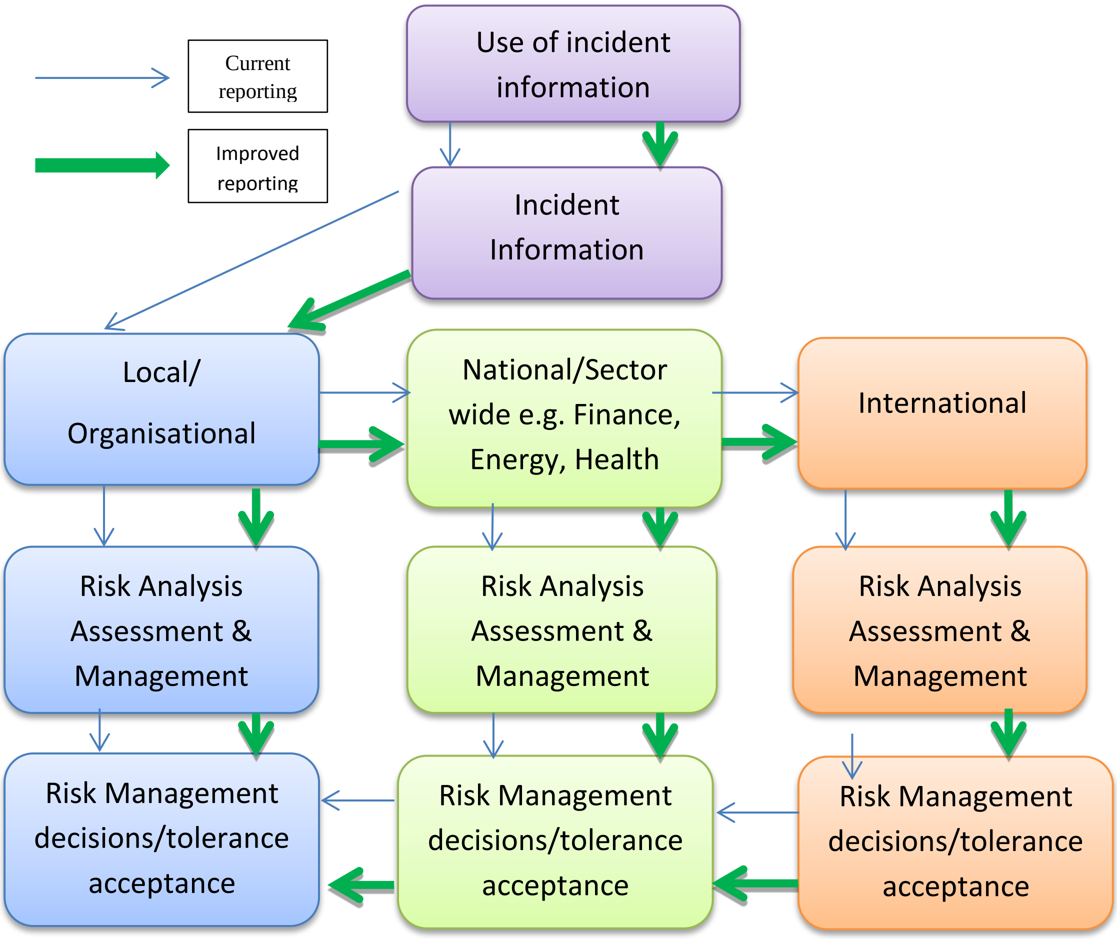

Current reporting
Improved reporting
Use of incident information
Incident Information
Local/ Organisational
National/Sector wide e.g. Finance, Energy, Health
International
Risk Analysis Assessment & Management
Risk Analysis Assessment & Management
Risk Analysis Assessment & Management
Risk Management decisions/tolerance acceptance
Risk Management decisions/tolerance acceptance
Risk Management decisions/tolerance acceptance

Figure 6-4 Authors Design of the Potential Relationship Between Local, Regional/Sector and National use of Improved Security Incident Reporting Data.

In this research the goal is to improve security incident reporting that will ultimately enable better and more informed information sharing within organisations. The Validation study and use of a control group has added assurances that the original findings as to what are the Critical Success Factors required to improve security incident reporting. By considering their results against the outcomes from the original Delphi groups finding does give credibility to the outcome. The next chapter sets out how this research could be applied to organisations.

Chapter 7 Summary and Conclusions

7.1 Summary

This research set out with an assumption, based on the author's previous findings through an MSc, that a proportion of information security incidents were not being reported. However to what degree there was under reporting was not known. The intention was to ascertain what research existed that may help to understand more about the issues surrounding security incident reporting. It became clear that, although there was research relating to sharing and the problems as a result of incidents occurring, there was little research that specifically focussed on security incident reporting.

The healthcare sector had many examples of research focussing on the reporting of incidents relating to patients. 'Adverse patient incidents', as this was referred to, gave an insight into what barriers there may be to reporting incidents in general, irrespective of what was to be reported. Having identified there appeared to be a gap in research into security incident reporting the author needed to test the assumption that there was indeed a problem with underreporting of information security incidents.

The conducting of a scoping study was intended to do just that. Recognising that to get an honest picture relating to the reporting of security incidents from those charged with protecting organisations information assets would need careful consideration. There would be real concerns that would surround confidentiality and trust when requesting detailed and honest views on a particular professional's employer's incident reporting failings and concerns. This in turn may result in poor returns to any attempts to obtain such information through research surveys. Other researchers had experienced this problem including Kotulic and Clark (2004) and Flores, Antonsen and Ekstedt (2014). By carefully considering the approach to take to elicit such sensitive information it was possible to encourage security professionals to give real insight into the problems associated with incident reporting. The scoping study, discussed in chapter 4, in 2011 was intended for anonymous responses to ensure participation and honesty. There was a good response to the questionnaire and surprisingly many respondents showed a willingness to provide their details, despite the offering of anonymity. It became apparent that there were real issues and the security profession wanted to assist in the research. This openness and trust continued in the subsequent Delphi and Validation studies.

Following the research and scoping study two distinct aims to try to reduce the problem of underreporting emerged. One was to identify the Critical Success Factors required to improve information security incident reporting, the other to identify a vehicle upon which those CSF's could be utilised to benefit any organisation. The one proposed was an Incident Reporting Maturity Model (IRMM). This would be achieved through the use of further surveys.

7.2 Results of Data Collection

By focussing on the appropriate groups and confidentiality of responses the three surveys provided a rich vein of information and the number of additional comments identified a willingness to assist in the research. The summary of each is set out below.

7.2.1 Scoping Study

The primary intention was to test the assumption there was a real concern that there was under reporting of security incidents. If this had not been evidenced in this study then the research may well have either ceased, or focused on other identified areas of concern that did emerge from the scoping study, such as incident classification. The scoping study also provides the assurance that the potential for reuse of research conducted elsewhere in the information security sector was worth pursuing.

7.2.2 Delphi Study

The Delphi method was selected as it was judged to be the most appropriate research method to take the findings from the literature and scoping study further and to seek consensus as to the identification of the Critical Success Factors required to improve the reporting of incidents. By using recognised security Communities of Interest and obtaining their permission and support for their members to be approached to participate was a key factor in gaining recognition that may persuade those security professionals, who met the eligibility criteria, to take part.

The result was a consensus after 2 rounds with valuable contributions in not only identifying the elements that could be CSF's, but also in the formulation of a better description of them that incorporated some of the supported aspects of the potential

CSF's that did not make it to the final list of four. This culminated in four CSF's which sat neatly into a cyclical process as shown in Figure 5-5 in Chapter 5 and reproduced below.

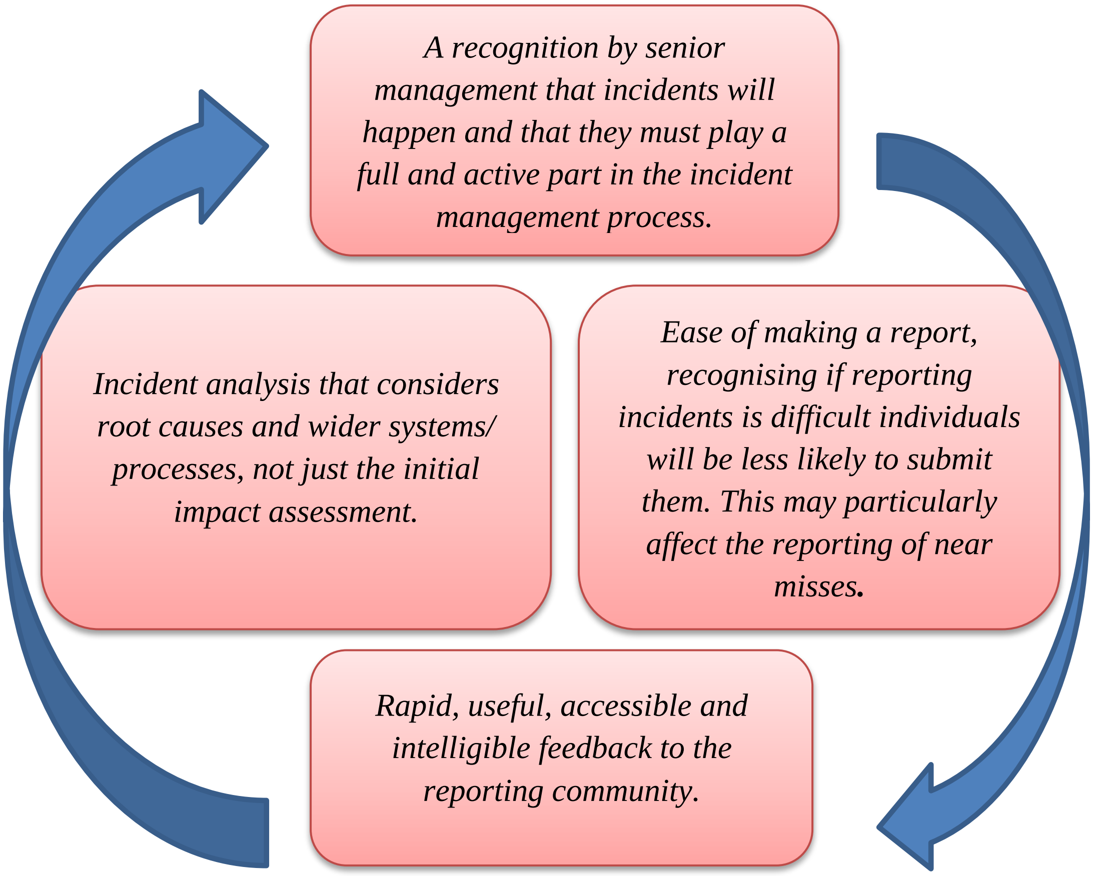

A recognition by senior management that incidents will happen and that they must play a full and active part in the incident management process.
Incident analysis that considers root causes and wider systems/ processes, not just the initial impact assessment.
Ease of making a report, recognising if reporting incidents is difficult individuals will be less likely to submit them. This may particularly affect the reporting of near misses.
Rapid, useful, accessible and intelligible feedback to the reporting community.

Figure 7-1 The Four CSF's in a Cyclical Process

7.2.3 Validation study

The study had two aims, one to validate the outcome of the analysis of the Delphi study and the iterative changes to the wording of the Critical success Factors and secondly, to seek the views of participants on the proposal to use a Maturity Model. This was achieved through the use of the original Delphi participants and a control group, who met the eligibility criteria for involvement, but were not at the time either in post or available to participate in the Delphi. Both groups completed the validation study and the comparison between the two showed considerable consensuses of opinion which gave a high level of confidence in the analysis of the original group’s contribution. It was reassuring that the control group, who had not been involved at all, scored very similarly to those who had. A number of the comments that were provided also indicated a real potential for the IRMM to be used in the real world. This is a recommendation later for areas of future research.

7.3 Answers to the Research Questions

The research questions *(in italics)* and the thesis outcomes to support the goals and provide a valuable contribution to the furtherance of research in information security incident reporting are:

> *(1) Is the perception that not all information security incidents are reported a correct one?*

This is a key element to the research and, if confirmed, what follows is to identify the possible reasons for this under reporting.

The Scoping study supports this assumption. The participants clearly indicate that there is under reporting of information security incidents. Only 38% of respondents believed the majority or all incidents were reported.

> *(2) Are the reasons for low reporting similar to those identified in other research such as the healthcare and safety industries?*

This will identify research already conducted elsewhere and examine whether any findings can be applicable to information security. The results can then be tested by conducting surveys through questionnaires on representatives of the information security profession. This in turn will enable the information security profession to make use of such findings to improve reporting in their sector.

The Scoping study, Delphi and Validation studies again support these

> *(3) Is it possible to identify the Critical Success Factors required to improve information security incident reporting?*

The identification of Critical Success Factors using information security professionals should enable a greater degree of focus on what is important and more likely to achieve results thereby improving the identification of methods to deploy to enable better reporting.

The Delphi study and Validation Study demonstrated that this is entirely possible with four CSF's being identified and the wording appropriately amended to ensure the CSF's reflected the views of the Delphi participants. In addition the four CSF's have been shown they can be used to compliment the ISO27035 incident management process and potentially assist in putting the standard into practice.

> *(4) Can a security incident reporting Maturity Model be developed that would enable an iterative approach to its deployment whilst taking account of any methods already in place?*

This will give information security professional a greater degree of knowledge in what activities and reporting mechanisms to deploy that may improve the level of reporting.

The validation study using original Delphi participants and a control group who had not been involved in the Delphi has shown strong support for the potential for an Incident Reporting Maturity Model

Overall, the research has been able to demonstrate it has answered those questions. The relationship between incident reporting metrics and risk assessments on a superficial level appears to be easy to comprehend but the research did not go on to test this in detail.

7.4 Research Contribution

There are two areas where it can be demonstrated this research has provided a substantive contribution to the body of knowledge in the subject of the reporting of Information Security Incidents.

7.4.1 Theoretical

The scoping study shows amongst the participants there is a lack of confidence that all or most information security incidents are reported. A range of views from information security professionals from both the public and private sector has validated the researcher's assumption that the true number of information security incidents is not known due to under reporting**.** This is despite 58% being subject to regulatory reporting and only 38% believing all or the majority of incidents are reported as opposed to 62% only believing that some or few are reported.

The study has demonstrated that findings from research into a similar under- reporting problem in the Health Care sector can be used and tested against the views of Information Security Professionals. As the barriers are human or organisational (or a mixture of both) it could be concluded that any strategies developed to overcome these barriers in one sector could bring a degree of acceptance and success in that of another. To some extent the workshop held in Lisbon, outlined in section 4.9 demonstrated this, where the discussion over ways to improve incident reporting led to very similar comments to those contained in a summary of findings from the Health care sector.

7.4.2 Practical

The contribution this thesis makes to the furtherance of knowledge regarding the reporting of information security incidents is to demonstrate, through validation from a wide range of information security professionals, that there is a strong view that a significant proportion of security incidents are not reported and that there appear to be similar barriers to reporting incidents as those found in research in the healthcare sector studying the reporting of ‘adverse patient incidents’.

The assumption is therefore, if a significant number of incidents are not reported, the data upon which decisions are made could be flawed. Subsequently initiatives to share security incident data to gain insight into the wider threats to sectors such as finance, pharmaceutical, government etc. would be adversely affected. Incomplete incident data could result in a false sense of security through lack of reported incidents and erroneous inputs to risk assessments. This in turn could place a higher degree of focus on certain types of incidents that are reported as being the main threat vectors. Although not a key part of the research an information security risk and security incident definition was proposed. The incident definition was created to ensure consistency in understanding of the term for the purposes of the Delphi and Validation studies

In addition the research methodology in obtaining sensitive information form security professionals has proved successful and could be replicated by others to overcome previously experiences of researchers in only achieving low level of response. Focussing on the anonymity (even though most waived this) and by engaging with the security communities of interest appears to have been successful.

7.5 Future Application of the Research

Since beginning this research for managing and reporting incidents has become paramount with the introduction in May 2018 of the EU GDPR legislation and their associated fines; As such this research is timely, relevant and necessary to enable organisations to be able to meet the reporting requirement should an incident occur. Under this legislation organisations must notify their relevant jurisdictions information Commissioner within 72 hours of a breach where it is likely to result in the risk and rights of individuals. Whilst this thesis has focussed on the reporting of security incidents in their widest sense, those relating to personal data which the GDPR is concerned with, represents some of those types of incidents. Therefore if the CSF's are applied they should equally improve the likelihood of the reporting of GDPR related incidents and potentially reduce the level of financial sanction levelled to organisations for either, not reporting, or indeed if such reported incidents are acted upon early may not result in a more serious breach that requires notification. The financial penalties for breaches under the new legislation can be punitive and when balanced against the potential costs of improving incident reporting may well represent a beneficial use time and resource. The use of the Maturity Model may well assist organisations to benchmark if the identified CSF's are in place in order to potential improve that reporting. Table 5-10 on page highlights how the CSF's can be used to support a security incident management process. The IRMM can be used by organisations to judge their current levels of maturity against the CSF's and identify areas for potential improvement. It terminology can always be tailored to suit the relevant business sector whilst the CSF's appear to be internationally and multi business sector acceptable.

7.6 Potential Papers

As a result of this thesis a number of potential papers based on the three studies have been identified which could benefit academia, business and security professionals.

1. The Scoping Study outlining how research from other sectors was demonstrated as having the potential for reuse in a different sector as well as the methods and approach used to obtain sensitive responses from security professionals

2. Delphi study being used to obtain consensus for CSF's and again obtaining honest views from security professionals

3. The Validation study as a method of confirming the consensus and proposing a potential Incident Reporting Maturity Model together with the involvement of a control group to compare the Delphi and IRMM views of this not previously involved group with the Delphi participants.

7.7. Reflections on the Data Collection Approach

7.7.1 Surveys: What Worked Well?

The construct of the surveys achieved its aim in eliciting honest and open views through the efforts made to ensure anonymity. Having said that, for whatever reason, the majority of respondents were more than happy to provide their full contact details. It could be assumed that this is due either to their belief in the research aims and the willingness to take part in further discussions with the author or, that although provided with the opportunity to be completely anonymous, they trusted the researcher in the promise to keep the identities confidential. The personal approach certainly assisted in obtaining a good response.

The fact the author is also a security professional and that previous research experience in eliciting sensitive information regarding critical infrastructure protection within policing potentially may have ensured a reasonable level of confidence amongst participants for them to want to be involved and provide honest responses. Coupled with the assurances of anonymity if chosen, the results were better than expected. Bearing in mind this was not just a UK audience but a worldwide one, it was surprising that only one participant asked for clarification on a question out of all the three studies, not one question was received seeking clarification in how to complete them. As a result, there were only a few where a note had to be made in the compilation of figures where a question had been missed. Interestingly there were no particular or repetitive mistakes. Therefore the error rate was small and the location of any mistake was random.

7.7.2 Surveys: What did not Work Well?

Surprisingly little went wrong apart from the problem with different versions of Microsoft Office and Adobe Acrobat resulting in the challenges with formatting of response boxes. The other issue was that of some organisations defences stripping out macros that were embedded in the questionnaires in the form of drop down menus.

This was identified in testing, particularly with Microsoft word and there was a risk some organisations defences may block one or other of the questionnaires. This was countered in the Delphi and validation survey by sending the word and pdf forms out separately.

In the paper based scoping study some interpretation of the handwriting did prove slightly challenging and this is where a typed response would have proved better. However, for primary evidence of completion a personally handwritten response is far better. Also for those seeking anonymity (as it turned out most declined this) using a machine would have left a record should there be any comeback later. Subsequent Delphi studies were mostly completed by typing and all the validation study responses were typed. The other issue is that of storage. Paper returns have a risk associated in that they are the sole record and to be on the safe side scanning or copying them to ensure a backup is available is now required. An electronic version is easier to replicate and provide resilience.

The one disappointing element of the scoping study was the low response from the Oil and Gas conference. Had the author been able to remain at the event during the evening and following day more forms may have been returned. In addition, the event was not attended by the same type of security professional that went to the NISC and NG conferences. The Oil and Gas event, even though billed as a security event, was more aimed towards technical security and fraud rather than a CISO/ISO audience. It appeared the maturity of the Oil and Gas industry in regards to Infosec seemed less than others. This may only be an indication from the presentations and conversations held during the event.

7.8 Areas for Suggested Further Research

It is suggested that an area for further research is a case study on of the use of the IRMM in one or a number of organisations to understand whether or not the IRMM did indeed result in an improvement in the number of incidents being reported. Using the IRMM with a small number of organisations to benchmark where they currently sit and then, over time, analyse following the application of the CSF's whether it made any improvement in the level of reporting.

It was identified during the scoping study, and through the literature review, that there is a problem with a lack of standard taxonomies for security incidents and information security risk. This makes comparisons of incident type challenging and the information sharing initiatives currently in place can suffer through this lack of clarity. It is recommended that this would be an area for research that could bring about further improvements in the overall incident management process.

If the issue of incident reporting were to improve, are there appropriate resources to handle them? If the pool of empirical data improves then this would benefit risk assessment however if the number of incidents that would be referred to CERTs increased the logistics of handling such an increase may be a challenge. In their paper, Limits to Effectiveness in Computer Security Incident Response Teams Wiik, Gonzalez and Kossakowski (2005) identify that, if there is an increase in reporting of incidents then there is the likelihood of lack of resources amongst CERTS to cope.
In their abstract Wiik, Gonzalez and Kossakowski (2005) state;

> “The main task of a CSIRT is to mitigate the effects of computer security incidents. A frequently identified problem is that CSIRTs are over-worked, under-staffed and under-funded”

Based on a case study they continue;

> “identified that short-term pressure from a growing incident work load prevents attempts for developing more response capability long-term, leading the CSIRT into a capability trap. Fundamental solutions will typically involve a worse-before-better trade-off for management.” (Wiik, Gonzalez and Kossakowski, 2005, p.1)

If this is the case, then an increase in incident reporting can leave to an overloading of already struggling CERTS and it may be that it will take some considerable time before any benefits derived from an increase in incident reporting will bring tangible empirical evidence based assumptions of risk trends. This should not be a reason for deterring any improvement in incident reporting. There is also a risk that if reporting increased there could be scope for misinterpretation and concern that the situation is getting worse, when in fact it is informing those responsible for managing risk and allocating resources where the true problems and challenges exist.

7.9 Conclusion and Recommendations

Through the use of a scoping study, a Delphi study and subsequent validation study the research identified four Critical Success Factors believed necessary to improve the reporting of security incidents and subsequently offer a security incident reporting Maturity Model that can be deployed by organisations to achieve this improvement in reporting. It outlined the apparent lack of consistency of information risk and incident definitions and classification and the subsequent challenges this places upon professionals tasked with implementing the growing number of information sharing initiatives.

The Scoping, Delphi and Validation studies have shown that by following recognised methods for the construct of surveys and can bring about valid and honest responses amongst a group of respondents who by the nature of the area being researched can be reticent in providing that information. This research has provided a strong view that incident reporting in itself can be complex as can the reasons why they are, or are not, reported. The various studies mix of quantitative and qualitative answers provided valuable and insightful responses and views that a simple quantitative survey would be unlikely to elicit.

It is also apparent that barriers to incident reporting do exist, as is the consensus is that not all incidents that occur are reported; this in fact relates to a considerable number that do not come to official notice. Thus potentially putting into jeopardy assumptions made by a range of risk assessment calculations, where security incidents form part of that analysis. Therefore, the current trust placed in the outcome of risk assessments needs to be carefully considered as an element of any risk assessment is based on likelihood of the occurrence of a threat or vulnerability.

It is evident from the literature review in Chapter 2 that the amount of research into the reporting of security incidents is limited. Critical to managing risk is to understand and have confidence in the level of protection against known vulnerabilities and accurate data relating to the types of adverse security incidents that have occurred and are still occurring. Knowledge of trends and emerging threats is key to this. However, without sufficient trusted data, such decisions can never be truly fully informed. There is also a real concern over the ability to identify and classify incidents to provide a true analysis of the number of type of incidents actually occurring. There is an identified a lack of standard taxonomies for security incidents and information security risk. This was not followed up in depth by this Thesis but as stated earlier is an area for recommended further research.

This research aimed to add value to academic knowledge by investigating the subject of security incident reporting which appears not have been studied in depth. It examined the potential re-use of research on the subject conducted elsewhere such as in healthcare studies into patient safety and the adverse incidents that can lead to harm as well as aviation and other safety industries. These research findings could be of relevance to the information security field. A potential method to improve incident reporting was proposed using the identified CSF's and placing them into an Incident Reporting Maturity Model which has the potential to be applied by organisations in an iterative, non-proscriptive and contextual manner.

The outcome may potentially result in improved security incident reporting which creates an increase in the knowledge of incident occurrence together with the true cause. This in turn may deliver a more informed analysis for future risk management through the availability of more empirical data than is currently available relating to such incidents. By potentially increasing the pool of incident reporting data this could enable improved analysis and lead to better informed risk based decisions and the ability of organisations and nations to share information in their quest to improve overall cyber security.

The research aimed to highlight that current national strategic approaches to information sharing rely on a belief that incidents are reported when in fact a considerable number are not. The inability to analyse what is not reported could result in flawed or less that optimal judgment on the causes and numbers of incidents and may well result in inaccurate assessments. It is recognised that the introduction of a proposed Maturity Model will not in itself make a significant and immediate impact. However, it may provide a catalyst for removing, or at least reducing, the effect of any identified barriers to reporting. Over time, should more incidents be reported, this may produce greater confidence in the true level of actual incidents occurring. This in turn may possibly enable better informed decisions on resource and financial expenditure to counter or reduce the likelihood of those incidents occurring.

References

Adams J. (2003) *Risk and Morality: three framing devices.* Available at *http*://john-adams.co.uk/wp-content/uploads/2006/risk_and_morality_in_press.pdf (Accessed: 12/7/15)

Argyris Chris (1997) Double Loop Learning in Organizations. *Harvard Business Review* Sept-Oct 1977 p 115-125 Available at: http://media.usm.maine.edu/~lenny/transferred2/DOUBLE%20LOOP/Argyris%20Double%20Loop%20Learning%20in%20Organizations.pdf (Accessed: 15/7/15)

Association of British Insurers. Insurance Advice on Home Security (2017) Available at: abi.org.uk/globalassets/sitecore/files/documents/publications/migrated/home/abi-guide-to –home-security.pdf (Accessed: 20/8/17)

ATOS http://in.atos.net/en-us/*olympic_games/what_we_deliver/our_challenges*/default.htm (Accessed: 28/1/12)

Andersen V, Henriksen H (2006) E- Governmental Maturity Models: Extension of the Layne and Lee model. *Government Information Quarterly* 23 (2006) 236-248. DOI 10.1016/j.giq.2005.11.008 Available at: http://ac.els-cdn.com/S0740624X05000973/1-s2.0-S0740624X05000973-main.pdf?_tid=8a6b82e8-ca3a-11e3-b809-00000aab0f26&acdnat=1398184033_6e3d57feb021d25328e030e4fcd41ddf

Ashenden D, Jones A (2005) *Risk Management for Computer Security*. Butterworth Heinemann. London.

Ashenden, D. Lawrence, D (2013) Can We Sell Security Like Soap? A New Approach to Behavioural Change. NSPW '13 Proceedings of the 2013 New Security Paradigms Workshop http://dx.doi.org/10.1145/2535813.2535823

Ashenden D, Sasse A (2013) CISOs and Organisational Culture: Their own worst enemy Computers *& Security 39 (2013) 396 e405* http://dx.doi.org/10.1016/j.cose.2013.09.004

Australia CERT Available at: www.cert.gov.au/incidents (Accessed: 28/9/12)

AusCERT Available at: www.auscert.org.au (Accessed: 28/9/12)

Baker, W.H. Rees, L.P. Tippett, P.S. (2007). 'Necessary Measures - Metric Driven Information Security Risk Assessment and Decision Making'. *Communications of the ACM* October 2007 Vol 50 No 10 Pages 101 to 106. http://dx.doi.org/10.1145/1290958.1290969

Baskerville, R. (1991). 'Risk Analysis As a Source of Professional Knowledge'. *Computers and Security*. 10 (8) Pages: 749-764. Elsevier Science Publishers Ltd. DOI https://extranet.cranfield.ac.uk/10.1016/,DanaInfo=dx.doi.org+0167-4048(91)90094-T

BBC (2007) *Hackers target TK Maxx customers* Available at: http://news.bbc.co.uk/1/hi/business/6508983.stm (Accessed: 9/7/17)

BBC (2009) *Cyber 'threat' to London Olympics* (referring to comments made by Blunkett, D.) Available at: http://news.bbc.co.uk/1/hi/england/london/8019948.stm (Accessed 1/9/13)

Beaubien, M and Baker, D, (2002) A review of Selected Aviation Human Factors Taxonomies, Accident/Incident Reporting Systems and Data Collection Tools. International Journal of Applied Aviation Studies, 2(2), 11-36

Becker, Dr Jorg. Knackstedt Dr Ralf, PoppelBub Jens (2009) Developing Maturity Models for IT Management - A Procedure Model and its Application *Business and Innovations Systems Engineering* DOI 10.1007/s12599-009-0044-5

Ben-Asher, N Gonzalez, C. (2015) Effects of cyber security knowledge on attack detection. *Computers in Human Behavior (*sic*) 48 (2015) 51-61 DOI10.1016/j.chb.2015.01.039*

Birch, D.G.W. McEvoy, N.A. (1992). 'Risk Analysis for Information Systems'. *Journal of Information Technology* 1992, 7, 44-53. doi:10.1057/jit.1992.7

Blakley, B. McDermott, E. Geer, D. (2002). 'Information Security Is Information Risk Management. *New Security Paradigms Workshop* '01 September 10-13 2002 Cloudcraft New Mexico USA http://dx.doi.org/10.1145/508171.508187

Blasch, E et al (2013) Revisiting *the JDL Model for Information Exploitation*. 16th International Conference on Information Fusion Istanbul, Turkey, July 9-12, 2013 Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6641155 (Accessed: 3/8/17)

Bodin, L. Gordon, L and Loeb, M. (2008) 'Information Security and Risk Management'. *Communication of the ACM April* 2008 Vol 51 No 4 Pages 64 to 68 DOI: 10.1145/1330311.1330325

Brostoff, S. Sasse, A. (1999) 'Are Passfaces More Usable Than Passwords? A Field Trial Investigation'. http://hornbeam.cs.ucl.ac.uk/hcs/teaching/GA10/lec2extra/hci2000.pdf (Accessed: 21/4/13)

Boynton A, Zmud R,. (1984) *An Assessment of Critical Success Factors* http://as.nida.ac.th/~waraporn/resource/704-1-50/Readings/6-Assessment%20CSF-Boynton-Zmud.pdf

Brown, A. (1995). *Organisational Culture.* Pitman Publishing London

Braithwaite, J Westbrook, M Travaglia , J (2008) 'Attitudes toward the large-scale implementation of an incident reporting system' *International journal for Quality in Health Care* volume 20 no 3 pp 184-191 doi 10.1093/intqhc/mzn004

Browne, N. De Crespigny, M. Reavis, J. Roemer, K. Samani, R. (2011). '*Business Assurance for the 21st Century'*. http://common-assurance.com/resources/Business_Assurance_for_the_21st_Century-final.pdf (Accessed: 8/3/12)

BSI ISO/IEC 27035. (2011). *Information Technology Security Techniques Information Security incident management* first edition 2011_9_01 BS ISO/IEC 27035:2011 ISO/IEC 27035:2011. ISBN 978 0 580 63587 8 British Standards Institute, London

BS ISO/IEC 27035 (2016) *Information Technology Security Techniques Information Security incident management* first edition 2016_11_01 BS ISO/IEC 27035:2016 ISO/IEC 27035:2016. ISBN 978 0 580 79888 7 British Standards Institute, London

Bullen, C Rockart, J. (1981) A Primer on Critical Success Factors. CISR No. 69. Sloan WP No. 1220-81. www.researchgate.net/publication/...A.../e0b495213a52095190.pdf (Accessed: 23/4/14)

Burck, C,. (2005) 'Comparing Qualitative Methodologies for Systemic Research: The Use of Grounded Theory, Discourse Analysis and Narrative Analysis.' *Journal of Family Therapy (2005) Volume 27, pages 237-262*

Burton, Sir E. (2013) introductory speech. Information Assurance Advisory Council – Annual Symposium London 11/9/13

Caldwell, C., Zeltmann, S. and Griffin, K., (2012) BYOD (Bring Your Own Device) Competition Forum, 10 (2), p 117-121 Available at: https://search.proquest.com/docreview/1196914876?pq-origsite=gscholar (Accessed: 27/8/17)

Canadian Internet Policy and Public Interest Clinic. University of Ottawa Faculty of Law. (2007). *Approaches to Breach Notification*. University of Ottawa http://www.cippic.ca/sites/default/files/bulletins/BreachNotification_9jan07-web.pdf (Accessed: 8/3/12)

Cantor, M (2002) 'Telling patients the truth: a systems approach to disclosing adverse events'. *Qual Saf Health Care* 11:7-8. DOI: 10.1136/qhc.11.1.7-a

Cantor, M (2002) citing in Witman AB, Park DM, Hardin SB. *How do patients want physicians to handle mistakes?* Arch Intern Med 1996;156:2565–9.

Cantor (2002) Citing Lo, B. *Resolving ethical dilemmas: a guide for clinicians*. Baltimore: Williams & Wilkins, 1995

Caralli, R. (2004) The *Critical Success Factor Method: Establishing a Foundation for Enterprise Security Management*. Carnegie Mellon University Technical Report CMU/SEI-2004-TR-010 ESC-TR-2004-010 http://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=10429247&AN=35409248&h=6lgSiyrlVfikIrZjnQ99HmBzbUIXRhtSyqViGpxx4Rf%2FYIAZF1hFTqiCnTDDUQO%2ByS%2BjK9EXzUgPHVr1IWDP4g%3D%3D&crl=c

Cavoukian, A. (2009). Privacy *Externalities, Security Breach Notification and the Role of Independent Oversight*. The Eighth Workshop on the Economics of Information Security University College London June 24th 2009 http://www.ipc.on.ca/images/Resources/privacy_externalities.pdf

CERTNL Available at: www.cert.nl (Accessed: 28/9/12)

Chiang Hui-Ying, PhD, RN; Lin Shu-Yuan, PhD, RN; Hsu Su-Chen, MBA, RN; Ma Shu-Ching, MSN, RN. (2010) ‘Factors determining hospital nurses’ failures in reporting medical errors in Taiwan’. *Nursing Outlook* ;58:17-25. doi:10.1016/j.outlook.2009.06.001

Chichonski, P. Millar, T. Grance, T. Scarfone, K. (2002) *NIST Computer Incident Handling Guide* Revision 2. Aug 2012 http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

Choo, Raymond. (2011) The cyber threat landscape: Challenges and future research directions. *Computers and Security 30 (2011) 719-731 DOI:10.1016/j.cose.2011.08.004*

Collis, J., Hussey, R. (2009) *Business Research: A Practical Guide for Undergraduate and Postgraduate Students* (3rd Edition). Palgrove McMillan.

Cornish, P. Livingstone, D. Clemente, D. York, C. (2010). *On Cyber Warfare*. A Chatham House Report. http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r1110_cyberwarfare.pdf (Accessed: 8/3/12)

Dalkey, N. (1969) *The Delphi Method: An Experimental Study of Group Opinion.* http://www.rand.org/content/dam/rand/pubs/research_memoranda/RM5888/RM5888.pdf (Accessed: 23/4/14)

Davenport, T. Harris, J. Morison, R. (2010) Analytics *at Work*. Harvard Business Press. Boston.

Day, J,. Bobeva M,. (2005) ‘A Generic Toolkit for the Successful Management of Delphi Studies.’ *The Electronic Journal of Business Research Methodology. Volume 3 Issue 2, pp 103-116*

De Bruin, T, Rosemann M,. (2005) *Towards a Business Process Management Maturity Model* http://eprints.qut.edu.au/25194/1/25194_rosemann_2006001488.pdf (Accessed: 18/2/14)

De Bruin T, Freeze R, Kulkarni U. Rosemann M (2005) *Understanding the Main Phases of Developing a Maturity Assessment Model* http://eprints.qut.edu.au/25152/1/Understanding_the_Main_Phases_of_Developing_a_Maturity_Assessment_Model.pdf (Accessed: 18/2/14)

Denning, D, (2014) Framework and principles for Active cyber defence. *Computers and Security 40 (2014) 108-113 DOI 10.1016/j.cose.2013.11.004*

Denyer, D Tranfield, D, Van Aken, E. (2008). http://oss.sagepub.com/content/29/3/393 Organisation Studies. DOI 10.1177/0170840607088020

Dhillon, G. S. (1995*) Interpreting the Management of Information Systems Security.* PhD Faculty of Economics. University of London

Drew, M (2007) BT Technology Journal January 2007, Volume 25, Issue 1, pp 19-29 10.1007/s10550-007-0004-x

Durkheim, E. (1982). *The Rules of Sociological Method.* The Free Press. New York

Easterby-Smith, M. Thorpe, R. Lowe, A. (2003) *Management Research: An Introduction* 2nd Edition. Sage Publications. London

Easterby-Smith, M. Thorpe, R. Jackson, P. (2011) *Management Research* Third Edition. Sage Publications. London

Effective Learning Service, *An Introduction to Research and Research Methods,* (Bradford, University of Bradford, School of Management, last updated Nov 2005) http://www.brad.ac.uk/acad/management/external/els/pdf/introductiontoresearch.pdf (Accessed: 1/8/13)

Eni, G (1989) The Concept of Critical Success Factors (CSFs) as a Planning Tool for Healthcare Managers. http://ac.els-cdn.com/S0840470410613695/1-s2.0-S0840470410613695-main.pdf?_tid=60e1cede-caf1-11e3-aac0-00000aacb362&acdnat=1398262561_68f6d189371a78defaa8662e1cb38191 (Accessed: 23/4/14)

Erffmeyer, Robert C., Elizabeth S. Erffmeyer, and Irving M. Lane. "The Delphi technique: An empirical evaluation of the optimal number of rounds." *Group & Organization Management* 11.1-2 (1986): 120-128.

Einarsson, S. Brynjarsson, B. (2008). ‘Improving human factors, incident and accident reporting and safety management systems in the Seveso industry’. *Journal of Loss Prevention in the Process Industries*. DOI:10.1016/j.jlp.2008.05.004

ENISA (European Network and Information Security Agency) 2010 *Incentives and Challenges for Information Sharing in the Context of Network and Information Security*. http://www.config.fr/press/ENISA.pdf (Accessed: 1/9/13)

ENISA list of Cyber Security Strategies (www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world) (Accessed: 8/3/15)

ENISA National Cyber Security Strategies Setting the course for national efforts to strengthen security in cyberspace (May 2012) https://www.enisa.europa.eu/publications/cyber-security-strategies-paper (Accessed: 8/7/17)

Ernst and Young. (2011). *Into the Cloud, Out of the Fog*. Ernst and Young, London.

European Commission. 2007. *Availability and robustness of Electronic Communication Infrastructures.* http://ec.europa.eu/information_society/policy/nis/docs/studies/areci_study/areci_report_fin.pdf

European Commission. (2009) *Regulatory Framework for Electronic Communications in the European Union.* http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf (Accessed: 10/5/13)

European Commission. (2011) *National and European Information Sharing and Alerting System* http://www.neisas.eu/ (Accessed: 10/5/13)

European Commission (2013) Directive of the European Parliament and of the Council *concerning measures to ensure a high level of network and information security across the Union {SWD (2013) 31 Final} { SWD (2013) 32 Final}* http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1666 (Accessed: 14/9/13)

Firth-Cozens, J. (2002) 'Barriers to Incident Reporting', *Quality & Safety in Health Care. British Medical Journal* ;11:7, doi: 10.1136/qhc.11.1.7

Flaatten H, Hevroy O. (1995) 'Errors in the intensive care unit (ICU): Experience with anonymous registration'. *Acta Anaesthesiol Scand*. 1995;43:614-617.)

Flores, Waldo. Rocha, Antonsen. Egil, Ekstedt, Mathias. (2014) Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security* Volume 43 (2014) 90-110 http://dx.doi.org/10.1016/j.cose.2014.03.004

Fraser P, Moultrie J, Gregory, M. (2002) The Use of Maturity Models/Grids as a tool in assessing product development capability 0-7803-7385-5/02 http://dx.doi.org/10.1109/IEMC.2002.1038431 http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1038431

Freund, York P. "Critical Success Factors." *Strategy & Leadership* 16.4 (1988): 20-23. DOI 10.1108/eb054225

Franke, U, Brynielsson, J. (2014) Cyber Situational Awareness – A systematic review of the literature. *Computers and Security 46 (2014) 18-31 DOI 10.1016/j.cose.2014.06.008*

Garret, T and Reeves, D. (2009) 'Beliefs and Attitudes that influence reporting of clinical interventions by pharmacists'. *Journal of Pharmacy Practice and Research*. 2009 Vol 39/2. 99-103.

Gates, L. (2010) *CMU/SEI-2010-TR-037 ESC-TR-2010-102. Strategic Planning with Critical Success Factors and Future Scenarios: An Integrated Strategic Planning Framework.* Software Engineering Institute. Available at: http://www.sei.cmu.edu/reports/10tr037.pdf (Accessed: 23/4/14)

Gordon, L.A. Loeb, M.P. Sohali, T. (2003) 'A Framework for Using Insurance for Cyber Risk Management'. *Communications of the ACM.* March 2003 Vol 46 No 3 P81 to 85 DOI.10.1145/636772.636774

Great Britain. Burton, Sir E. (2008). *Report into the Loss of MOD Personal Data*. Available at: http://www.mod.uk/nr/rdonlyres/3e756d20-e762-4fc1-bab0-08c68fdc2383/0/burton_review_rpt20080430.pdf (Accessed: 13/7/12)

Great Britain CERT. Available at: www.govcertuk.gov.uk (Accessed: 8/3/12)

Great Britain. CESG (2010) *Information Assurance Maturity Model and Assessment Framework.* Available at: http://www.cesg.gov.uk/publications/Documents/iamm-assessment-framework.pdf (Accessed: 17/2/14)

Great Britain. CESG GovCERTUK. (2008). *Incident Response Guidelines*. Available at: http://www.govcertuk.gov.uk/pdfs/incident_response_guidelines.pdf (Accessed: 20/2/13)

Great Britain. (2012) CESG *IS Technical Risk Assessment Model – IS1* Available at: www.cesg.gov.uk/publications/Documents/is1_risk_assessment.pdf (Accessed: 20/2/13)

Great Britain. Civil Aviation Authority. Available at: http://www.caa.co.uk/default.aspx?catid=1425&pagetype=90&pageid=8178 (Accessed: 20/2/13)

Great Britain. Dept of Health Expert Group (2000). *An Organisation With A Memory*. The Stationary Office. ISBN 011 322441 9

Great Britain. Department of Transport (1988) *Investigation into the Kings Cross Underground Fire* D. Fennell QC Available at: http://www.railwaysarchive.co.uk/documents/DoT_KX1987.pdf (Accessed: 20/2/14)

Great Britain. Department of Transport. (1987). *MV 'Herald of Free Enterprise'. Report of court no 8074 Formal investigation.* Lord Justice Sheen. HMSO London ISBN 0 11 550828 7 Available at: http://www.maib.gov.uk/cms_resources.cfm?file=/HofFEfinal.pdf (Accessed: 4/7/13)

Great Britain. Health and Safety Executive *Definition of risk* Available at: http://www.hse.gov.uk/risk/theory/alarpglance.htm (Accessed: 1/9/13)

Great Britain. Home Office (1985) *Committee of Enquiry into Crowd Safety and Control at Sports Grounds Interim Report*. Mr Justice Popplewell HMSO Available at: http://bradfordcityfire.files.wordpress.com/2012/09/popplewell-inquiry-interim-report-bradford-city-fire.pdf (Accessed: 20/2/14)

Great Britain. Home Office (1986) *Committee of Enquiry into Crowd Safety and Control at Sports Grounds* Final *Report*. Mr Justice Popplewell HMSO Available at: http://bradfordcityfire.files.wordpress.com/2013/02/popplewell-final-report-1986.pdf (Accessed: 20/2/14)

Great Britain. HM Government (2013) Cyber *Security Organisational Standards - A call for views and evidence.* Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/132466/bis-13-659-cyber-security-organisational-standards-call-for-views-and-evidence.pdf (Accessed: 20/2/13)

Great Britain. HM Government Cabinet Office. (2008). *Data Handling Procedures in Govt. Final Report*. Available at: http://www.cabinetoffice.gov.uk/sites/default/files/resources/final-report.pdf (Accessed: 9/3/12)

Great Britain. HM Government Cabinet Office. (2010). A *Strong Britain in an Age of Uncertainty - The National Security Strategy*. Available at: www.official-documents.gov.uk ISBN 9780101795326 (Accessed: 9/3/12)

Great Britain. HM Government. (2010). *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review*. ISBN 9780101794824 Available at: http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191634.pdf?CID=PDF&PLA=furl&CRE=sdsr (Accessed: 8/3/12)

Great Britain. HM Government (2015) National Security Strategy and Strategic Defence and Security Review 2015 A Secure and Prosperous United Kingdom. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf (Accessed:5/8/17)

Great Britain. HM Government (2013) *Cyber Security Information Sharing Partnership* Available at: https://www.gov.uk/government/news/government-launches-information-sharing-partnership-on-cyber-security (Accessed: 10/5/13)

Great Britain. HM Government. Cabinet Office. (2011) *The UK Cyber Security Strategy, Protecting and Promoting the UK in a Digital World* Available at: http://www.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategy-final.pdf Accessed: Nov 25th 2012 Note now moved to https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf (Accessed: 28/6/17)

Great Britain. HM Government Cabinet Office (2012) *Security Policy Framework* Available at: http://www.cabinetoffice.gov.uk/sites/default/files/resources/HMG_Security_Policy_Framework-v8_April-2012.pdf Accessed: (20/2/13)

Great Britain HM Government Cabinet Office (2013) *Security Policy Framework* Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/255910/HMG_Security_Policy_Framework_V11.0.pdf (Accessed: 20/2/14)

Great Britain HM Government Cabinet Office (2014) *Security Policy Framework* Available at: https://www.gov.uk/government/publications/security-policy-framework (Accessed: 27/6/17)

Great Britain, National Crime (2014) Agency *Strategic Assessment of Serious and Organised Crime* Available at: http://www.nationalcrimeagency.gov.uk/publications/207-nca-strategic-assessment-of-serious-and-organised-crime/fileNational Strategic Assessment 1st of May 2014, p4 (Accessed: 8/3/15)

Great Britain, National Crime Agency (2017) New assessment warns industry that cyber criminals are imitating nation state attacks. Available at; http://www.nationalcrimeagency.gov.uk/news/1043-new-assessment-warns-industry-that-cyber-criminals-are-imitating-nation-state-attacks (Accessed: 5/8/17)

Hagen, J . (2009). 'Human Relationships A never ending security education challenge'. *IEEE Security and Privacy* . July/August 2009 (vol. 7 no. 4) pp. 65-67__Available at: _http://doi.ieeecomputersociety.org/10.1109/MSP.2009.92

Haines T, Cornwell P, Fleming J, Varghese P, Gray l. (2008). 'Documentation of 'in hospital' falls on incident reports: Qualitative investigation of an imperfect process'. *British Medical Council. BMC Health Services Research*. 2008:8:254 DOI:10.1186/1472-6963-8-254

Hasson F, Keeney S, McKenna H, (2000) Research guidelines for the Delphi survey technique) *Journal of Advanced Nursing 32(4), 1008±1015*
DOI: 10.1046/j.1365-2648.2000.t01-1-01567.x

Henin S . (2008). *Control System Cyber Incident Reporting Protocol. Technologies for homeland Security* 2008 IEEE Conference DOI:10.1109/THS.2008.4534497

Hood, C. (2002). *The Risk Game and the Blame Game* Available at: www.onlinelibrary.wiley.com/doi/10.1111/1477-7054.00085/pdf

Horne, N. (1995) Information as an Asset - The Board Agenda. *Computer Audit Update Volume 1995, Issue 9, September 1995, Pages 5-11* doi.org10.10160960-2593(95)90246-5

Hove, C and Tarnes, M (2013) *Information Security Incident Management An Empirical Study of Current Practice.* Master of Science in Communication Technology. Department of Telematics. Norwegian University of Science and Technology

Hubbard, D, and Evans, D. (2010) Problems with scoring methods and ordinal scales in risk assessment. *IBM Vol 54 No 3 Paper 2* DOI:10.1147/JRD.2010.2042914

Hughes, J, and. Jones, S,. (2003) '*Reflections on the use of Grounded Theory in Interpretive Information Systems Research*.
Available at:
http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1065&context=ecis2003

Humphrey, M. (2004) *Monitoring, Response and Alerting Capability of a Secure Community: A Strategic Approach.* MSc - University of Westminster (Not publicly available for security reasons)

Hurtzburg A.M. (2007). 'Risk Management and the Limitations of Measurement'. *Published in Statistics, Science and Public Policy XII: Measurement, Risk and Society, proceedings of Conference on Statistics, Science and Public Policy Measurement, Risk and Society, Herstmonceux Castle 18-21 April 2007, A.M. Herzberg editor*. http://john-adams.co.uk/wp-content/uploads/2008/11/risk-management-and-the-limitations-of-measurement.pdf (Accessed: 8/3/12)

Hutchinson, A. Young, T.A. Cooper, K.L. McIntosh, A. Karnon, J.D. Scobie, S. and Thomson, R.G. (2007) 'Trends in healthcare incident reporting and relationship to safety and quality data in acute hospitals: results from the National Reporting and Learning System'. *Quality and Safety in Health Care* 2009;18:5–10. doi:10.1136/qshc.2007.022400

Information Assurance Advisory Council and National Infrastructure Security Coordination Centre. (2001) *Sharing is Protecting: A review of Information Sharing.* Available at: http://www.warp.gov.uk/downloads/IAAC%20NISCC%20Sharing%20is%20Protecting%20v21.pdf last downloaded 8/3/12

Information Security Forum tools. Available at: https://www.securityforum.org/whatwedo/publictools/ (Accessed: 18/7/12)

Jacobson, N, Gewurtz, R, and Haydon, E (2007) Ethical Review of Interpretive Research: Problems and Solutions *Ethics and Human Research* Vol 29, No 5 p 1-8

Jang-Jaccard, J Nepal, S. (2014) A survey of emerging threats in cybersecurity. *Journal of computer and System Sciences. 80 (2014) 973-993. DOI 10.1016/j.jcss.2014.02.005*

Jenkins A, Milton, *Research Methodologies and MIS Research*. Indiana University USA Available at: http://tricycle.csisdmz.ul.ie/staff/BF/phd-seminar-series/Jenkins.pdf (Accessed: 18/2/14)

Jensen, M. C. (1993), The Modern Industrial Revolution, Exit, and the Failure of Internal Control Systems. *The Journal of Finance*, 48: 831–880. doi:10.1111/j.1540-6261.1993.tb04022.x Available at: http://onlinelibrary.wiley.com/enhanced/doi/10.1111/j.1540-6261.1993.tb04022.x/

Jesson,J,. Matheson, L, and Lacey, F. (2011) Doing *your Literature Review: Traditional and Systematic Techniques*. Sage publications, London

Johnston, C (2015) TalkTalk customer data at risk after cyber-attack on company website. *The Guardian October* 2015 Available at: https://www.theguardian.com/business/2015/oct/22/talktalk-customer-data-hackers-website-credit-card-details-attack (Accessed: 9/7/17)

Jones, N, O'Neill, L-J, (2017) The Profession Understanding Careers and Professionalism in Cyber Security Available at: https://www.iaac.org.uk/wp-content/uploads/2017/06/2017-03-06-iaac-cyber-profession-final.pdf (Accessed 29/7/17)

Jones, S, Kirchsteiger, C, Bjerke, W (1999) The importance of near miss reporting to further improve safety performance. *Journal of Loss Prevention in the Process Industries* Volume 12 (1999) 59–67 Available at: https://doi.org/10.1016/S0950-4230(98)00038-2

Jugdev, K, Thomas, J. (2002) Project Management Maturity Models: The Silver Bullets of Competitive Advantage? *The Project Management Institute* 2002, Vol 33, No 4. 4-14 Available at: http://dspace.ucalgary.ca/bitstream/1880/44250/1/2002%20PMJ%20PM%20maturity%20models.pdf (Accessed: 22/2/14)

Kahneman, D. Tversky, A. (1977). *Intuitive Prediction. Biases and Corrective Procedures. Decision Research*. A Branch of Perceptronics Technical Report PTR 1042-77-6. Available at: http://www.dtic.mil/dtic/tr/fulltext/u2/a047747.pdf (Accessed 18/2/13)

Kessels-Habraken, M, Van der Schaaf, T, De Jonge, J and Rutte, C. (2010) Defining near misses: Towards a sharpened definition based on empirical data about error handling processes. *Social Science & Medicine* Volume 70 (2010) 1301-1308. DOI:10.1016/j.socscimed.2010.01.006

Keohane, R. Nye, J, (1998) Power and Independence in the Information Age. Foreign Affairs; Sep/Oct 1998; 77, 5; Alumni - Research Library pg. 81 Available at: http://s3.amazonaws.com/academia.edu.documents/30534624/power_and_interdependence.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1499597370&Signature=7HwyNTnigGD0n3BuWneat8uuOKw%3D&response-content-disposition=inline%3B%20filename%3DPower_and_interdependence_in_the_informa.pdf (Accessed: 9/7/17)

Kim, C (2016) Granting standing in Data Breaches: The seventh circuit paves the way towards a solution to the increasingly pervasive data breach problem. Available at: https://ssrn.com/abstract=2735897 Accessed: 6/8/17)

Kingston M.J, Evans S. Smith B. Berry J. (2004) 'Attitudes of doctors and Nurses towards incident reporting: a qualitative analysis'. *The Medical Journal of Australia* Volume 181 No 1 36-39 5th July 2004 (Accessed: 21/11/10)

Kotulic, A, Clark, J. (2004) 'Why there aren't more information security research studies' *Information and Management* Volume 41 (2004) 597-607. DOI:10.1016/j.im2003.08.001

Lagazio, m, Sherif n, Cushman, M (2014) A multilevel approach to understanding the impact of cyber crime on the financial sector. *Computers and Security* Volume 45 p58-74 http://dx.doi.org/10.1016/j.cose.2014.05.006 (Accessed: 15/11/16)

Layne, K and Lee Jungwoo. (2001) Developing fully functional E-government: A four stage Model. *Government Information Quarterly* Volume 18 (2001) 122–136 Available at:http://www.ekt.gr/content/img/product/5593/Government%20Information%20Quarterly%3B%2018%20(2)%202001,%20p.122-36.pdf (Accessed: 23/4/14)

Lawton, R Parker, D. (2002) 'Barriers to incident reporting in a healthcare system'. *Quality Safety in Health Care* 2002 Volume 11:15-18. DOI:10.1136/qhc.11.1.15

Leidecker, J and Bruno, A. (1984) Identifying and Using Critical Success Factors *Long Range Planning*. Vol. 17, No. 1, pp. 23 to 32 1984 http://dx.doi.org/10.1016/0024-6301(84)90163-8

Linstone, H and Turoff, M (1975) *The Delphi Method Techniques and Applications* Addison-Wesley Pub. Co., Advanced Book Program, 1975 ISBN 0201042940, 9780201042948

Lipsky, John (1980) *Street Level Bureaucracy* https://books.google.co.uk/books?hl=en&lr=&id=QN4FBAAAQBAJ&oi=fnd&pg=PA389&dq=lipsky+1980+street+level+bureaucracy+theory+&ots=D6jBvMxoj6&sig=dCahNFP6wm8cdQn3UbYGoFmvA2o#v=onepage&q=lipsky%201980%20street%20level%20bureaucracy%20theory&f=false (Accessed: 30/7/17)

Lloyds List http://www.rmg.co.uk/researchers/library/research-guides/lloyds/lloyds-list-brief-history (Accessed: 10/5/13)

Lockridge, B, Barnett, R (2011) Cyber Defence University of Pittsburgh eleventh Annual Freshman conference paper no. 2193 (paper copy)

Lukic, D. Margaryan, A. and Littlejohn, A. (2010). 'How organisations learn from safety incidents: a multi-faceted problem'. *The Journal of workplace learning* Vol 22 No 7 2010 p 428- 450. doi: 10.1108/13665621011071109

Luokkala, P. Virrantaus, K, (2014) Developing information systems to support situational awareness and interaction in time-pressuring crisis situations. *Safety Science* Volume 63 P 191-203 http;//dx.doi.org/10.1016/j.ssci.2013.11.014

MacAskill and Syal (2017) Cyber-attack on the UK parliament: Russia is suspected culprit.

The Guardian (2017) https://www.theguardian.com/politics/2017/jun/25/cyber-attack-on-uk-parliament-russia-is-suspected-culprit (Accessed: 5/8/17)

Mahajan R.P. (2010) 'Critical Incident Reporting and Learning'. *British Journal of Anaesthesia*. 2010 Vol 105/1 69-75. DOI:10.1093/bja/aeq133

Mendosa, Alejandro Marius, María Pérez, Anna C. Grimán Critical success factors for a customer relationship management strategy. *Information and Software Technology* 49 (2007) 913–945 http://ac.els-cdn.com/S0950584906001352/1-s2.0-S0950584906001352-main.pdf?_tid=8a9e8b6c-caf2-11e3-83e6-00000aab0f26&acdnat=1398263060_c365973bcc1adf09820dad7f5fc9a768 doi:10.1016/j.infsof.2006.10.003

Messenger, M. (2005). *Why Would I tell You? Perceived Influences for Disclosure Decisions by Senior Professionals in Inter Organisational Sharing Forums.* MSc University of London Available at: http://www.warp.gov.uk/downloads/Why-would-I-tell-you.pdf (Accessed: 2/8/13)

Mettler, T. Rohner, P. (2009) 'Situational Maturity Models as Instrumental Artifacts for Organizational Design*' DESRIST'09 May 7-8, 2009, Malvern PA, USA ACM 978 – 1 – 60558-408-9/09/05 DOI:10.1145/1555619.1555649*

McNeill, P., (1990) *Research Methods.* London. Routledge

Mitnick, K., 2002: *The Art of Deception*. USA. Wiley

Moga, C,. Guo, B,. Schopflocher, D,. and Harstall, C,. (2012) Development of a Quality Appraisal Tool for Case Series Studies using a Modified Delphi

Technique. Available at: http://www. ihe.ca/documents/Case% 20series% 20studies% 20using% 20a% 20modified% 20Delphi% (Accessed: 29/7/17)

Moody, D, Walsh. P (1999) Measuring the Value of Information An Asset Valuation Approach *European Conference on Information Systems* (ECIS'99) http://wwwinfo.deis.unical.it/~zumpano/2004-2005/PSI/lezione2/ValueOfInformation.pdf (Accessed: 9/7/17)

National Health Service. NHS Commissioning Board. *Serious Incident Framework 2015 Supporting learning to prevent recurrence.* https://improvement.nhs.uk/uploads/documents/serious-incidnt-framwrk.pdf (Accessed: 27/6/17)

National Aeronautics and Space Administration – NASA. (2009) *Apollo 13 "Houston we've had a problem……"* https://www.nasa.gov/mission_pages/apollo/missions/apollo13.html (Accessed: 5/8/17)

Netherlands CERT Available at: www.govcert.nl (Accessed: 28/9/12)

Nguyen QT, Weinberg J, Hilborne LH. (2005) Physician Event Reporting: Training the Next Generation of Physicians. Cited in: Henriksen K, Battles JB, Marks ES, et al., editors. *Advances in Patient Safety: From Research to Implementation* (Volume 4: Programs, Tools, and Products). Rockville (MD): Agency for Healthcare Research and Quality (US); 2005 Feb. Available from: http://www.ncbi.nlm.nih.gov/books/NBK20579/ (Accessed: 8/7/12)

Nili, Y. Harvard Law School Forum on Corporate Governance and Financial Regulation 2014 http://corpgov.law.harvard.edu/2014/12/24/top-10-topics-for-directors-in-2015/ post of predicted top Ten Topics for Directors 2015 http://cdn.akingump.com/images/content/3/4/v2/34387/CORPORATE-ALERT-121214-v6.pdf (Accessed: 11/7/15)

Nulty, D (2008) The adequacy of response rates to online and paper surveys: what can be done? *Assessment & Evaluation in Higher Education* Vol. 33, No 3 June 2008, 301-314 DOI: 10.1080/02602930701293231

Olsen, S Neale, G Schwab, K Psaila, B Patel, t Chapman, J Vincent, C (2006 Hospital staff should use more than one method to detect adverse events and potential adverse events: incident reporting, pharmacist surveillance and local real-time record review may all have a place) *Qual Saf Health Care 2007*; 16 40-44 doi 10.1136/qshc. 2005.017616

Onwuegbuzie, A J., and Leech. N,. (2005) "On becoming a pragmatic researcher: The importance of combining quantitative and qualitative research methodologies." *International Journal of Social Research Methodology* 8.5 (2005): 375-387. http://dx.doi.org/10.1080/13645570500402447

Parasuraman, A 2000, 'Technology Readiness Index (Tri): A Multiple-Item Scale to Measure Readiness to Embrace New Technologies' *Journal of Service Research*, vol 2, no. 4, pp. 307-320. DOI: 10.1177/109467050024001

Parker, D. (2006). Making the Case for replacing risk based security. *Information Systems Security Association ISSA Journal* May 2006 (no page numbers) http://www.issa.org/Library/Journals/2006/May/Parker%20-%20Replacing%20Risk-Based%20Security.pdf (Accessed: 8/3/12)

Parker, D. (2008). A Diligence-Based Idealized Security Review. *Information Systems Security Association ISSA Journal* January 2008 35-40 http://www.issa.org/Library/Journals/2008/January/Parker-A%20Diligence-Based%20Idealized%20Security%20Review.pdf (Accessed: 8/3/12)

Parker, D. (2009). Positive and Negative Security Methods. *Information Systems Security Association ISSA Journal* December 2009 31-38 https://www.issa.org/Library/Journals/2009/December/Parker-Positive%20and%20Negative%20Security%20Methods.pdf Accessed: (8/3/12)

Parker, D. (2010). Our Excessively Simplistic Information Security Model and How to Fix It. *Information Systems Security Association ISSA Journal* July 2010 12-21. http://www.issa.org/images/upload/files/Parker-Simplistic%20Information%20Security%20Model.pdf (Accessed: 8/3/12)

Perry, C. (1998) Processes of a case study methodology for postgraduate research in marketing. *European journal of Marketing* Vol. 32 No 9/10, 1998 pp785-802 https://doi.org/10.1108/03090569810232237

Perry, W (Perri6), Moffat, J, (2004), *Information Sharing Amongst Military Headquarters – The effects on Decision Making.* Rand Corporation www.rand.org/pubs/monographs/2004/RAND_MG226.pdf (Accessed: 9/3/12)

Perri 6, Bellamy C, Raab, C. (2004). *Data Sharing and Confidentiality: spurs, barriers and theories.* Political Studies Association Conference, University of Lincoln April 5-8, 2004 1-20 Available at: https://s3-eu-west-1.amazonaws.com/esrc-files/.../yGqKfSOLG0KrkQaLAxdtDw.pd (Accessed: 30/7/17)

Pfleeger, S , Caputo, D. (2012) Leveraging behavioural science to mitigate cyber security. *Computers and Security 31 (2012) 597-611* DOI. 10.1016/j.cose.2011.12.010

Perrow, C. 1984. *Normal Accidents Living with High Risk Technologies*. Basic Books, New York

Perrow, C. 2007. *The Next Catastrophe*. Princetown University Press. New Jersey

Pollitt, M, (1998) Cyber Terrorism Fact or Fancy? *Computer Fraud and Security* 1998 Vol 2 p 8-10 https://doi.org/10.10.1016/S1361-3723(00)87009-8 Available at: www.sciencedirect.com/science/article/pii/S1361372300870098 (Accessed: 27/8/17)

Ponemon Institute and Symantec. (2010). 2010 *Annual Study: U.K. Cost of a Data Breach.* http://www.symantec.com/content/en/us/about/media/pdfs/UK_Ponemon_CODB_2010_031611.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Mar_worldwide_costofdatabreach (Accessed: 4/7/13)

Poon, P, Wagner C. (2001) Critical Success Factors revisited: success and failure cases of information systems for senior executives *Decision Support Systems* volume 30 2001 393–418 http://ac.els-cdn.com/S0167923600000695/1-s2.0-S0167923600000695-main.pdf?_tid=3a88cae6-caef-11e3-927c-00000aab0f6c&acdnat=1398261638_6cb7cedd2602a2b4dbfd45edbd263dca https://doi.org/10.1016/S0167-9236(00)00069-5

Power, D (2013) Mobile decision support and business intelligence: an overview. *Journal of Decision Systems* vol. 22 No 1, p4-9 www.tandfonline.com/doi/pdf/10.1080/12460125.2012.760267?needAccess=true (Accessed: 27/8/17)

Poynter, K. (2008). *Review of information security at HM Revenue and Customs Final Report.* http://webarchive.nationalarchives.gov.uk/+/http:/www.hm-treasury.gov.uk/media/0/1/poynter_review250608.pdf (Accessed: 13/7/12)

PWC. (2011) *Delusions of Safety The Cyber Savvy CEO Getting to grips with today's growing cyber threats*. www.pwc.co.uk/cybersavvyceo (Accessed: 8/3/12)

PWC. (2012) *Information Security Breaches Survey 2012: Technical Report.* http://www.pwc.co.uk/en_UK/uk/assets/pdf/olpapp/uk-information-security-breaches-survey-technical-report.pdf (Accessed: 4/7/13)

PWC. (2012) *Information Security Breaches Survey 2012: Executive Summary.* http://www.pwc.co.uk/en_UK/uk/assets/pdf/olpapp/uk-information-security-breaches-survey-executive-summary.pdf (Accessed: 4/7/13)

RAND Corporation. *Origin of the Delphi Technique* http://www.rand.org/topics/delphi-method.html Accessed: (23/4/14)

Rail Safety and Standards Board (RSSB). (2011). Final *Report Independent Review of RIDDOR reporting by Network Rail and its Contractors*. http://www.rssb.co.uk/SiteCollectionDocuments/RIDDOR%20Review.pdf (Accessed: 8/3/12)

Reason, J (1990). *Human Error*. Cambridge University Press. 1990.

Reason, J. (2000). 'Human Error models and Management'. Volume 172 June 2000 WJM 393 originally published in the *British Medical Journal* 2000; Volume 320;768-770 doi:10.1136!bm}.320.7237.768.

Regan, P. (2009). 'Federal Security Breach Notifications: Politics and Approaches'. *Berkeley Technology Law Journal* Vol 24:3 2009 1103-1132 http://dx.doi.org/doi:10.15779/Z38NM42

Robinson, N. Valeri, L. Cave, J. Starkey, T. Graux, H, Creese, S. Hopkins, P.. (2010). *The Cloud: Understanding the Security, Privacy and Trust Challenges.* Available at: http://www.rand.org/content/dam/rand/pubs/technical_reports/2011/RAND_TR933.pdf (Accessed: 4/7/13)

Robson, C. (2011) *Real World Research*. Wiley and Sons, Chichester, W. Sussex

Romanosky, S. Telang, R. Acquisti, A. (2008). Do Data Breach Disclosure Laws Reduce Identity Theft? (Updated). Heinz School of Public Policy and

Management. Carnegie Mellon University. (Updated) (September 16, 2008*). Journal of Policy Analysis and Management*, Vol. 30, No. 2, pp. 256-286, 2011. Available at SSRN: http://ssrn.com/abstract=1268926 (Accessed: 8/3/12)

Romanosky, S and Acquisti, A. (2009). 'Privacy Costs and Personal Data Protection: Economic and Legal Perspectives'. *Berkeley Technology Law Journal*, Vol. 24, No. 3, 2009 (December 12, 2009). Berkeley Technology Law Journal, Vol. 24, No. 3, 2009. Available at SSRN: http://ssrn.com/abstract=1522605 (Accessed: 8/3/12)

Romanosky, S, Acquisti, A and Sharp, R. (2010). '*Data Breaches and Identity Theft: When is Mandatory Disclosure Optimal?'* (August 15, 2010). *TPRC 2010*. Available at SSRN: http://ssrn.com/abstract=1989594 (Accessed: 8/3/12)

Romanosky, S. Hoffman, D. A. and Acquisti, A. (2012). 'Empirical Analysis of data Breach Legislation'. *The Journal of workplace learning* Vol 22 No 7 2010 p 428-450. doi: 10.1108/13665621011071109 Emerald Publishing group.

Rooksby, J, Gerry, R, Smith, A (2007) 'Incident reporting schemes and the need for a good story' I*nternational journal of medical informatics* 76S (2007) S205–S211. http://ac.els-cdn.com/S1386505606001407/1-s2.0-S1386505606001407-main.pdf?_tid=dc4bec2e-4236-11e3-8e95-00000aacb35f&acdnat=1383229094_43af3e003189ac7e1a2bde2e3d2e07bf doi:10.1016/j.ijmedinf.2006.05.019

Room, S. (2009). *Butterworths Data Security Law and Practice*. Lexis Nexis. London

Rowe, G, Wright, G, Bolger, F. (1991) Delphi A Re-evaluation of Research and Theory. *Technological Forecasting and Social Change* Volume 39, 235-251 https://doi.org/10.1016/0040-1625(91)90039-I (Accessed: 25/5/17)

Rumsfield, D http://www.nato.int/docu/speech/2002/s020606g.htm (Accessed: 31/10/13)

Schectman J.M., M.D., M.P.H. Pews-Ogan M.L. (2006) 'Physician Perception of Hospital Safety and Barriers to Incident Reporting'. *M.D Journal on Quality and Patient Safety* June 2006 Vol 32 No 6. 337-343 (Paper Document)

Schein, E. (1992) *Organisational Culture and Leadership* . Joey-Bass. San Francisco, California

Shekelle, P (2002). 'Why don't physicians enthusiastically support quality improvement programmes?' *Quality and Safety in Health Care*;11:6 doi:10.1136/qhc.11.1.6

Scheurich, J. (1997) *Research Method in the Postmodern*. Biddles, Guildford

Schiffman, M. (2011). *The Common Vulnerability Reporting Framework.* http://www.icasi.org/docs/cvrf-whitepaper.pdf (Accessed: 8/3/12)

Schneier, B. (2008). *Schneier on Security*. Wiley Publishing. Indianapolis

Shakleton P, Fisher J, Dawson L. (2004*) Evolution of Local Government E - Services; the applicability of e-business Maturity Models. Proceedings of the 37th Hawaii International conference on System Sciences* – 2004 http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1265308 (Accessed: 22/2/14)

Singh, S. (1999). *The Code Book The Secret History of Codes and Code-Breaking.* Fourth Estate, Harper Collins. London

Skulmoski G, Project Maturity and competence interface. (2001) *Cost Engineering* Vol 43 no 6 p 11-19. https://extranet.cranfield.ac.uk/ehost/pdfviewer/,DanaInfo=eds.b.ebscohost.com+pdfviewer?sid=1429b216-68cd-4dc2-a149-c7909f96faae%40sessionmgr114&vid=2&hid=104 (Accessed: 23/4/14)

Skulmoski, G., Hartman, F,. Krahn, J,. 'The Delphi Method for Graduate Research'. *Journal of Information Technology Education* Volume 6, 2007 1-21 *(*Accessed: 7/2/14)

Snow, R, Snow, M (2007) Ethics in the Information exploitation and manipulation age. *Campus Wide Information Systems*, Vol. 24 Issue 3, pp.207-216Available at: http://www.emeraldinsight.com/doi/pdfplus/10.1108/10650740710762248 (Accessed: 3/8/17)

Smartcitiescouncil *Definition of a smart City* http://smartcitiescouncil.com/smart-cities-information-center/definitions-and-overviews?page=1 (Accessed: 27/6/17)

Smith and Elliot (1999), Firth Cozens (2000) and Wason (1960) which were published in the document Great Britain. *Department of Health: Organisation with Memory* (2000). The Stationary Office ISBN 0-11-322441-9

Soderberg, J. Grankvist, K. Brulin, C Wallin, O. (2009) 'Incident Reporting Practices in the pre-analytical phase: Low reported frequencies in the primary health care setting'. *Scandinavian Journal of Clinical and Laboratory Investigation* 2009 Vol 69/7 731-735. DOI:10.3109/00365510903007018

Solms, R and Niekerk, J. (2013) From information security to cyber security. *Computers and Security* Volume 38 p97-102 http://dx.doi.org/10.1016/j.cose.2013.04.004

Sommer, P. (2012). *Digital Evidence, Digital, Investigations and E-Disclosure: A Guide to Forensic Readiness for Organisations, Security Advisers and Lawyers.* http://www.iaac.org.uk/_media/DigitalInvestigations2012.pdf (Accessed: 22/3/12)

Stahl, B, (2005) A Critical View of the Ethical Nature of Interpretative Research: Paul Ricceur and the Other. *European Conference on Information Systems* ECIS Proceedings p.29 http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1002&context=ecis2005 (Accessed:8/8/17)

Sveen, F. Sarriegi J,. Rich E,. Gonzalez, J. (2007) 'Toward viable Information Security Reporting systems', *Information Management & computer Security, Vol 15* Iss 5 pp. 408 – 419 http://dx.doi.org/10.1108/09685220710831143

United States. Department of Commerce. Mell, P. Grace, T. (2011) NIST *definition of cloud computing* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (Accessed: 8/3/15)

Taleb, N (Kindle edition 2011) *The Black Swan: The Impact of the Highly Improbable*. E book Amazon www.amazon.co.uk D01-5676917-6889345

Tamuz, M. and Thomas, E. J. (2006), Classifying and interpreting threats to patient safety in hospitals: insights from aviation. J. Organiz. Behav., 27: 919–940. doi: 10.1002/job.419

Taxis, K. Gallivan, S. Barber, N. Franklin, B.D. (2005). *Can the Heinrich ratio be used to predict harm from medication errors?* Report to the Patient Safety Research Programme (Policy Research Programme of the Department of Health) originally on http://eprints.pharmacy.ac.uk/764/1/BarberMedication_Errors.pdf (Accessed: 6/7/2012) now on http://discovery.ucl.ac.uk/78901/1/BarberMedication_Errors.pdf (Accessed: 29/7/17)

Taylor, R (2014) Sony Pictures computer system hacked in on line attack Available at: http://www.bbc.co.uk/news/technology-30189029 (Accessed: 9/7/17)

Throckmorton, T. Etchegaray, J. (2007). 'Factors Effecting Incident Reporting by Registered Nurses: The relationship of Perceptions of the Environment for Reporting Errors, Knowledge of the Nursing Practice Act and Demographics on Intent to Report Errors'. *Journal of Perianesthesia.* 2007 Vol 22/6 400-412. DOI:10.1016/j.jopan.2007.09.006

Tighe, C, Woloshynowych, M, Brown, R, Wearsa, B, Vincent, C (2006*). Incident reporting in one UK accident and emergency department.* Accident and Emergency Nursing (2006) 14, 27-37 DOI:10.1016/j.aeen.2005.10.001

Toft, B and Reynolds, S., (1999): *Learning from disasters - a management approach.* Leicester. Perpetuity Press.

TØndel, I, Line, M, Jaatun, M (2014) Information security incident management: Current practice as reported in the literature. Computers and Security Volume 45 (2014) 42-57 http://dx.doi.org/10.1016/j.cose.2014.05.003

United States. Department of homeland Security (2014) *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)* Available at: http://energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf (Accessed: 18/2/14)

United States. Department of Homeland Security. (2009). *Cybersecurity Roadmap* Available at: http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf (Accessed: 8/3/12)

United States. Whitehouse Press Office. Available at: http://www.whitehouse.gov/the-press-office/2013/02/12/*executive-order-improving-critical-infrastructure-cybersecurity* (Accessed: 13/4/13)

Venkatesh, Viswanath and Thong, James Y.L. and Xu, Xin, (2012)Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology (February 9, 2012). *MIS Quarterly, Vol. 36, No. 1, pp. 157-178, 2012*. Available at SSRN: https://ssrn.com/abstract=2002388 (Accessed: 9/7/17)

Verizon. (2012). *Verizon data breach investigation report*. Available at: http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf (Accessed: 6/7/12)

Verizon (2017) *Verizon Data Investigation Breach Report* Available at: www.verizonenterprise.com/verizon-insights-lab/dbir/2017/ (Accessed:20/8/17)

Voss, M. Wagner, K. 2010. Learning from (small) disasters. *National Hazards* (2010) Vol 55: 657-669. DOI: 10.1007/s1 1069-010-9498-5

Waring, J. (2005). Beyond Blame: cultural barriers to medical incident reporting. Social Science & Medicine 60 (205) 1927-1935. DOI:10.1016/j.socsimed.2004.08.055

Webb, j, Ahmad, A, Maynard, S, Shanks, G (2014) *A situational awareness model for information security risk management.* Computers & Security 44 (2014) 1-15 DOI: 10.1016/j.cose.2014.04.005

Wiant, T. 2005. *Information security policy's impact on reporting security* incidents Computers & Security (2005) 24, 448-459 doi:10.1016/j.cose.2005.03.008

Wiik J, Gonzalez, J. Kossakowski, K. (2005*) Limits to Effectiveness in Computer Security Incident Response Teams.* www.cert.org/archive/pdf/Limits-to-CSIRT-Effectiveness.pdf (Accessed: 9/3/12)

Wilde Gerald J S, 2008 'Risk homeostasis theory: an overview. Injury prevention' 1998;4:89-91 *Inj Prev*1998;4:89-91 doi:10.1136/ip.4.2.89

Willcocks, L, Margetts, H, (1993), 'Risk Assessment and Information Systems', *European Journal of Information Systems*, Vol 3, No 2, pp 127-137 (Accessed: 28/10/13)

Williams, M. May, T. (2000) *Introduction to the Philosophy of Social Research.* Routledge. London

Yin, R. (1981) The Case Study Crisis: Some Answers. *Administrative Science Quarterly 1981,* Volume 26No1 pp 58-65 DOI: 10.2307/2392599

Yin, R. (2014) *Case Study Research Design and Methods.* Sage California USA

GLOSSARY

Term	Description of Term
Bring Your Own Device (BYOD)	Employees are more and more likely to want to organize their personal lives using a smart telephone. They bring this expectation to the workplace and want to use their telephones to organize their work life too. Available at: https://search.proquest.com/docreview/1196914876?pq-origsite=gscholar (Accessed: 27/8/17)
CARO	Computer Antivirus Research Organisation http://www.caro.org/naming/scheme.html (Accessed: 5/7/15)
Candour	Any patient harmed by the provision of a healthcare service is informed of the fact and an appropriate remedy offered, regardless of whether a complaint has been made or a question asked about it. Page 8 Regulation 20: Duty of Candour – Information for providers Care Quality Commission March 2015 http://www.cqc.org.uk/content/regulation-20-duty-candour Accessed: 15/7/15
CESG Certified Consultancy Scheme	CESG's approach to assessing the services provided by consultancies and confirming that they meet CESG's standards. This approach replaces the CESG Listed Advice Scheme (CLAS), which focussed on individual consultants. Certified Consultancy builds on the strength of CLAS but certifies the competence of suppliers to deliver a wider and more complex range of cyber security consultancy services to both the public and private sectors. https://www.cesg.gov.uk/servicecatalogue/service_assurance/consultancy/Pages/consultancy.aspx (Accessed: 11/7/15)
CESG Certified Professionals CCP	The CESG Certified Professional (CCP) scheme has been developed to address the growing need for specialists within the cyber security profession and is building a community of recognised professionals in both the UK public and private sectors. CCP has been acknowledged as HMG's standard for cyber security professionals http://www.cesg.gov.uk/awarenesstraining/certified-professionals/Pages/index.aspx (Accessed: 11/7/15)
Cyber security Information Sharing Partnership (CiSP)	The Cyber-security Information Sharing Partnership (CiSP), part of CERT-UK, is a joint industry government initiative to share cyber threat and vulnerability information in order to increase overall situational awareness of the cyber threat and therefore reduce the impact on UK business. CiSP allows members from across sectors and organisations to exchange cyber threat information in real time, on a secure and dynamic environment, whilst operating within a framework that protects the confidentiality of shared information. https://www.cert.gov.uk/cisp/ (Accessed: 2/5/15)
Cloud	The cloud definition is described in NIST Special Publication 800-146 Sept 2011. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential

	characteristics, three service models, and four deployment models. Available at: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (Accessed: 8/3/15.)
Cyberspace	The computers, networks, programs and data which make up the information infrastructure Pollitt, M, (1998) Cyber Terrorism Fact or Fancy? *Computer Fraud and Security* 1998 Vol 2 p 8-10 https://doi.org/10.10.1016/S1361-3723(00)87009-8 Available at: www.sciencedirect.com/science/article/pii/S1361372300870098 (Accessed: 27/8/17)
Digital by Default	Digital by Default. Government digital Strategy: December 2013 'By digital by default, we mean digital services that are so straightforward and convenient that all those who can use them will choose to do so whilst those who can't are not excluded.' https://www.gov.uk/government/publications/government-digital-strategy/government-digital-strategy. (Accessed:5/7/15)
Employee Risk	Employee risk is defined as counterproductive behaviour, whether inadvertent, negligent or malicious, that can cause harm to an organisation. http://www.cpni.gov.uk/Documents/Publications/2012/2012021-homer.pdf (Accessed: 11/7/15)
Financial Conduct Authority	FCA Financial Conduct Authority. Its oversight includes data security "Customer data protection is a serious issue. 'You [referring to those subject to its oversight] are responsible for securing your customer data and protecting it from fraudsters'. https://www.fca.org.uk/firms/financial-crime/data-security (Accessed: 30/7/17)
HIPAA	The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, was enacted on August 21, 1996. Sections 261 through 264 of HIPAA require the Secretary of HHS to publicize standards for the electronic exchange, privacy and security of health information. Collectively these are known as the *Administrative Simplification* provisions. The US Department of Health and Human Services (HHS) https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (Accessed: 30/7/17)
HoMER	Holistic management of Employee Risk – HoMER guidance to help manage the risk of employees' behaviour damaging business. Http://www.cpni.gov.uk/advice/Personnel-security1/homer/ (Accessed: 7/7/15)
Information Exchanges.	Sharing of information about the risks facing networks is beneficial to both government and industry. CPNI facilitates 'information exchanges' which allow one company to learn from the experiences, mistakes and successes of another, without fear of exposing company sensitivities. - See more at: http://www.cpni.gov.uk/about/Who-we-work-with/Information-

	exchanges/#sthash.thSdjpSC.dpuf (Accessed: 11/7/15)
Information Sharing and Analysis Centres - ISACs	ISACs are trusted entities established by Critical Infrastructure Key Resource (CI/KR) owners and operators to provide comprehensive sector analysis, which is shared within the sector, with other sectors, and with government. https://www.nationalisacs.org/about-isacs Accessed: 5/8/17)
NG	NG Next Generation. Organisers of the NG Security Summit conference in Portugal
Phishing	Phishing. Phishing emails are crafted to look as if they've been sent from a legitimate organization. These emails attempt to fool you into visiting a bogus web site to either download malware (viruses and other software intended to compromise your computer) or reveal sensitive personal information. The perpetrators of phishing scams carefully craft the bogus web site to look like the real thing. https://www.us-cert.gov/sites/default/files/publications/emailscams_0905.pdf (Accessed: 15/7/15)
RIDDOR Reporting of Injuries, Diseases and Dangerous Occurrences Regulations	Is the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013. These Regulations require employers, the self-employed and those in control of premises to report specified workplace incidents. http://www.hse.gov.uk/healthservices/riddor.htm (Accessed: 11/7/15)
Risk Appetite	The amount of risk exposure, or potential adverse impact from an event, that the enterprise is willing to accept or retain. This risk appetite provides a threshold beyond which the enterprise will apply risk treatments and controls to reduce the risk exposure level to within the appetite of the enterprise. Drew, M (2007) BT Technology Journal January 2007, Volume 25, Issue 1, pp 19-29 10.1007/s10550-007-0004-x
Risk Assessment.	Risk assessment. A systematic process of evaluating the potential risks that may be involved in a projected activity or undertaking. http://www.oxforddictionaries.com/definition/english/risk-assessment (Accessed: 5/7/15)
Risk Tolerance	The amount of uncertainty an organization is prepared to accept in total or more narrowly within a certain business unit, a particular risk category or for a specific initiative. https://www.rims.org/resources/ERM/Documents/RIMS_Exploring_Risk_Appetite_Risk_Tolerance_0412.pdf Accessed: 15/7/15
Root Cause Analysis	A structured evaluation method that identifies the root causes for an undesired outcome and the actions adequate to prevent recurrence. Root cause analysis should continue until organizational factors have been identified, or until data are exhausted. http://www.hq.nasa.gov/office/codeq/rca/rootcauseppt.pdf p.31 Accessed: 2/5/15 Now moved to https://sma.nasa.gov/docs/default-source/safety-messages/safetymessage-2005-08-01hurricanekatrina-vits.pdf Accessed

	2/8/17 Author O'Conner B p.5
Sarbanes Oxley Act 2002	Sarbanes Oxley Act 2002 The legislation came into force in 2002 and introduced major changes to the regulation of financial practice and corporate governance. Named after Senator Paul Sarbanes and Representative Michael Oxley, who were its main architects, it also set a number of deadlines for compliance. http://www.soxlaw.com/ (Accessed: 30/7/17)
SCADA	Supervisory Control and Data Acquisition. The flow of gas and oil through pipes, the processing and distribution of water, the management of the electricity grid, the operation of chemical plants, and the signalling network for railways. These all use various forms of process control and 'supervisory control and data acquisition' - known as SCADA technology. http://www.cpni.gov.uk/scada/ (Accessed: 5/7/15)
Security Policy Framework	Security Policy Framework (SPF) The security policy framework describes the standards, best-practice guidelines and approaches that are required to protect UK government assets (people, information and infrastructure). https://www.gov.uk/government/publications/security-policy-framework (Accessed: 11/7/15)
Smart City	One that has digital technology embedded across all city functions. http://smartcitiescouncil.com/smart-cities-information-center/definitions-and-overviews Accessed: 2/5/15
Smart Phone	A wireless phone with computing capabilities. Power, D (2013) Mobile decision support and business intelligence: an overview. Journal of Decision Systems vol. 22 No 1, p4-9 www.tandfonline.com/doi/pdf/10.1080/12460125.2012.760267?needAccess=true (Accessed:27/8/17)
Social engineering.	Social engineering is a strategy for obtaining information people wouldn't normally divulge, or prompting an action people normally wouldn't perform, by preying on their natural curiosity and/or willingness to trust. https://www.us-cert.gov/sites/default/files/publications/emailscams_0905.pdf (2008, p.4) (Accessed: 15/7/15)
Stuxnet	A computer worm that targets industrial control systems that are used to monitor and control large scale industrial facilities like power plants, dams, waste processing systems and similar operations. It allows attackers to take control of systems without the operators knowing. http://uk.norton.com/stuxnet (Accessed: 12/7/15)

CRANFIELD UNIVERSITY

MIKE HUMPHREY

IDENTIFYING THE CRITICAL SUCCESS FACTORS TO IMPROVE INFORMATION SECURITY INCIDENT REPORTING

Appendices

CRANFIELD DEFENCE AND SECURITY
PhD

Academic Year: 2010- 2017

Supervisor: Dr Ruth Massie
August 2017

CRANFIELD UNIVERSITY

CRANFIELD DEFENCE AND SECURITY
PhD

Academic Year 2010- 2017

MIKE HUMPHREY

Identifying the Critical Success Factors to improve Information Security Incident Reporting

Appendices

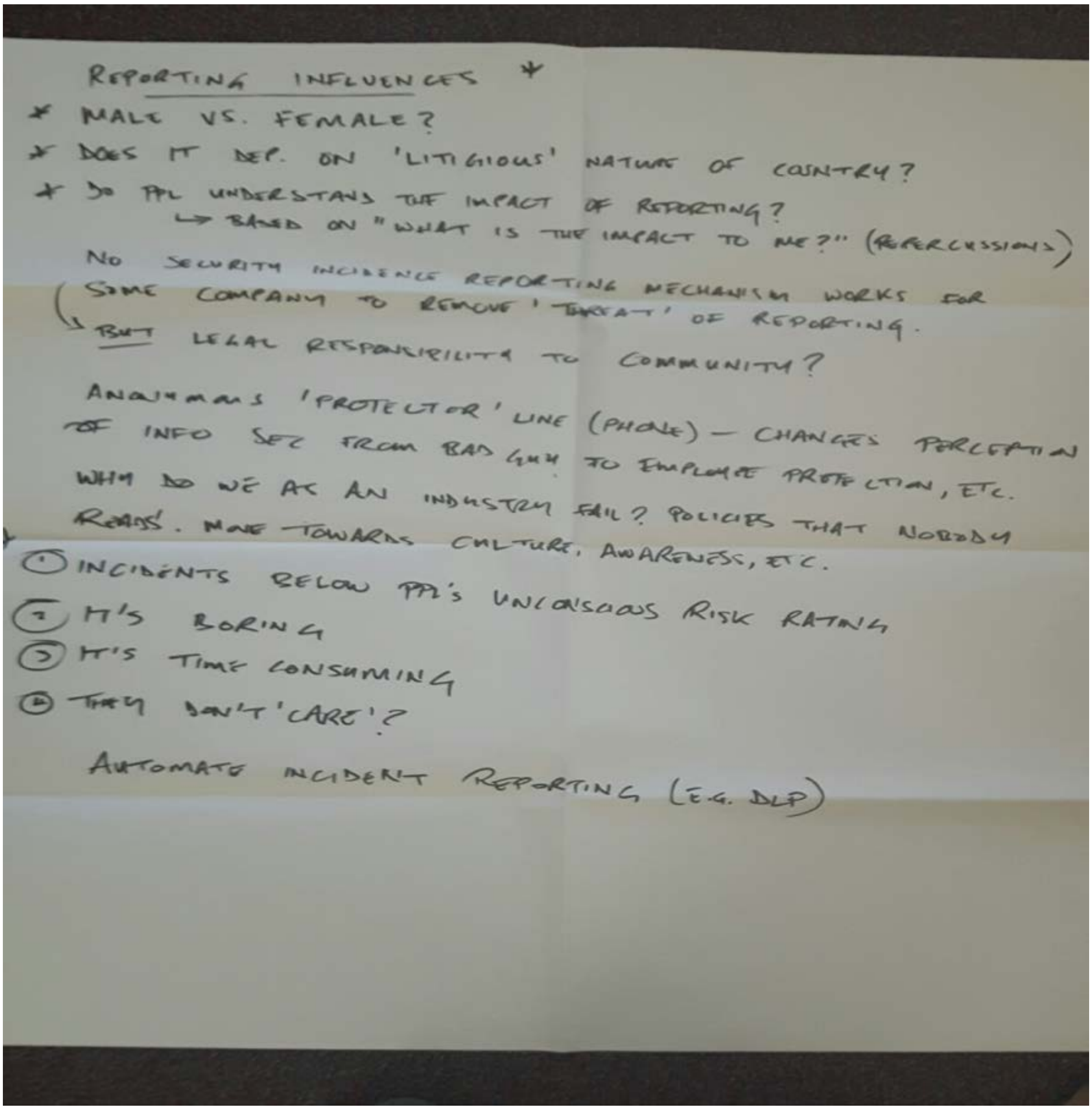
Supervisor: Dr Ruth Massie
August 2017

LIST OF APPENDICES

(Separate Document)

APPENDIX 1

Photograph of NG Security Summit Lisbon 2011 Workshop Flipchart



REPORTING INFLUENCES *

* MALE VS. FEMALE?

* DOES IT DEP. ON 'LITIGIOUS' NATURE OF COUNTRY?

* DO PPL UNDERSTAND THE IMPACT OF REPORTING?
↳ BASED ON "WHAT IS THE IMPACT TO ME?" (REPERCUSSIONS)

NO SECURITY INCIDENCE REPORTING MECHANISM WORKS FOR SOME COMPANY TO REMOVE 'THREAT' OF REPORTING.
↳ BUT LEGAL RESPONSIBILITY TO COMMUNITY?

ANONYMOUS 'PROTECTOR' LINE (PHONE) – CHANGES PERCEPTION OF INFO SEC FROM BAD GUY TO EMPLOYEE PROTECTION, ETC.

WHY DO WE AS AN INDUSTRY FAIL? POLICIES THAT NOBODY READS! MOVE TOWARDS CULTURE, AWARENESS, ETC.

① INCIDENTS BELOW PPL'S UNCONSCIOUS RISK RATING
② IT'S BORING
③ IT'S TIME CONSUMING
④ THEY DON'T 'CARE'?

AUTOMATE INCIDENT REPORTING (E.G. DLP)

APPENDIX 2

PhD Security Incident Reporting Survey

I am currently studying for a PhD at Cranfield University - Defence Academy UK. The aim of this research is to identify the reasons why people, departments or organisations find the reporting of security incidents a challenge. What are the barriers? Are they people specific, organisational or a mixture of both?

Many professionals and researchers believe the actual number of incidents that occur against those reported is significantly different. This perceived discrepancy could have a significant adverse effect on decisions made where to direct resources to protect information assets.

As respected professionals attending NG Security Summit Europe your personal and professional experiences and views will be of particular value. You may well have your own thoughts as to how these actual or perceived barriers can be dismantled.

The attached questionnaire can be completed either anonymously or, if you wish, identify yourself and participate more fully in the research. If you do not wish be identified, could you at least indicate the nature and size of your organisation to assist in identifying any specific sector trends. If you are willing to engage with me for further discussions on your views and opinions I would be most grateful.

I am attending NG Security Summit Europe and available to answer any questions, or, if you are willing, conduct face to face interviews. I can assure you that any information provided in the questionnaire and/or subsequent discussions will be handled and stored securely.

I have tried to keep the questionnaire simple with most responses being tick box, whilst providing space for comments. It is intended for completion by hand as trying to cater for different versions of office products is not always easy. I am sure there are many valuable viewpoints out there so please do not be inhibited in any response.

The survey is in 5 small sections.

1. About you/your organisation.
2. Incident reporting requirements and methods of reporting.
3. Confidence in the level of security incident reporting in your organisation and your opinion of incident reporting levels in general.
4. Barriers to reporting.
5. Your chance to add any additional views or further comments on any specific question.

I appreciate your work time is precious and often longer than there are hours in the day. Any contribution is gratefully received and I thank you in anticipation of your co-operation in this research. I will provide a summary of the findings of the results (sanitised of course) through the organiser of NG Security Summit Europe and individually to those who ask for it. Details on how to return completed questionnaires are at the end.
Regards,

Mike Humphrey MSc. M.Inst.ISP May 2011
+44(0)7767 392434
m.humphrey@cranfield.ac.uk

SECTION 1

About you (if you wish to identify yourself) or some detail regarding the industry (Govt/ Private Sector/Academia etc.) you work in to assist in identifying any possible differences in these groups. ***Note. If self- employed, some questions are not easily answered or applicable. Therefore please indicate in the box below you are self- employed and also which sector your answers are based on from previous experience or consultancy.**

Name

Role

Organisation

Tel/ Mobile

E mail

Irrespective of any wish to remain anonymous, to assist in analysis of the information can you please complete the following which will assist in identifying the sector or size of your organisation and whether this has any effects on the responses?

Staff size of your organisation;

0-500 □ 501-1000 □ 1001-5000 □ 5001-10000 □ 10000 + □ *Self employed □

Which Sector do you work in?

Public Sector □ (If one of the boxes below does not describe your sector please tick other and add a description)

Central Govt □ Local Govt □ Health □ Law Enforcement □

Other (please specify) □

Private Sector □ (If one of the boxes below does not describe your sector please tick other and add a description)

Finance □ Retail □ Transport □ Manufacturing □

Service industry □ Communications □ Energy □ Consulting □

Other (please specify) □

Academia □ □

1.1 Where is your organisation based? Tick all that apply

UK □ Europe □ Elsewhere □ (please specify below)

1.2 If your organisation is multi-based do you feel your answers given may be different according to the country where the incident occurred?

Yes □ No □ Add any additional explanation below

SECTION 2

Incident reporting requirements and methods of reporting: For example are you subject to any regulatory reporting? How do staff report security incidents? Incident definitions: Do you work to any if so what ones do you work to?

2.1. Are you subject to any regulatory reporting for incidents (e.g. Government, Financial, contractual? Etc.)

Yes □ No □

If yes - please describe

2.2 Do you have a formal policy and procedure for reporting?

Yes □ No □

2.3 What methods are used to report incidents? Please tick all that apply

Verbal □

E mail □

Specific form □

Website/intranet □

To line manager □

Specific team/person □

Anonymously □

Other (Please describe below) □

2.4 How would you rate your current reporting system?

Fit for purpose □ Adequate □ Not fit for purpose □

2.5. If you were in charge of the incident reporting system, what changes, if any, would you make?

2.6. Who investigates reported incidents?

Line manager □

Specific person/team □

Other (specify) □

2.7. Do you use any software tool to manage the reports/provide management information?

Yes □ No □ If yes please provide details below

2.8. Do you use any 'incident definitions' in separating incident types?

Yes □ No □ If yes can you briefly list them or attach to this survey?

2.9. Are other people/teams/ groups involved in the investigation of incidents or their resolution?

(E.g. training, HR)

Yes □ No □

If yes please specify

SECTION 3

Confidence in the level of security incident reporting in your organisation and your opinion of incident reporting levels in general. Do you feel all /most/some etc. are reported? Who is more likely to report? What do you do with the reports?

3.1. With regards to your incident reporting system, how confident are you regarding the number of incidents reported?

a. All or most incidents are reported □

b. The majority are □

c. Some are □

d. Few are □

3.2. In your experience or opinion are some groups of workers more likely to report than others?

General staff	More Likely □	Less likely □	Do not know □
Junior managers	More Likely □	Less likely □	Do not know □
Middle managers	More Likely □	Less likely □	Do not know □
Senior management	More Likely □	Less likely □	Do not know □
Director level	More Likely □	Less likely □	Do not know □

3.3. Are security incidents reported to Board Level?

Only if serious □

Regularly □

Occasionally □

Rarely □

Never □

3.4. Is Management information on incidents created? Yes □ No □

3.5. Does this take into account under reporting? Yes □ No □

3.6. If subject to a serious/targeted malware or external attack do you warn/inform anyone outside of your organisation? (E.g. a Government, CERT etc.)

Yes □ No □ If yes who? Please indicate below

If no, are there any particular reasons why not?

3.7. If certain types of incident were mandated to be reported to a central body (e.g. Information Commissioners) what type of incidents do you think these should be?

3.8. Do you feel mandated reporting would increase the number of incidents reported locally?

Yes □ No □ Not sure □

3.9. If mandated reporting was introduced, what safeguards would you like to see in place?

3.10. Do you read/make use of the various incident report surveys? (Verizon, Symantec, PWC etc.)

Yes □ No □

3.11. Do you feel the security incident data they collect/made available to them represents;

The full picture □ a reasonable picture □ a partial picture □

Note: This is not a criticism of the surveys - they can only report what is made available.

SECTION 4

From research carried out in other sectors it is apparent that there may be barriers to reporting and therefore learning from incidents.

Below is a list of some of those identified barriers. Can you indicate to what degree they could apply as barriers to reporting and learning from information security incidents?

4.1. An undue focus on the immediate event rather than on the root causes of problems;

Strongly Agree □ Agree □ Neither Agree/ Disagree □ Disagree □ Strongly Disagree □

Comment? (If any)

4.2. Latching onto one superficial cause or learning point to the exclusion of more fundamental but sometimes less obvious lessons;

Strongly Agree □ Agree □ Neither Agree/ Disagree □ Disagree □ Strongly Disagree □

Comment? (If any)

4.3. Rigidity of core beliefs, values and assumptions, which may develop over time – learning is resisted if it contradicts these;

Strongly Agree □ Agree □ Neither Agree/ Disagree □ Disagree □ Strongly Disagree □

Comment? (If any)

4.4. Lack of corporate responsibility – it may be difficult, for example, to put into practice solutions which are sufficiently far-reaching;

Strongly Agree □ Agree □ Neither Agree/ Disagree □ Disagree □ Strongly Disagree □

Comment? (If any)

4.5. Ineffective communication and other information difficulties – including failure to disseminate information which is already available;

Strongly Agree □ Agree □ Neither Agree/ Disagree □ Disagree □ Strongly Disagree □

Comment? (If any)

4.6. An incremental approach to issues of risk – attempting to resolve problems through tinkering rather than tackling more fundamental change;

Strongly Agree □ Agree □ Neither Agree/ Disagree □ Disagree □ Strongly Disagree □

Comment? (If any)

4.7. Pride in individual and organisational expertise can lead to denial and to a disregard of external sources of warning – particularly if a bearer of bad news lacks legitimacy in the eyes of the individuals, teams or organisations in question;

Strongly Agree □ Agree □ Neither Agree/ Disagree □ Disagree □ Strongly Disagree □

Comment? (If any)

4.8. A tendency towards scapegoating and finding individuals to blame, rather than acknowledging and addressing deep-rooted organisational problems;

Strongly Agree □ Agree □ Neither Agree/ Disagree □ Disagree □ Strongly Disagree □

Comment? (If any)

4.9. The difficulties faced by people in "making sense" of complex events is compounded by changes among key personnel within organisations and teams;

Strongly Agree □ Agree □ Neither Agree/ Disagree □ Disagree □ Strongly Disagree □

Comment? (If any)

4.10. Human alliances lead people to “forgive” other team members their mistakes and act defensively against ideas from outside the team;

Strongly Agree □ Agree □ Neither Agree/ Disagree □ Disagree □ Strongly Disagree □

Comment? (If any)

4.11. People are often unwilling to learn from negative events, even when it would be to their advantage;

Strongly Agree □ Agree □ Neither Agree/ Disagree □ Disagree □ Strongly Disagree □

Comment? (If any)

4.12. Contradictory imperatives – for example communication versus confidentiality;

Strongly Agree □ Agree □ Neither Agree/ Disagree □ Disagree □ Strongly Disagree □

Comment? (If any)

4.13. High stress and low job-satisfaction can have adverse effects on quality and can also engender a resistance to change;

Strongly Agree □ Agree □ Neither Agree/ Disagree □ Disagree □ Strongly Disagree □

Comment? (If any)

4.14. Inability to recognise the financial costs of failure, thus losing a powerful incentive for organisations to change;

Strongly Agree □ Agree □ Neither Agree/ Disagree □ Disagree □ Strongly Disagree □

Comment? (If any)

End of Questionnaire (unless you wish to add any comments etc. in Section 5)

Thank you again for taking the time to complete this questionnaire. Your responses can be returned in one of the following ways.

1. By post

Mike Humphrey (Infosec), Security Dept. PO Box 8000 London SE11 5EN England.

2. Electronically

If you wish to scan it and e mail it to me (thereby potentially identifying yourself or your organisation) but still require me to remove any reference/ indication to you or your organisation I will keep the questionnaire and delete the e mail.

E mail m.humphrey@cranfield.ac.uk

3. You can hand it in at the NG Security Summit conference to one of the Organisers

Confidentiality and Security of responses

Where anonymity is requested it will be honoured. If you wish to contribute, but not be identified, I will ensure that is the case. I appreciate that to be honest in a response and identify an organisation those comments relate to may cause concern or a reluctance to fully answer a question. That is why I have provided sectors and staff sizing in a way that would make any obvious department or company identification difficult.

I work for an organisation that handles information to the highest level of security classification and therefor electronic and paper storage of any responses will be protected within that environment. I have the support of that organisation in my research and therefore permission to store any responses. One of the reasons I chose the Defence Academy for this research was for their recognised ability and capability to handle any sensitive information.

Regards

Mike Humphrey MSc. M.Inst.ISP May 2011
+44(0)7767392434
m.humphrey@cranfield.ac.uk

SECTION 5

Your chance to add any additional views or further comments on any specific question. For example you may disagree with my assumptions with reference to under reporting, you may have views on the barriers listed.   This is your opportunity to state your views on the issues, again in the knowledge the responses will be un-attributable.

If you wanted to add more to any of your answers please indicate the section and paragraph.

APPENDIX 3

Table of Results

The below table provide a comparison of the primary findings between the two events

Subject	**NISC**		**NG**		**Other conferences**		**Total**	
Attendees eligible to complete the questionnaire	70 **(*a)**		44					
Number completed	20	29%	16	36%	2		38	
SECTION 1								
Identified themselves	16	80%	14	88%	1		31	82%
Public Sector	15	75%	1	6%	0		16	42%
Private Sector	5	25%	15	94%	2		22	58%
Subject to regulatory reporting	14	70%	8	50%	0		22	58%
SECTION 2								
Have a formal policy and procedure for reporting	19	95%	14	88%	1		34	89%
Methods to report								
Verbal	15	75%	9	56%	2		26	68%
E mail	16	80%	14	88%	2		32	79%
Specific form	10	50%	7	44%	0		17	45%
Website/intranet	7	35%	9	56%	0		16	42%
To line manager	16	80%	9	56%	0		25	66%
Specific team	14	70%	12	75%	1		27	71%
Anonymously	7	35%	9	56%	1		17	45%
Other	2	10%	2	13%	1		5	13%
How they rate their current reporting system								
Fit for purpose	8	40%	4	25%	0		12	32%
Adequate	8	40%	7	44%	2		17	45%
Not fit for purpose	4	20%	5	31%	0		9	24%
Who investigates								
Line Manager	4	20%	2	13%	0		6	16%
Specific Person/Team	17	85%	13	81%	2		32	84%
Other	4	20%	5	31%	0		9	24%
Use a software tool	11	55%	10	63%	0		21	55%
Use incident definitions	10	50%	12	75%	0		22	58%
Others involved in investigation/resolution	18	90%	16	100%	1		35	92%
SECTION 3								
Confident in number of incidents reported **(*b)**								
All	3	15%	0	0%	0		3	8%
Majority	4	20%	7	47%	0		11	30%
Some	8	40%	7	47%	2		17	46%
Few	5	25%	1	6%	0		6	16%
Group of workers most likely to report **(*b)**								
General staff	6	30%	5	33%	0		11	30%
Junior managers	8	40%	9	60%	0		17	46%
Middle managers	7	35%	13	87%	1		21	58%
Senior management	7	35%	6	40%	0		13	35%
Directors	4	20%	7	47%	1		12	32%
Incidents reported to Board level								

(*b)								
Only if serious	5	25%	7	47%	1		13	35%
Regularly	11	55%	4	27%	0		15	41%
Occasionally	2	10%	0	0%	0		2	5%
Rarely	1	5%	4	27%	1		6	16%
Never	1	5%	0	0%	0		1	3%
Management information on incidents created	15	75%	11	69%	0		26	68%
If a serious targeted malware or external attack do you warn/inform outside your organisation	18	90%	13	81%	0		31	82%
Would mandating incident reporting increase those reported locally **(*c)**								
Yes	7	37%	6	40%	1		14	39%
No	7	37%	5	33%	0		12	33%
Not sure	5	26%	4	27%	1		10	28%
Do you read/use incident report surveys	15	75%	15	94%	0		30	79%
Do they represent the….								
Full picture	0	0%	0	0%	0		0	0%
Reasonable picture	9	45%	13	81%	0		22	58%
Partial picture	7	35%	3	19%	0		10	26%
SECTION 4 Barriers to reporting *(d)								
1. Undue focus on immediate event…..								
Strongly agree	4	20%	4	25%	1		9	24%
Agree	9	45%	6	38%	0		15	40%
Neither agree/disagree	4	20%	3	19%	1		8	21%
Disagree	3	15%	1	6%	0		4	11%
Strongly disagree	0	0%	2	13%	0		2	5%
2. Latching onto superficial cause….								
Strongly agree	2	10%	2	13%	0		4	11%
Agree	6	30%	5	31%	1		12	32%
Neither agree/disagree	5	25%	7	44%	0		12	32%
Disagree	6	30%	2	13%	1		9	24%
Strongly disagree	1	5%	0	0%	0		1	3%
3. Rigidity of core beliefs…..								
Strongly agree	2	10%	3	19%	0		5	13%
Agree	10	50%	9	56%	0		19	50%
Neither agree/disagree	5	25%	2	13%	1		8	21%
Disagree	3	15%	2	13%	1		6	16%
Strongly disagree	0	0%	0	0%	0		0	0%
4. Lack of Corporate Responsibility……								
Strongly agree	5	25%	3	19%	0		8	21%
Agree	11	55%	6	38%	1		18	47%
Neither agree/disagree	0	0%	4	25%	1		5	13%
Disagree	4	20%	2	13%	0		6	16%
Strongly disagree	0	0%	1	6%	0		1	3%

5. Ineffective communication and other…….								
Strongly agree	5	26%	5	31%	0		10	27%
Agree	9	47%	8	50%	1		18	49%
Neither agree/disagree	3	16%	3	19%	1		7	19%
Disagree	1	5%	0	0%	0		1	3%
Strongly disagree	1	5%	0	0%	0		1	3%
6. Incremental approach to issues of risk…….								
Strongly agree	4	22%	2	13%	0		6	17%
Agree	6	33%	8	50%	1		15	42%
Neither agree/disagree	3	17%	5	31%	0		8	22%
Disagree	5	28%	1	6%	1		7	19%
Strongly disagree	0	0%	0	0%	0		0	0%
7. Pride in individual and organisational expertise…….								
Strongly agree	4	22%	1	6%	0		5	14%
Agree	5	26%	11	69%	1		17	46%
Neither agree/disagree	2	11%	1	6%	1		4	11%
Disagree	8	42%	3	19%	0		11	30%
Strongly disagree	0	0%	0	0%	0		0	0%
8. A tendency towards scapegoating								
Strongly agree	4	22%	4	25%	0		8	22%
Agree	2	11%	3	19%	0		5	14%
Neither agree/disagree	5	26%	5	31%	0		10	27%
Disagree	8	42%	2	13%	1		11	30%
Strongly disagree	0	0%	2	13%	1		3	8%
9. Difficulties making sense of complex events…….								
Strongly agree	2	11%	2	13%	0		4	11%
Agree	8	42%	7	44%	0		15	41%
Neither agree/disagree	3	16%	4	25%	1		8	22%
Disagree	6	32%	3	19%	1		10	27%
Strongly disagree	0	0%	0	0%	0		0	0%
10. Human alliances lead to forgiveness……								
Strongly agree	3	16%	5	31%	0		8	22%
Agree	9	47%	5	31%	0		14	38%
Neither agree/disagree	4	21%	2	13%	0		6	16%
Disagree	3	16%	3	19%	2		8	22%
Strongly disagree	0	0%	1	6%	0		1	3%
11. Unwillingness to learn….								
Strongly agree	3	16%	4	25%	0		7	19%
Agree	5	26%	5	31%	0		8	22%
Neither agree/disagree	2	11%	3	19%	0		5	14%
Disagree	8	42%	4	25%	2		14	38%
Strongly disagree	1	5%	0	0%	0		1	3%

12. Contradictory Imperatives………..								
Strongly agree	3	16%	3	19%	0		6	16%
Agree	13	68%	8	50%	0		21	57%
Neither agree/disagree	0	0%	3	19%	1		4	11%
Disagree	3	16%	1	6%	1		5	14%
Strongly disagree	0	0%	1	6%	0		1	3%
13. High stress and low job satisfaction………..								
Strongly agree	6	32%	7	44%	0		13	35%
Agree	9	47%	6	38%	2		17	46%
Neither agree/disagree	2	11%	2	13%	0		4	11%
Disagree	2	11%	1	6%	0		3	8%
Strongly disagree	0	0%	0	0%	0		0	0%
14. Inability to recognise financial cost of failure…..								
Strongly agree	5	26%	5	31%	0		10	27%
Agree	9	47%	7	44%	2		18	49%
Neither agree/disagree	1	5%	2	13%	0		3	8%
Disagree	4	21%	2	13%	0		6	16%
Strongly disagree	0	0%	0	0%	0		0	0%

*a: It is difficult to assess accurately as the attendee list although it excluded exhibitors did include some suppliers who attended as delegates who would not be in a position to answer the questionnaire. The estimate of 70 is based on removing duplicate attendees and those who appeared to be suppliers.

*b: One respondent for the NG conference did not provide any response in these sections therefore the % scores were based on the resultant lower number of responses of 15 as opposed to 16 for the remainder of questions. This is also reflected in the overall scores for that section being out of 37 instead of 38.

*c: One respondent for NISC and one for NG conference did not provide any response in these sections therefore the % scores were based on the resultant lower number of responses of 19 as opposed to 20 and 15 as opposed to 16 for the remainder of questions. This is also reflected in the overall scores for that section being out of 36 instead of 38.

*d: one respondent did not return section 4 complete and answers for Question 4.5 onwards were missing hence the % for these scores will be out of 19 respondents instead of 20 except for Q6 where another responder did not answer this question so this question for NISC the % is out of 18 respondents and not 20.

APPENDIX 4

Information Security Incident Reporting Delphi Study - December 2015

An opportunity to contribute to research into the reporting of information security incidents

Dear Colleague,

I am a part time PhD student at Cranfield University at the Defence Academy of the UK, Shrivenham. My PhD research looks at the issue of security incident reporting. My day job is that of the Head of Information Assurance and Operational Security at the National Crime Agency. I am a Fellow of the Institute of Information Security Professionals (IISP) and an elected member of the Information Assurance Advisory Councils' (IAAC) management committee.

I have come to a stage in my research where I need to seek the views from information security professionals on what could be considered the Critical Success Factors required to support the security incident reporting process. This request for assistance in contributing to academic research has reached you through your membership of a recognised Information Security Community of Interest. It may be you have also received this through other CoI's that you belong to and, if this is the case, may I apologise if it appears that you are being spammed. One response would be really appreciated.

The enclosed questionnaire contains a list of elements identified through my research that are considered to be effective in the reporting of security incidents and it is your views on the relevance of these elements that I am seeking. There is also the facility within the questionnaire to add any factor(s) that you think has not been considered and you feel worthy of inclusion. It may be included in the next round for your fellow professionals to consider.

Completion of the questionnaire should take no more than 15 minutes. Once returned I will analyse all the responses and send the collective view back to you so you can then further score/comment on any emerging consensus from fellow professionals. Normally such exercises take the form of no more than three rounds, the final one being as near to consensus as possible. In the second, and possible, third rounds the completion time is a lot shorter as you are being asked whether you agree or disagree with the emerging consensus (assuming that there will be consensus, it may be there is not) and will have already understood the content and aims.

For the purpose of this study, as there is no universally accepted definition, I am using one I have crafted for my thesis:

> *An information security incident is either, an actual or potential event that has, or is likely to, cause harm to the confidentiality, integrity and/or availability of data, assets, systems or infrastructure whether caused by people, processes or technology.*

Eligibility criteria for completion of the questionnaire.

Through your experience in information security many of you will meet the requirements. I am particularly looking for those of you who at some point have been involved or provided advice and guidance on one or more of the following;

i) the reporting of, investigation or management of security incidents,
ii) risk analysis, risk assessment and/or risk management,
iii) any policy, regulatory or legal role that covered incident reporting.

However, even if you do not meet the above but feel you have a valuable contribution to make your involvement in this research will definitely be most welcome. If you know of someone else who is equally eligible, but may not have received this, please forward them a copy of this letter and questionnaire.

The attached questionnaire contains details on completion, submission and reassurance re the confidentiality and attribution of responses. Should you have any questions or concerns re sensitive responses please contact me on the e mail address below.

For the first round can you please complete and return by Monday the 21st December. This will then give me time over the Christmas break to analyse the returns and send out Round 2 early in the New Year.

I do hope you can find the time to add your valuable contribution to the research. Thank you for reading this.

Yours faithfully,

Mike Humphrey MSc

Part Time PhD Student Defence Academy Shrivenham

m.humphrey@cranfield.ac.uk

APPENDIX 5

Copy of Email text sent to respective CoI's to then use to forward the Delphi survey to IAAC/IISP/ISO's

Once again thank you for allowing your organisation/community of interest to distribute the enclosed Delphi questionnaire as part of my research into the reporting of information Security Incidents.

I have enclosed an introductory letter explaining the Delphi study process and the questionnaire itself. It is a pdf form that can be completed electronically and returned. Other methods of completion are explained in the accompanying letter.

Could you please now distribute them both to your community and copy me in.

If you feel willing and able to add some supportive message encouraging your community to contribute this would be most welcome. I enclose a possible draft you may wish to base this on below.

Draft intro to any distribution message

Mike Humphrey is an active member of our community. He has sought and obtained permission to use our community of interest/membership to support his research into the reporting of information security incidents. As security professionals you are well placed to give an accurate insight into this subject and your opinion is greatly valued. The eventual outcome of Mike's research is to produce a set of elements that are considered important to be included in any information security incident reporting process. Their inclusion should improve the number of incidents being reported and reduce the barriers to such reporting.

Please can you find the time in your busy lives to complete and return the questionnaire to the address contained in the instructions. Mike would appreciate returns by the 21st December to allow him time over Christmas to analyse the initial results and identify any emerging consensus before sending out a second round for your view on that potential consensus of opinion.

Regards

Mike

Reference no.

APPENDIX 6

Security Incident Reporting Delphi Study - Round One - Instructions

Section One - Identification of respondent and relevant business sector

This survey will be conducted in strict confidence and your responses anonymised. I will be the only person analysing the responses. All responses will be collated, analysed and any emerging consensus will be sent to you again by email for further comment. As stated in my letter it is likely that only three iterations will be issued, each one taking less time than the previous. You can either complete as a pdf form or, as sometimes there are compatibility issues, print it out, complete by hand, scan and return. If you do not want to email your response but post it instead the address for posting replies is**:** Mike Humphrey Standards and Security PO Box 8000 London SE11 5EN. My e mail address for the survey responses is m.humphrey@cranfield.ac.uk You can withdraw from the survey at any time and after the completion of the survey I am happy to provide a de-brief on the results.

Please be assured all responses will be treated with strict confidentiality and the final analysis and any reporting will not identify individuals or companies.

Section Two – Suggested Possible Critical Success Factors to Improve Reporting of Security Incidents

This section contains a suggested list of elements considered to be important to the effective reporting of incidents. Against each one can you state 'yes' or 'no' if you believe if it is relevant to information security incident reporting. Then the same again for whether you believe it could be considered a Critical Success Factor (CSF). The elements listed can be very important but not necessarily a Critical Success Factor. CSF's have been described as[1]:

> "Important to achieving overall corporate goals and objectives,
> Measurable and controllable by the organisation to which they apply,
> Relatively few in number – not everything can be critical,
> Expressed as things that must be done not the end point of the process,
> Applicable to all companies in the industry with similar objectives and strategies and hierarchical in nature."

Please rank your view of the importance of each of various elements from 1 to 5. With 1 being highly important to 5 being highly unimportant. Finally if you wish you may comment on your answer. If you feel any others are missing please add them and score appropriately on page 7. Any additional elements identified may be incorporated in the second or third round to seek consensus.

[1] Freund, Y,. Planners Guide - Critical Success Factors (1988, p.20)

SECTION 1 – About you and/or your organisation

About you or some detail regarding the industry (Govt/ Private Sector/Academia etc.) you work in to assist in identifying any possible differences in these groups**. *Note. If self- employed or retired, your experience and views are still invaluable. Some questions in Section One are not easily answered or applicable. Therefore please indicate in the box below if you are self- employed/retired and also which sector your answers are based on from previous experience or consultancy. ALL RESPONSES WILL BE TREATED WITH COMPLETE CONFIDENTIALITY**

Name

Role

Organisation

Tel/ Mobile E mail

Please note: To be involved in subsequent rounds in the survey I will need to know how to send it so please include a reply to email or postal address

To assist in analysis of the information can you please complete the following which will assist in identifying the sector or size of your organisation and whether this is reflected in any responses?

Staff size of your organisation;

0-500 □ 501-1000 □ 1001-5000 □ 5001-10000 □ 10000 + □ *Self-employed/retired □

Which Sector do you work in?

Public Sector □ (If one of the boxes below does not describe your sector please tick other and add a description)

Central Govt □ Local Govt □ Health □ Law Enforcement □ Military □

Other (please specify)

Private Sector □ (If one of the boxes below does not describe your sector please tick other and add a description)

Finance □ Retail □ Transport □ Manufacturing □ Service industry □ Communications □ Energy □ Insurance □

Consulting □ Other (please specify)

Academia □ **Other sector (please specify)**

1.1 Where is your organisation based? Tick all that apply

UK □ Europe □ Elsewhere □ (please specify below) Select other options as below

1.2 If your organisation is multi-based do you feel your answers given may be different according to the country where the incident occurred?

Yes □ No □ Add any additional explanation below

Which Community of Interest did you receive this survey from? IISP □ CISP □ Police □ IAAC □ Other □ please specify below

SECTION 2 Survey Round 1				
List of elements to improve Incident reporting	**Is it relevant to information security incidents -** **Select as appropriate or Circle the Yes or No**	**Is this a possible Critical Success Factor -** **Select as appropriate or Circle the Yes or No**	**Rank the importance of the element to improve incident reporting by selecting or circling as appropriate one of the below numbers as applicable to the key below;** **1. Highly important** **2. Important** **3. Neither Important/unimportant** **4. Unimportant** **5. Highly unimportant**	**Comment (if any)**
1. **Separation of collection, and analysis from any discipline or regulatory process**	□ □ YES NO	□ □ YES NO	Select from below list 1 2 3 4 5	
2. **Collection of reports of ‘near misses’ as well as actual incidents**	□ □ YES NO	□ □ YES NO	Select from below list 1 2 3 4 5	
3. **Rapid, useful, accessible and intelligible feedback to the reporting community**	□ □ YES NO	□ □ YES NO	Select from below list 1 2 3 4 5	
4. **Ease of making a report**	□ □ YES NO	□ □ YES NO	Select from below list 1 2 3 4 5	

List of elements to improve Incident reporting	Is it relevant to information security incidents - Select as appropriate or circle the Yes or No	Is this a possible Critical Success Factor - Select as appropriate or Circle the Yes or No	Rank the importance of the element to improve incident reporting by selecting or circling as appropriate one of the below numbers as applicable to the key below; 1. Highly important 2. Important 3. Neither Important/unimportant 4. Unimportant 5. Highly unimportant	Comment (if any)
5. Standardised reporting systems within organisations	□ □ YES NO	□ □ YES NO	Select from below list 1 2 3 4 5	
6. A working assumption that individuals should be thanked for reporting incidents rather than being automatically blamed for what has gone wrong	□ □ YES NO	□ □ YES NO	Select from below list 1 2 3 4 5	
7. **Mandatory reporting**	□ □ YES NO	□ □ YES NO	Select from below list 1 2 3 4 5	
8. Standardised risk assessment (to determine the impact of the incident)	□ □ YES NO	□ □ YES NO	Select from below list 1 2 3 4 5	

List of elements to improve incident reporting	Is it relevant to information security incidents - Select as appropriate or circle the Yes or No	Is this a possible Critical Success Factor - Select as appropriate or Circle the Yes or No	Rank the importance of the element to improve incident reporting by selecting or circling as appropriate one of the below numbers as applicable to the key below; 1. Highly important 2. Important 3. Neither Important/unimportant 4. Unimportant 5. Highly unimportant	Comment (if any)
9. A common understanding of what factors are important in determining risk	□ YES □ NO	□ YES □ NO	Select from below list 1 2 3 4 5	
10. **A mechanism or process for confidential reporting**	□ YES □ NO	□ YES □ NO	Select from below list 1 2 3 4 5	
11. A recognition by senior management that incidents will happen	□ YES □ NO	□ YES □ NO	Select from below list 1 2 3 4 5	
12. Incident reporting systems that are designed appropriately to ensure learning is possible	□ YES □ NO	□ YES □ NO	Select from below list 1 2 3 4 5	
13. **Incident analysis that considers root causes and wider systems/processes and not just the initial impact assessment**	□ YES □ NO	□ YES □ NO	Select from below list 1 2 3 4 5	
Thank you for completing this questionnaire. Please go to page 7 for details of returning the form				

You can add any factor that you think has not been considered and feel worthy of inclusion. It may be included in the next round for your fellow professionals to consider. **Please add any in the format below and score as previous advised**				
Additional suggested elements to improve incident reporting	**Is it relevant to information security incidents -** **Select as appropriate or circle the Yes or No**	**Is this a possible Critical Success Factor –** **Select as appropriate or circle the Yes or No**	**Rank the importance of the element to improve incident reporting by selecting or circling as appropriate one of the below numbers as applicable to the key below** **1. Highly important** **2. Important** **3. Neither Important/unimportant** **4. Unimportant** **5. Highly unimportant**	**Comment (if any)**
14.	□ □ YES NO	□ □ YES NO	Select from below list 1 2 3 4 5	
15.	□ □ YES NO	□ □ YES NO	Select from below list 1 2 3 4 5	
16.	□ □ YES NO	□ □ YES NO	Select from below list 1 2 3 4 5	

Thank you for your time. Please e mail your completed form to m.humphrey@cranfield.ac.uk Alternatively if you wish to post it please send to Mike Humphrey Standards and Security PO Box 8000 London SE11 5EN

APPENDIX 7

Dear [insert name],

Firstly, may I thank you again for taking the time to complete round one of my Delphi study research questionnaire into Security Incident Reporting. I had a very positive response, with many of you adding valuable comments in the spaces provided next to the elements.

I did say that once I had analysed the responses I would contact those who did respond with details of any emerging consensus, together with a request that you again kindly set aside 15 minutes of your time to provide your views on these findings.

The next stage should be quicker to complete. It contains three sections. Firstly, as you had already responded with your full details and sector, size of organization etc. I will not be asking for that again. Instead I have allocated you a reference number that will ensure I can marry up your response in round 2 to that of round one. This also will save you time repeating your details. In addition, I again provide reassurances re confidentiality. You can go straight to the questions in section 2 and 3. Your reference number is

Section 2 contains four elements that scored the highest in round one responses. These have been considered as the Critical Success Factors. As many of you added valuable comments on the elements I have tried to incorporate the main recurring comments into an amended version of the original element, which in theory adds more value to the statement.

I am then asking whether you feel this amended wording improves or reduces the value of the element as a Critical Success Factor. This is a tick box section with the same opportunity to comment if you wish.

The 3rd section is of a similar vein, but includes the next three highest scoring elements that could assist in the reporting of incidents. These did not score high enough to be included as a Critical Success Factor. I am asking whether the additional description adds to these elements or not and, if it does, can it now be considered as a CSF to join the other four?

There was an opportunity in round one for you to suggest any element not listed as a potential CSF. A number of you made suggestions and I have incorporated aspects of these views into the descriptions of the elements where appropriate. These comments included aspects of governance and education.

I will enclose two documents, the 2nd round questionnaire as a pdf form and as a word form format (whichever is easiest for you to complete). I have sent them separately as some defences do not like certain types of pdf form. Hopefully you will receive one of them.

Please note some respondents had difficulty where they completed a response but did not save it as a separate document and then forwarded the unsaved one to me. With some versions of mail and office document management, if you completed the form as it arrived without renaming and saving it, when it was sent back to me your response was blank. So please save your response and then send that saved version.

Some of you took the option of printing, completing then scanning the response and then emailing the scanned version, others printed and completed and then posted it to me. All these options are still open to you in round 2.

I would be grateful if you could return your answers to the above email address or as before if you prefer post to me at the address shown in the instructions.

c:\users\mike\documents\phd\thesis commenced feb 2013\chapter 3 methodology\round two documents\draft round 2 delphi intro email 30_03_16 v.2 10_4_16.docx

Your Reference no.

APPENDIX 8

Security Incident Reporting Delphi Study - Round Two - Instructions

Section One - Identification of respondent and relevant business sector

As this section was completed by yourself in Round One I have allocated your response a reference number (top right of this page). This reduces the amount of time taken to complete round two. Again, as in Round One, this survey will be conducted in strict confidence and your responses anonymised. I will be the only person analysing the responses. All responses will be collated, analysed and any further emerging consensus will be sent to you again by email for further comment. As stated in my original letter, it is likely that only three iterations will be issued, each one taking less time than the previous. This is the second iteration of the Delphi study. You can complete as a PDF form, word document or, as sometimes there are compatibility issues, print it out, complete by hand, scan and return by email. If you do not want to email your response but post it instead the address for posting replies is**:** Mike Humphrey Standards and Security PO Box 8000 London SE11 5EN. My e mail address for the survey responses is m.humphrey@cranfield.ac.uk You can withdraw from the survey at any time and after the completion of the survey I am happy to provide a de-brief on the results.

Please be assured all responses will be treated with strict confidentiality and the final analysis and any reporting will not identify individuals or companies.

Section Two – Emerging Consensus of Critical Success Factors to Improve Reporting of Security Incidents

This section contains the emerging consensus of those elements that respondents considered a Critical Success Factor (CSF) and scored the highest amongst the choices of elements. There are four of them (not in any order of preference).

Element 3.	**Rapid, useful, accessible and intelligible feedback to the reporting community**
Element 4.	**Ease of making a report**
Element 11.	**A recognition by senior management that incidents will happen.**
Element 13.	**Incident analysis that considers root causes and wider systems/processes and not just the initial impact assessment.**

As a reminder, Critical Success Factors have been described as[1]:

> "Important to achieving overall corporate goals and objectives. Measurable and controllable by the organisation to which they apply, Relatively few in number – not everything can be critical. Expressed as things that must be done not the end point of the process. Applicable to all companies in the industry with similar objectives and strategies and hierarchical in nature."

The CSF descriptions have been added to, based on the responses and comments provided in round one. This section asks your views on whether you feel the additional description affects the element as a Critical Success Factor.

There are again five choices available for you to indicate your preference. This time the options ask your opinion whether the amended wording of the element either; significantly improves its value as a CSF, improves its value as a CSF, neither improves or reduces its value as a CSF, reduces its value as a CSF and finally significantly reduces its value as a CSF. In addition, please indicate whether this amended element remains a CSF - Yes or No? There is also space for any comments you may wish to make.

Section Three - Elements that could be considered as Critical Success Factors but did not score as highly as those in Section Two above.

This section contains those elements that scored well, but not as well as the above four elements, but were scored higher than the rest. As in Section 2, the descriptions have been added to, based on the responses and comments provided in round one. This section asks your views on whether or not you feel the additional description affects the element and improves it to such an extent that it can be considered eligible to be included as a Critical Success Factor amongst the four already identified in Section 2. There are three of them (again not in any order of preference).

Element 2. Collection of reports of near misses as well as actual incidents
Element 7. Mandatory Reporting
Element 8. Standardised risk assessment (to determine the impact of the incident)

Again, there are five choices available for you to indicate your preference. The options are that the amended wording either; significantly improves the element such that it should now be included as a Critical Success Factor with the four CSF elements above, improves the element such that it should now be included as a Critical Success Factor with the four CSF elements above, neither improves or diminishes the element such that it should remain where it is, it diminishes the element such that it should not be included as a Critical Success Factor with the four CSF elements above and finally it significantly diminishes the element such that it should not be included as a Critical Success Factor with the four CSF elements above. There is also space for any comments you may wish to make.

[1] Freund, Y, Planners Guide - Critical Success Factors (1988, p.20)

Section 2. Emerging Consensus on Critical Success Factors – The four most popular elements considered to be a Critical Success Factor.

Below are the four highest scoring elements that were considered by consensus as Critical Success Factors to improve Incident Reporting. Further descriptions of the element have been added as a result of comments made by respondents in Round One. The original element number is shown in brackets. Please place your view against each of the four elements considered to be a Critical Success Factor by selecting or circling, as appropriate, one of the five numbered choices.

1. Original wording (Element 3) ***Rapid, useful, accessible and intelligible feedback to the reporting community*** **1a. Amended wording:** **Rapid, useful, accessible and intelligible feedback to the reporting community[2] recognising:** • People will only continue to report incidents if they are acknowledged and, even better, can see that reporting has been useful. • Feedback need not be detailed, often a simple acknowledgement of the report and that action is being taken may be sufficient. • Staff that have been responsible for a security incident can at times become extremely anxious, sometimes unnecessarily so and it is helpful to discus with them what the risk (or otherwise) is and for them to be kept up to date and involved.	**How do you feel the amendments impact on the value of the element as a Critical Success Factor?** **1. Significantly improves the value of the element as a Critical Success Factor** **2. Improves the value of the element as a Critical Success Factor** **3. Neither improves or reduces the value of the element as a Critical Success Factor** **4. Reduces the value of the element as a Critical Success Factor** **5. Significantly reduces the value of the element as a Critical Success Factor** **1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐** **In view of the above, does this element remain a Critical Success Factor? YES ☐ NO ☐**	**Comment (If Any)** Click here to enter any comments you may wish to make.

[2] Community being the one that your organisation may belong to law enforcement, finance, healthcare etc.

2. Original wording (Element 4)	**How do you feel the amendments impact on the value of the element as a Critical Success Factor?**	**Comment (If Any)**
Ease of making a report **2a. Amended wording:** **Ease of making a report, recognising if incident reporting is difficult individuals will be less likely to submit them. This may particularly affect the reporting of near misses. The reporting process should:** • Include a sufficiently clear level of education and awareness to all staff in how the reporting process works. • Describes what an incident is. • Describes how to report it and what escalation needs to take place. • Sets out levels of expected feedback. • Be clearly set out as part of any governance process.	**1. Significantly improves the value of the element as a Critical Success Factor** **2. Improves the value of the element as a Critical Success Factor** **3. Neither improves or reduces the value of the element as a Critical Success Factor** **4. Reduces the value of the element as a Critical Success Factor** **5. Significantly reduces the value of the element as a Critical Success Factor** **1** ☐ **2** ☐ **3** ☐ **4** ☐ **5** ☐ **In view of the above, does this element remain a Critical Success Factor? YES** ☐ **NO** ☐	Click here to enter any comments you may wish to make.

3. Original wording (Element 11) ***A recognition by senior management that incidents will happen.*** **3a. Amended wording:** **A recognition by senior management that incidents will happen and that they must play a full and active part in the incident management process by.** • Fully accepting that incident reporting is to be seen positively and not punitive. • Recognising security incidents are part of life and business and, like accidents, the reporting process is part of the prevention strategy. • Supporting a culture which encourages reporting • Recognising an organisation which handles an incident well enhances its reputation	**Do you feel the amendments impact on the value of the element as a Critical Success Factor?** **1. Significantly improves the value of the element as a Critical Success Factor** **2. Improves the value of the element as a Critical Success Factor** **3. Neither improves or reduces the value of the element as a Critical Success Factor** **4. Reduces the value of the element as a Critical Success Factor** **5. Significantly reduces the value of the element as a Critical Success Factor** **1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐** **In view of the above, does this element remain a Critical Success Factor? YES ☐ NO ☐**	**Comment (If Any)** Click here to enter any comments you may wish to make.

4. Original wording (Element 13) ***Incident analysis that considers root causes and wider systems/processes, not just the initial impact assessment.*** **4a. Amended wording** **Incident analysis that considers root causes and wider systems/processes, not just the initial impact assessment. This is crucial to understanding what actually contributed to an incident otherwise if the true cause is not identified repeat incidents or larger scale impact ones can occur.** **It should be recognised:** • The incident may be just a symptom of a larger organisational or process flaw. • Superficial investigations may be counterproductive in the long term	**Do you feel the amendments impact on the value of the element as a Critical Success Factor?** **1. Significantly improves the value of the element as a Critical Success Factor** **2. Improves the value of the element as a Critical Success Factor** **3. Neither improves or reduces the value of the element as a Critical Success Factor** **4. Reduces the value of the element as a Critical Success Factor** **5. Significantly reduces the value of the element as a Critical Success Factor** **1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐** **In view of the above, does this element remain a Critical Success Factor? YES ☐ NO ☐**	**Comment (If Any)** Click here to enter any comments you may wish to make.

Section 3 Elements that could be considered as Critical Success Factors but did not score as highly as those above

The below elements scored well, but not as well as the above four elements but were scored higher than the rest. Further descriptions of the element have been added as a result of comments made by respondents in Round One. The original element number is shown in brackets. Please place your view against each of the three elements that the emerging consensus scored well, but not as well as the above four elements in Section 2 by selecting or circling, as appropriate, one of the five numbered choices.

Original wording (Element 2)

Collection of reports of near misses as well as actual incidents

2a. New wording

Collection and review of reports of near misses as well as actual incidents. Recognising;

- Much can be learnt from near misses
- By doing so can identify the required preventive measures that need to be in put in place to deal with organisational learning and/ or a change in policy & procedure to ensure that such near misses do not, in future become actual incidents.

Do you feel the amendments impact on the value of the element and its potential to join the four Critical Success Factors in Section 2?

1. **Significantly improves the element such that it should now be included as a Critical Success Factor.**
2. **Improves the element such that it should now be included as a Critical Success Factor.**
3. **Neither improves or diminishes the element and that it should remain where it is.**
4. **Diminishes the element such that it should not be included as a Critical Success Factor.**
5. **Significantly diminishes the element such that it should not be included as a Critical Success Factor.**

1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

Comments (if any)

Click here to enter any comments you may wish to make.

Original wording (Element 7) ***Mandatory Reporting*** **7a New wording** **The reporting of incidents should be mandatory. An organisation cannot mitigate any impact or learn from an incident unless there is an awareness something has happened. Recognising:** • A true record of incidents can provide accurate management information which enables amongst other things; trend analysis, a greater understanding of actual rather than perceived threats and risks and more evidence based resource allocation. • Although the decision to report should not be optional the actions taken should be tailored to the incidents severity. For example a manager should have some discretion to deal locally with minor issues such as not locking computer screens or not complying with the clear desk policy. • Staff need clear guidance on what and how to report.	**Do you feel the amendments impact on the value of the element and its potential to join the four Critical Success Factors in Section 2?** **1. Significantly improves the element such that it should now be included as a Critical Success Factor.** **2. Improves the element such that it should now be included as a Critical Success Factor.** **3. Neither improves or diminishes the element and that it should remain where it is.** **4. Diminishes the element such that it should not be included as a Critical Success Factor.** **5. Significantly diminishes the element such that it should not be included as a Critical Success Factor.** **1** ☐ **2** ☐ **3** ☐ **4** ☐ **5** ☐	Comments (if any) Click here to enter any comments you may wish to make.

Original wording (Element 8) ***Standardised risk assessment (to determine the impact of the incident)*** **8a New wording** **Having Standardised risk assessment (to determine the impact of the incident) whilst recognising:** • There are advantages to standardise within a single organisation or sector but wider standardisation can be a challenge. • Risk and impact assessment are essential as part of post event and incident management criteria. An initial standard approach will enable comparison of similar incidents and facilitate fact-based resolution.	**Do you feel the amendments impact on the value of the element and its potential to join the four Critical Success Factors in Section 2?** **1. Significantly improves the element such that it should now be included as a Critical Success Factor.** **2. Improves the element such that it should now be included as a Critical Success Factor.** **3. Neither improves or diminishes the element and that it should remain where it is.** **4. Diminishes the element such that it should not be included as a Critical Success Factor.** **5. Significantly diminishes the element such that it should not be included as a Critical Success Factor** **1** □ **2** □ **3** □ **4** □ **5** □	Comments (if any) Click here to enter any comments you may wish to make.

Again thank you for your time to complete the second stage of this Delphi study. Please save your response and as before please e mail your completed form to m.humphrey@cranfield.ac.uk Alternatively if you wish to post it please send to Mike Humphrey Standards and Security PO Box 8000 London SE11 5EN

APPENDIX 9

Additional Suggestions for CSF’s

Private Sector 10 of the total of 43 made additional suggestions (23%)

Public Sector 34 of the total of 67 (50%) made additional suggestions. Academia made no suggestions

Private Sector additional elements						
Respondent	Suggestion	Relevant	CSF Y/N	Importance	Comment	Include Y/N
56	A mechanism for incident alerting	Y	Y	2	Covered by element 2,5,	N
56	Additional Process for incident analysis	Y	Y	2	Covered by element 13	N
15	Feedback on how an incident has been managed	Y	Y	1	Covered by element 3	N
39	Realistic threat intelligence	Y	N	2	More of a result of better reporting	N
39	3rd Party certification frameworks	Y	N	2	Possibly referring to validation of reporting mechanisms	N
115	Joint incident reporting and management processes	Y	Y	1	Covered by 12,5,	N
115	Having a SWG	Y	No score	2	Using the SWG to review incidents. This is after they have been reported so not applicable	N

115	Education and awareness re incident reporting	Y	N	2	Possible inclusion but not considered as a CSF by respondent. Linked to others suggesting education linked to making a report	Y
89	Publication of case studies	Y	N	2	More of a result of reporting	N
89	Improved enforcement by ICO for example	Y	Y	2	Possibly linked to Mandated reporting 7	N
45	Anonymous reporting	Y	N	2	Covered by element 10	N
36	Standard input mechanism to enable sharing	Y	Y	2	Covered by 5 re common systems and possibly 3 re feedback and 12	N
34	Technical rigour in risk assessments	Y	Y	1	Possibly linked to 8, 9,	N
34	Provide a legal and procedural framework	Y	Y	2	Possibly covered by 5, 7	N
34	Better informed business justification for conducting an investigation proactively	Y	Y	2	Possibly covered by 9,12,13,	N
102	Effective tooling to support incident identification, reporting and analysis	Y	Y	1	Covered by 12,5,4	N
102	Integration of incident reporting into corporate governance policies and processes to reporting to the Board	Y	Y	1	Covered by 3,5,9,11 but goes further into reporting mechanisms that include reporting to the board	N

54	Adapting and learning from event	Y	Y	1	Definitely covered by 3,12,13	N
54	Intelligence information	Y	Y	1	More of use of information gleaned from threats and previous incidents	N[i]

Public Sector suggested additional elements

Respondent	Suggestion	Relevant	CSF Y/N	Importance	Comment	Include Y/N
87	Reporting bad practice	Y	N	3	More about non-compliance than incidents	N
4	Dissemination And analysis	Y	N	1	Covered by 3,5,12 and 13	N
95	Resources available	Y	Y	1	Not covered original elements	
95	Involvement of other stakeholders	Y	Y	2	Possibly covered by 5 and 3	N
79	Establishment of clear governance	Y	Y	1	Similar to comment by 102 from private sector. Covered by 3,5,9,11 but goes further into reporting mechanisms that include reporting to the board	N
79	Establish clear criteria for external notification	Y	Y	1	Possibly an outcome of improved reporting part of the conceptual framework improvement of outcomes then needs further work Part of 7	N
28	Linking to corporate mechanisms	Y	Y	1	As per 79, and 102	N

58	Training and education re incident reporting that is not linked to witch hunting	Y	Y	1	Covered in part by 1, 6 but links to 115. Include in ease of making a report	N
80	Provide added value?	Y	Y	1	No explanation given	N
86	Defined metric to enable reporting effectiveness	Y	N	2	Covered by 5,8,9,	N
70	Clarity of reporting systems (who do I tell)	Y	Y	1	4 embellishment of 4 and 10	N
112	Organisational awareness of process	Y	Y	1	Covered by 4 and 5 but embellishment of ease or reporting and awareness communication of its existence	Add to CSF
112	No blame culture	Y	Y	1	Covered by 1,6	N
103	Clear and structured reporting process	Y	N	2	Covered by 4 and 5 but again could be added to better describe the CSF	Add to CSF
73	Sharing of trends address issues in policy	Y	No score		3,5,12 cover elements of this	N
82	Relationships between teams to resolve issues	Y	N	3	Possible covered by 3, 5,12	N
82	Proof incident has been resolved	Y	Y	1	Covered by 3,12	N
59	Wider considerations re onward reporting	Y	N	2	Covered by 3,5,7 but possible addition to CSF	N
83	Weak approach could have adverse	Y	No score	2	Possibly covered by 1 but embellishment to determine accident	N

	affect				as opposed to reckless	
83	Weak line management by turning blind eye resulting in not reporting	Y	No score	2	Possibly covered by 6,7, 11,	N
90	Guidelines on remedial action	Y	Y	4	Covered by 12,	N
97	Mandatory reporting	Y	Y	2	Covered by 7	N
97	Standardisation of reporting	Y	N	2	Covered by 5	N
44	Include in incident report the measures already taken to prevent loss etc	Y	Y	2	Possible embellishment of reporting process to ensure format includes actions already taken	N
77	Probability impact threshold	Y	N	3	Linked to near misses when is it an incident or near miss and when to report. Linked to 2	N
110	Onward reporting is this covered eg to ICO	No score	No score	No score	Linked to 7 mandated reporting his should state who too.18	N
18	Understanding of the legal implications of incidents and need to report	Y	Y	1	Possibly linked to 7 but also to education and awareness	N
12	As above	As above	As above	As above	As above	N
55	Functional area affected accountability and reporting lines	Y	N	2	3,4,5,12	N
55	Early identification of incidents	Y	Y	1	Linked to 2 near misses	N

2	Education	Y	Y	1	Linked to 102, 28,and 79, 91	Y
75	Risk based approach	No score	No score	No score	Covered by 9	N
91	Training of managing incidents	Y	N	3	Include education on ease of making a resport	Y
1	Regular security briefings	Y	Y	1	Include education in ease of making a report	Y
19	Identification of root cause	Y	Y	1	Covered by 13	N
19	Knowing a near miss has occurred	Y	Y	1	Covered by 2	N
69	Staff awareness re incident reporting	Y	Y	2	Include education in ease of masking report	Y
[	Increase staff skills in use of reporting systems				Include education in ease of m making a report	Y
3	Collaboration of other partners in organisation HR, ICT etc	N	Y	2	Partly covered by 12,13	N
20	Encourage to report anything they perceive to be a potential security weakness	Y	Y	2	Covered as near miss but also definition of near miss may be helpful	N
67	Publicise standard management actions for incident management	Y	Y	2	Linked to education and awareness not just for staff but actions on by management. Embellishment of reporting mechanism	N
67	Collaboration of internal teams	Y	Y	2	Partly covered by 12,13	N

67	Performance metrics and education and awareness	Y	Y	2	Include education in ease of making a report	Y
57	Neutral anonymous impartial feedback from management	Y	Y	2	Covered by 1 and 6,11,10	N
6	Reporting lines (possibly linked to governance)	Y	No score	2	Possibly covered by 6,7, 11,	N
6	Should CSO/CRO be on board	Y	No score	1	Possibly covered by 6,7, 11,	N

Key

Suggested CSF regarding Education	🟧
Suggested CSF regarding Governance	▨

i

APPENDIX 10

Comments on the top four CSF and three Possible CSFs from round one and two of the Delphi

Round one comments

CSF	Comments made (respondent number)	Useful wording to consider
3. Rapid, useful, accessible and intelligible feedback to the reporting community	1.Correcting where people went wrong is only possible with honest feedback. An essential element of the OODA loop. 3. if the reporting community is top of the organisation : visibility of the IM process and leaks in the infrastructure 4. ISOs in police forces are under considerable pressure, reporting needs to be quick and easy but with enough info to allow useful communication 6. Gov is a good example of never feeding back despite all the info sharing bodies CiSP, CPNI 8. Probably depends on the source of reporting 10. The reporting unit is not necessarily the unit under investigation 12. If the reporting community do not receive at least acknowledgment and, hopefully, some recognition of contribution then there is less impetus for them to spend the time doing so. 17. Users may be discouraged from reporting incidents if it is perceived that reports are ignored or are not appropriately prioritised. 21. Allows other organisations to prepare and respond, particularly with technical threats 26. This is the second most important success factor, after 4. People will only continue to report incidents if they are acknowledged and even better can see it has been useful. Zero feedback results in no further reporting. 32. Depends on the context of the incident and related parties and how many it affects 34. must be actionable and in my experience most won't share 35. Without it, the reporting community may be inclined to give up and ask: why bother? It should also be part of the service's Continuous Improvement Process. 37. There is little point in investing time and money to establish a reporting process and develop a reporting culture if there is no feedback. The reporting community will soon stop reporting if it is felt that their time and effort is disappearing into a 'black	• Recognise some incidents may require faster feed back than others which may be less impactive but feedback must always be given unless in very specific sensitive incidents where the feedback may just be a thankyou for reporting. • reporting needs to be quick and easy but with enough info to allow useful communication. • If the reporting community do not receive at least acknowledgment and, hopefully, some recognition of contribution then there is less impetus for them to do so again. • People will only continue to report incidents if they are acknowledged and even better can see it has been useful. Zero feedback results in no further reporting. • The reporting community

	hole'. 39. Visualisation of attacks, drill down for my organisation but provenance of attack is important. 41. I think that if you used terminology such as 'business language' then it may help the question. Reputation is important especially when we are seen as 'black box' in the majority of situations. Once the reputation becomes tarnished without justification then this leads to mistrust and circumvention. 43. The lack of 360 feedback relayed to the "coal face" is a continual cause of disgruntlement of those charged with defending the enterprise. 53. Recent experience of CyrptoLocker incidents has required immediate action / notification to avoid similar incidents. 61. What community? Needs clarification. 63. If there is no feed back reporters cannot be expected to have confidence in the reporting system 67. Feedback and thanks is given automatically to reporting staff via a tool generated email/message. This is an important part of encouraging staff to report security incidents through the **** Live Incident Assurance Management process. 70. So they see the value in reporting, particularly if the feedback helps them - then they are more likely to report. 71. Critical to disseminate details of threats, vulnerabilities and mitigations quickly. 75. It is in the eye of the beholder what rapid, useful, accessible and intelligible is (and balacing between legal regulations, (local, national, European, woldwide) impact,... 77. Feedback about "was this a useful report" more valuable to goal than "and this is what we did about what you reported", but both seem a little peripheral 80. Ifthey do not get added value (in exchange) for their report, they will limit it to the minimum (necessity v desire) 82. Lessons learnt are essential for practitioners to develop, this also impacts staff motivation. However, for management I don't see this as a crucial activity for making business decisions. 87. Feedback provides incentive to contribute 89. Ideally showing successful investigations and detections/prosecutions. Also showing that every organisation has a similar experience 96. Officers that have been responsible for a security incident can at times become extremely anxious, sometimes unnecessarily so and it is helpful to discus with them what the risk (or otherwise) is and for them to be kept up to date and involved,	will soon stop reporting if it is felt that their time and effort is disappearing into a 'black hole'. • If there is no feed back reporters cannot be expected to have confidence in the reporting system • Consider auto feed back via reporting sysyem as a start of the notification process. Then some human intervention to elicit more detail and provide expectation of reporter • Where necessary provide support to the reporter if the impact of the incident is severe. • Feedback provides incentive to contribute

	including letting them know when no further action is required. Contrary to this some officers have a complacent attitude to what can be quite serious incidents and it is important to get the message across quickly to both them and their management as to the potential consequences to ensure the incidents are not repeated. 98. Yes rapid reporting can help contain incidents. 102. 102. Far too little information-sharing within and across sectors, resulting in insufficient timely warning and learning from other orgs' experiences, 103. It is extremely important to have feedback - one of the most important aspects of the incident management process as it helps organisational learning. However, I questions the need for 'rapid' - it is more important to provide useful and considered advice back to the community, including mitigation actions, rather than just a 'it has happened' response. 107. The feedback could confirm the analysis results of incidents and prevent further occurrence. 110. Reportees like to feel that the effort they are making to report incidents is time well spent. 114. I feel that it is important but not a critical success factor because the reporting can still proceed as usual even if the reporting community does not get adequate feedback. However if the feedback is lacking too much that might, in theory, affect the behaviour the reporting community. 115. Depending upon the outcome of the following investigation, it may not be appropriate to share the results to all concerned. This is common when I make reports.	
4. Ease of making a report	1.The system must be user-friendly by being intuitive, especially with potentially technical incidents being reported. An over-emphasis on the request for information on protocols for instance would encourage the reporter to become frustrated. 3. reports are filled-in by volunteers 6. Cardinal points 10. this is vital as the majority of our users might only ever report one incident in their career. Plus users are inherently lazy if it is not easy they will not do it. 12. If it is too complicated or long winded they will simply not be bothered to complete it. 17. If incident reporting is difficult individuals will be less likely to submit reports. This may may particularly impact the reporting of near misses. 18. Easy reporting allows user community to make early and informative reports which	• system must be user-friendly by being intuitive, especially with potentially technical incidents being reported. is vital as the majority of our users might only ever report one incident in their career. • Particular from the perspective of the end user. Need to get the balance of collecting all data and mitigations taken without

	in turn assists in determining and auctioning counter compromise measures 21. Ease of use is a critical factor to determine whether people will act (Foggs Behaviour Model) 24. If it is not easy making report then will discourage from making future reports 26. People will try once, or if you are lucky, twice to make a report. If it's too difficult or slow, you will never hear from them again. Everything else then becomes irrelevant. 29. In order to increase reporting the process must be easy 32. Simple reporting mechanisms should be in place that are not too onerous and which may thwart coming forward. 34. anonymity often key 35. Ease is often proportional to inclination to use. If it were a Critical Success Factor, how would you measure it to know it's done? 37. The reporting process should be as easy and quick as possible if it is to gain acceptance within the workplace. Todays society is very much a 'three click' culture from the ubiquitous web way of life, especially with the Gen Y and Z groups, which is encroaching all aspects of life. Therefore, simplicity and ease of use is the key to a successful take-up of a new process. 43. Reports should be aimed at a specific audience, however it is important the subtlety and severity of an incident is not lost on the senior management when reporting "up". Painting a picture of "everything is rosy because we've fixed it" is not advisable. 45. If it is difficult, especially with medium to high volume they simply wont do it. 50. This is extremely important, if it isn't easy for users to report incidents and events then they will probably not be bothered to do so. 53. Depends on underlying perspective of the question but the reporting mechanism is varied and so considered less critical. The mechanism for early reporting / alerting / communication across the organisation is paramount. 59. Particular from the perspective of the end user. Need to get the balance of collecting all data and mitigations taken without turning them off to the process. 62. As an example, we have seen the reporting of phishing rocket within the organisation when we created a simple Outlook "button" to report the phish in the moment of its detection by the recipient. 63. Action Fraud is not user friendly and does not allow for the reporting of incidents which did not result in a loss or at least did not when I last tried to report something.	turning them off to the process. • The most important factor is knowing who to communicate with and how • Consider having several reporting means available if the organisation set up makes a one stop shop difficult.

	So it is pretty useless as an intelligence gathering tool. 67. Over the past 8 years HMRC have used an Incident Reporting Tool which automates parts of the incident management process. On introduction of the system there was a marked increase in reports made by staff as it made the reporting of incidents easier. 70. Mixed feelings about CSF, but on balance I think it is. 71. Detailed techie bits can follow using other channels 75. But a requirement is that the report is spread within a selected group on a need to know basis and that they all know how to handle this kind of information. 77. This should include the follow up activities - if the reporter is suddenly going to find their diary full of meeting invites after hitting "send" or the inbox overflowing, then that is a negative 80. Of course the report should not be too complicated. But there is always a different view from the reporter (as little as necessary) to the receiver (as much info to asses the situation) 82. The report is crucial to the success of alerting people as to the severity of the incident but is not necessarily critical for measuring success. 96. The most important factor is knowing who to communicate with and how. The mechanism thereafter (e.g. complexity of any paperwork) does not seem as relevant as some officers seem incapable of completing the simplest of forms yet others will produce minute detail including further information such as photos, downloads & scans etc. 101. I think a lot of people are put off reporting cybercrime/incidents because they do not know where or how to report it. 103. Must have a method by which reporting is easy - preferably having several reporting means available. 107. This will allow the security staff to make report promptly. 114. I feel that all parties involved benefit from a proper report which at a minimum concludes the key aspects of the incident and how it was handled. 115. It is essential to make reporting as simple and straight forward as possible otherwise, busy people may avoid reporting.	
11. A recognition by senior	1. The only factor that this would influence is the blame culture that can exist and therefore the "thirst for blood" that can sometimes follow an incident. Even if senior	• critical if you want reporting to be seen positively and not

management that incidents will happen	management did recognise that security incidents were going to happen then would this influence people to report them? It probably wouldn't make a difference in my view. Slightly facetious but a large share of security incidents are committed by senior management anyway (note did not score as CSF) 4. Yes critical if you want reporting to be seen positively and not punitive. And an antidote to "It wouldn't happen here" syndrome 6. Management buy in is essential today 10. Whilst keen to see a reduction in incident we cant say whether any reduction in reports is a reduction in incidents or a reduction in reporting. We should be looking at eradicating the avoidable incidents and reducing the impact of the inevitable ones 12. The senior management must have an understanding of the possible incidents and the potential impact they could have to ensure the issue is treated appropriately and staff see the drive from their management. 15. Plus the recognition that often no one is to blame, in some cases you simply have to accept the attacker was better than your defenses, and the mode of attack could not have been predicted with the budget/resource level assigned. 17. Yes, otherwise there is a danger that insufficient effort and preparation will be undertaken by the organisation to support incident reporting and management. 18. This requirement is supported by ISO27001:2013 21. It is important to understand that risk can't be reduced to zero. Removing the human factor just leads to excessive technical or procedural controls which unduly impacts on operational effectiveness and can alienate people. 32. Top down understanding awareness and the willingness to support the incident process is key. This supports a culture which is accepting and where incidents are very much handled correctly, learned from and the actions forthcoming from them will reduce or mitigate future occurrences. 35. Important, yes. If it were not a Critical Success factor it would soon come about of its own accord. 37. The security culture of an organisation is a reflection of the security ethos of the senior management. There should not be a blame culture, but a training culture If an incident was internally generated, did the person responsible receive the correct guidance beforehand to prevent it? Did the incident occur as a result of a previously unknown vulnerability, if so, what is being done to remove that vulnerability? 39. Senior management are fickle and crass. They pay lip-service to security in general.	punitive. • recognition that often no one is to blame, • It is important to understand that risk can't be reduced to zero. • security culture of an organisation is a reflection of the security ethos of the senior management. There should not be a blame culture, but a training culture • Mistakes will happen even in the best of systems. The expectation of perfection is counter productive. • There must be no fear of reprisals when reporting and no blindness to the need to respond well to incidents. An organisation which handles an incident well enhances its reputation

	Greater governance is required with communities of interest being the focus of incident management. 42. People need to be sure they won't be blamed or stigmatized after making a report. 43. I think expectation management - and a lack of crisis management is key here. 45. Mistakes will happen even in the best of systems. The expectation of perfection is counter productive. 50. No matter how much technical or procedural security you impose on staff at the end of the day staff are only human and incidents will always occur which management need to be aware of. It is the response procedure that is important. 53. This has to be a CSF as any thing else is avoiding the truth. Sadly experience is that they have to experience a "reality" moment, serious incident, before they come to this realisation. 62. Again this is related to the blame culture (question 6) though a slightly different aspect. There must be no fear of reprisals when reporting and no blindness to the need to respond well to incidents. An organisation which handles an incident well enhances its reputation (remember Commercial Union after the St Mary Axe bomb?) while one which handles it poorly ... well, think TalkTalk. 66. get their heads out of the sand to release funds to mitigate risk 67. Organisationally this has not always been the case, however in recent times there is a recognition from the top down that these things do sometimes happen. 70. Part of the cultural issues around blame and recognising that people are human and make mistakes or do stupid things (and often the wrong thing for what they perceive as the right reason). 75. And that they accept and can explain why the accept (Financial, 100% ia not possible, risk based approach,is very important,...etc) 77. Ought to be obvious, but... 80. If your management does not understand about incidents they do not want to have any reporting. And they should see the added value. 85. Incidents like accidents are part of life and business. What is important is trying to overcome or reduce to zero the impact or chances of an incident occurring, rather ensuring that sufficiently robust as well as exercised procedures are in place to recover from an incident when …. (cannot be read as a scanned copy) 87. If 100% prevention is unachievable, containment/ repair is needed. 89. Ideally senior managers are engaged in this. More likely they are advised by someone. In some cases security stll happens despite senior management.	

	91. It depends of matter of incidents, It is difrent for whole system incident or incident of part of system. 98. Senior management support is vital to manage incidents. 103. As stated above - feedback and learning is fundamental to the incident management process. Previous answer re feedback in brackets (It is extremely important to have feedback - one of the most important aspects of the incident management process as it helps organisational learning. However, I questions the need for 'rapid' - it is more important to provide useful and considered advice back to the community, including mitigation actions, rather than just a 'it has happened' response.) 107. The senior management should be aware the incidents to prepare necessary resources to prevent the incidents. 115. If senior management do not sponsor and openly demonstrate their support for security incident reporting within an organization the risks increase significantly 116. This is the real crux we are seeing. CEOs are employing CISO level folks on the (wrong) presumption that they will solve /address all identified risks - and indeed the unidentified ones too and, if they don't, it's the CISO who must fall on their sword - in spite of the fact that the business will have been found wanting and will have made a risk based decision to not adequately address the identified risk.	
13. Incident analysis that considers root causes and wider systems/processes and not just the initial impact assessment	3. it's the real plus-value of the IM 6.The incident may be just a symptom of a larger organisational malaise 10. This impacts on policy developments and alternative solutions 12. To some degree this varies depending on the severity of the incident simply due to time and resource availability. More serious issues require consideration of root causes and process impact in order to avoid a repeat in the future. 17. Without an appreciation of the root cause behind incidents, successful prevention / avoidance of future incidents will be less likely. 21. Otherwise the same problem is likely to occur again. 29. Understand root causes to reduce the chances of reoccurrence 32. How do you know what the problem actually relates to unless you get to the root cause, key to any analysis performed and will hopefully provide the business with suitable protections going forward to ensure incidents are not repeated or their impact is reduced by appropriate controls being put in place learned from previous issues	• The incident may be just a symptom of a larger organisational malaise • Without an appreciation of the root cause behind incidents, successful prevention / avoidance of future incidents will be less likely. • Understand root causes to reduce the chances of reoccurrence • Whilst understanding the immediate impact of an

	35. I have always considered this a “standard” part of problem analysis. However this can’t be done for every security incident so perhaps you are looking at the higher-risk category? 37. Whilst understanding the immediate impact of an incident is important, getting to the root cause that led to the incident occurring is more important to ensure better prevention/mitigation measures are implemented or, at least, the risks are better understood. 39. Consideration is fine - how does that translate into strategy? Without this piece it is a futile exercise. 43. In my opinion, any incident management or impact assessment process which doesn't conduct some form of RCA, is simply a papering over the cracks exercise. 44. The risk assessment results should always be communicated to the Management. Most higher level incident reports should be aknowledged to the Management. Periodic statistics of incidents should be provided to the Management. 50. An excellent idea if this can be achieved. 51. The analysis methodology does not really affect the incident reporting process, except where it is perceived as so poor as to be useless and thereby discourages potential reporting. If the question were broadened to cover critical success factors for incident management rather than just reporting then this factor would become substantially more important. 53. Fundamental to any Incident Response service. 61. In most organisations, incident response teams will be constrained by available effort and will not be able to do this for all incidents. 62. This is crucial to understanding what actually contributed to an incident. Fact, not fantasy or assumption. 66. Root cause analysis essential otherwise repeats can occur as root not found means report highly likely 67. Incident management is not critical to incident reporting. 75. This is up to the organisation. 77. Might be drifting outside of scope of topic, if in scope then as stated. 80. Desirable but most often not shared. Unfortunately obligatory reporting will be reduced the minimum. But that information would be helpful to others. 82. This is a secondary consideration and a business decision depending on whether they want to carry such risks. I think a security team needs to be able to articulate the	incident is important, getting to the root cause that led to the incident occurring is more important to ensure better prevention/mitigation measures are implemented or, at least, the risks are better understood. • Deal with the disease, not just the symptoms.

	risk in a way that is understood by the organisation. This might be financial or reputational etc... 87. Deal with the disease, not just the symptoms. 89. In many cases the early response is dominated by tech issues. (eg an infection from a USB stick).Without determined intervention the behaviour of staff and attackers is overlooked when that is of central importance 98. Lessons learnt and post incident reviews will help to ensure continuous improvement is implemented to ensure incidents are not repeated and if they are, can be managed appropriately. 107. The initial evaluation process may need to assess the root causes of incident. 110. The more incident reports the better because you have an understanding of what is going on in your organisation. 114. In order to establish efficient management of incidents the root causes should always be considered and analyzed. I feel that certain incidents can be handled with success without analyzing the root causes. Depending on what counter-measures the organisation is able to implement the incident might never appear again. However an analysis of the root cause is almost always recommended.	

Possible CSF	**Comments made (respondent number)**	**Useful wording to consider**
2. **Collection of reports of 'near misses' as well as actual incidents**	1. Provides the full picture and can be useful to highlight any possible lack of knowledge or lack of procedures that individuals or organisations may have. 4. Psychologically lessons from near misses are often more potent than those after an incident and the damage has been done. 6. Those in charge of risk need to know the whole picture 10. I struggle to define a near miss;.whilst an incident may have no impact, it usually involves a breach of policy and is therefore still an incident. As well as assigning a risk rating which asseses impact and likelihood we also apply an assessed breach level for sanction purposes which looks at the actions of the person, not the impact of the incident. 12. Near misses can provide useful trend information that may result in action being taken to avoid potential actual incidents. 15. Needed to build a bigger picture, e.g., looking for evidence of a sustained attack. 17. Provides an opportunity to address near miss incidents such that future real security	• Near misses can provide useful trend information that may result in action being taken to avoid potential actual incidents. • collection of near miss data provides valuable trend information which can result in actions being undertaken to minimise future incidents. • Prevention better than cure, as they say. By analysing near misses it will hopefully avoid a full blown incident.

	incidents may be avoided. 18. collection of near miss data provides valuable trend information which can result in actions being undertaken to minimise future incidents. 21. This helps to inform the lessons learned or could indicate a persistent threat. 29. Prevention better than cure, as they say. By analysing near misses it will hopefully avoid a full blown incident. 32. For trend analysis, near misses can be grouped across several locations, themes and may aggregated be an incident as a whole. In trends this may show repeated activity which needs to be dealt with or rising impact. 34. much can be learnt from both your own and others near misses. near misses are easier to share too. 35. Lots of places collect violations and other potential incidents, but all too often do not do anything with them. Question asked about collection and not review. Had you asked about both then it would be a Critical Success Factor. 37. If anything, this should be considered more important than actual incidents. This is the opportunity to take action to avoid future incidents and real damage. 39. How is a near miss determined? Subjective and dependent on experience. 42. Could risk collecting too much information, which would slow down the analysis. 43. Understanding a "near miss" should promote discussion - and potentially action about what could happen in event of an incident. 44. Reports of "near misses" should only be considered as important if the "near miss" was prevented by a man' s will and would not have been auto-prevented by an already applied technical measure. 45. The more data the easier it is to determine a pattern. 47. Analysis of near misses as well as of actual incidents helps you understand how robust (or otherwise) your security systems are. 50. It is vital to collect this information as it could help prevent any potential future major incident occurring. 53. Identify all potentially critical events to maintain where / what is causing current threats are coming from and which measures are effective at mitigating. 61. Important but not a CSF as not vital. How do you capture this information and can you justify the effort? 62. We have found that collecting and analysing near misses in the safety space is crucial to understanding where interventions can be made before a major problem occurs. We are still learning how to apply that lesson to security incidents but the	• much can be learnt from both your own and others near misses. near misses are easier to share too. • Question asked about collection and not review. Had you asked about both then it would be a Critical Success Factor. • If anything, this should be considered more important than actual incidents. This is the opportunity to take action to avoid future incidents and real damage • Reports of "near misses" should only be considered as important if the "near miss" was prevented by a man' s will and would not have been auto-prevented by an already applied technical measure. In other words a detected virus or Trojan is not a near miss but a failed signature and a member of staff recognising strange behaviour in a message that prevented execution of malware is a near miss. • The more data the easier it is to determine a pattern. • We have found that collecting and analysing near misses in the safety space is crucial to

	safety experience suggests it will be crucial to sustainable management of incidents. 63. It follows from the above (the respondents answer to Element 1. But only up to a point. There should not be an automatic default to discipline/regulation but that is not to say that some response may be appropriate in the worst cases. It might, for example, involve retraining. But disciplinary action, in the first instance, should apply to failure to report) that this is a 1. The aviation industry culture of collectiv responsibiity to identify shortcomings is the desirable outcome. 67. Definition provided includes near misses and operations within **** (name removed). 71. Though difficult to define a "near miss" accurately and has obvious resource implications. 75. These kind of information has to be shared with a specific group for coherency and to see the bigger picture (not only a a small scale but as well for a bigger picture) 80. Near misses are difficult to determine. They go unnoticed by the outside. It needs tremendous trust to report them, as there will be consequences without an incident that needed consequences. 81. I see this as a tool for justifying business cases. Arguably a near miss is not an incident and therefore should not broadly reported to avoid knee jerk reactions. But being able to highlight numbers in a monthly report might be valuable. 78. Information security is provided by a series of layers, with no single layer 100% penetration proof. 89. From an attacker’s point of view there is little difference. In one case dealt with we suffered tens of near misses before we suffered actual damage. 96. ear misses in relation to security are as important as near misses in relation to Health & Safety and can flag up organisational learning and/ or a change in policy & procedure to ensure that near misses do not, on other occasions, turn into major incidents. Reporting of near misses also illustrates the level of understanding amongst the orgaisation of security issues and therefore acts as feedback on the departments ability to communicate. 98. Useful information for trend analysis and post incident reviews. Reports of 'near misses' can also help identify the required preventive measures that need to be in put in place to deal with such incidents before they become actual incidents. 102. Very few organisations have effective (blame-free) near-miss reporting, but it is a key characteristic of a mature approach to incident and risk management. 103. Near misses are just as important - as they could identify potential weakness and	understanding where interventions can be made before a major problem occurs. We are still learning how to apply that lesson to security incidents but the safety experience suggests it will be crucial to sustainable management of incidents. • Near misses in relation to security are as important as near misses in relation to Health & Safety and can flag up organisational learning and/ or a change in policy & procedure to ensure that near misses do not, on other occasions, turn into major incidents. Reporting of near misses also illustrates the level of understanding amongst the organisation of security issues and therefore acts as feedback on the department’s ability to communicate. • Reports of 'near misses' can also help identify the required preventive measures that need to be in put in place to deal with such incidents before they become actual incidents. • Near misses are just as important - as they could identify potential weakness

	indicate where a breach may occur again. 107. The report of actual incident should be considered as important to understand the reality of incidents. 110. Near misses are the misses of tomorrow and tracking and analysing near misses can be critical in stopping bad things before they happen. 114. It would give a good insight in what measures are effective and working and which measures are not working as intended. It could also be used to study what measures need "tweaking" or improvement and in which way theese tweaks should be implemented. 115. Reporting of near miss events enables lessons to be learned in the interests of incident and breach prevention in the same manner as H&S events.	and indicate where a breach may occur again. • Reporting of near miss events enables lessons to be learned in the interests of incident and breach prevention in the same manner as H&S events.
7. **Mandatory reporting**	1. People brushing incidents under the carpet only provides a false picture of the overall security culture and can drastically undermine our work to become more secure. 4. There has to be a fall-back position that says if nothing else you have to report to "this" level or when"this" occurs. This should act as a benchmark that can be raised over time but will provide minimum assurance. 10. Sanction action should be taken at those that do not. Without comprehensive reporting trend analysis is meaningless, corporate lessons cannot be identified and counter compromise and mediation action may not be taken correctly. We always stress that we can’t help if we do not know about it. 12. Staff should be reporting because of the value of doing so rather than because they have to although I acknowledge in some cases that may not always be possible and some degree of mandatory reporting may be required. 17. Whilst it should be made clear all users are required to report security incidents and near-misses, other factors such as ease of reporting and the supportiveness of the organisation will have a strong influence on whether issues are actually reported. 18. Staff should report because of the value of doing so, however mandatory requirements (‘should’ may be missing here) provide guidance and consistency. 21. A question I had difficulty with. There are many examples where reporting should be mandatory but I also think a manager should have some discretion to deal locally with minor issues such as not locking computer screens or complying with the clear desk policy. I would like the option of a very simple incident report that does require a details	• brushing incidents under the carpet only provides a false picture of the overall security • Sanction action should be taken at those that do not report not those who do. • Staff should report because of the value of doing so not just because it is mandated • the supportiveness of the organisation will have a strong influence on whether issues are actually reported. • There are many examples where reporting should be mandatory but I also think a manager should have some discretion to deal locally with minor issues such as not locking computer screens or complying with the clear desk policy.

	submission or need to identify the perpetrator. They would just be for stats purposes to identify patterns, such as challenging somebody that didn't have an access pass displayed . 32. Cannot learn and mitigate unless you know something has happened, preventative actions cannot be put in place to learn from this. 34. while difficulties exist if reporting was made wide spread more learning would result in better defences. Not simple to put in place though. 37. This most definitely should be a key policy. The difficulty lies in how it can be enforced and monitored. Inevitably, as with all aspects of corporate life, judgement calls will be made by individuals and management as to whether a situation is an incident or not. Furthermore, this policy may adversely impact response teams if not sufficiently resourced. 39. The decision to report should not be optional. 41. It all depends on the frame of reference on mandatory. Over reporting needs to be considered on the effectiveness of users to respond if they are having to report minor incidents. If there was a way of making the mandatory reporting easier i.e. yes/no single answer approach then absolutely. narrative for spam type incidents will only hamper efforts unless they are targeted incidents. 42. If many users were targeted, then only a few need make a report. Mandatory reporting could lead to too much information and slow the analysis process. 43. I think severity is the key here. Incidents which are localised and can be managed at the lowest level may not warrant a mandatory reporting (escalation) process, particularly if the wider organisation is not affected. 44. The importance of an incident is mainly directly decided by the organization's administration with respect to the persons involved, the impact it had and the general circumstances of the incident. The purpose of the reporting is the identification of an incident in order to take specific technical measures to rapidly recover the loss or restrain the impact. The risk assessment is a procedure which mainly indicates the general (not incident specific) technical measures to be taken or remaining risk to be accepted by the Organization. A standardized risk assessment should exist in any case, in order to give more objective aspect of the impact of all risks, and be taken into account in cases where difficult and expensive countermeasures, or discipline penalties are to be applied. 45. You can’t fix what you do not know about.	• It would be better if reporting occurred because it was easier and seen of benefit before mandation. • Incidents which are localised and can be managed at the lowest level may not warrant a mandatory reporting (escalation) process, particularly if the wider organisation is not affected. • The purpose of the reporting is the identification of an incident in order to take specific measures to rapidly recover the loss or restrain the impact. • even if the reporting is mandatory the actual reports will be affected by how the staff are met when reporting incidents. • Mandatory training on incident management is fundamental to ensure all personnel understand and adhere to the security requirements and are aware of the incident management process. •

	47. To be effective, all incidents and near misses must be reported. 50. Where possible this should be implemented and staff who fail to report on major or moderate incidents should be challenged and disciplined where appropriate. 53. For most organisations this is or will be come a mandatory requirement. Always keep one eye on future requirements and build in to current culture at the earliest opportunity. 55. hum - the mandatory reporting MIGHT be to a very closed stakeholder group. 61. But difficult to implement unless enforced legally or by a regulatory body. Interesting implications with new EU directive. 63. How would it be enforced? 67. Essential to **** (name removed). 70. Mixed feelings on this, not least because just mandating it doesn't mean it will happen. There has to be a reason to report it (and 'because you say I have to' is not a reason). 71. Needs to be a mandatory condition of membership of any community. 72. Depends on the sector and the effort available. If either all incidents are high impact, or you have sufficient resource that handling all incidents won't distract you from the high impact ones, then maybe. 77. Needs to be very clear about what to report, when to report, and the level of certainty that actually a security incident needs to have for it to be mandatory. 80. Voluntary reporting works only in highly trusted working-level environments. As soon as the lawyers and compliance officers come in, there is no voluntary reporting. 82. I don't really understand what this means, if an incident was similar to a prior one and occurs regularly I would argue that there would be limited value in reporting more than its occurrence. It really depends on the content of the report. 85. Making something mandatory brings the risk of it becoming perceived as a burden. At present where cyber security is not backed up by legislation I think it is difficult to make a company's procedures mandatory. I consider 'reward' and 'cajoling' a better option. 87. Only of use where the incident cannot be concealed! 89. Many organisations (most? all??) see a security problem as a threat to their reputation. I see this as the primary reason for failing to report. 96. It's important, and is a requirement in the organisation - potentially it might not be 100% enforceable. 98. Mandatory training on incident management is fundamental to ensure all personnel	

	understand and adhere to the security requirements and are aware of the incident management process. 101. Many victims of cybercrime do not actually perceive themselves to have been the victim of a crime and, therefore, do not report it. E.g. An individual has their credit card cloned on a website. They report fraudulent payments to their bank, which refunds them the money. The individual ultimately suffers no financial loss and does not consider themselves a victim of crime, therefore, not reporting it to the police. 103. Difficult to define boundaries as to what is and what isn't an incident. If mandated, then will show that incident reporting is important to the organisation. 107. Mandatory reporting could sometimes work since some security staff has a tendency to hide the incident due to some reasons. 110. People rarely do what is mandated and they will spend more time nuancing their understanding of the mandation or re-reading guidance to find a reason not to report than they will reporting 114. I believe that #7 is highly related to #6 (individuals should be thanked), even if the reporting is mandatory the actual reports will be affected by how the staff are met when reporting incidents. 115. Failure to report means that risk cannot be mitigated and counter compromise action cannot be undertaken therefore mandatory reporting is essential. 116. Likely to be coming with intended regulatory changes anyway....so it's better to "be prepared"!	
8. **Standardised risk assessment (to determine the impact of the incident)**	1.See answers 4 & 5. Again, making the process easier will prevent people from become frustrated with the reporting scheme. The system should be as simple as possible. 4. Yes for the same reason as Q5. (With a diverse community such as Policing you need a common set of standards and variables to assess incoming incidents and levels of harm involved) I have started referring to the level of Harm or Potential Harm, rather than risk. 10. It is important to rank incidents against each other, but where we struggle is that we use the same reporting process for all types of incident (info, cyber, physical, personnel etc) and it is pretty impossible to come up with one risk assessment process that can be applied to them all. 12. Certainly in our sector the vast diversity of security incidents would make it	• With a diverse community such as ******** you need a common set of standards and variables to assess incoming incidents and levels of harm involved • Recognise is pretty impossible to come up with one risk assessment process that can be applied to them all • Certainly in our sector the vast diversity of security

	impossible to standardise a risk assessment covering all types. 15. The importance should be inherent in the organisation culture, so this is a core part of doing business. Mandating it could act as a reverse incentive, with people turning a blind eye to suspect activity. 17. Not critical though where a number of methods are used it would be undesirable if different methods generated very different impact determinations. 18.diversity of security incidents in our sector (‘Law Enforcement’) would make standardisation difficult. 21. There are advantages to standardise within a single organisation but not more widely. 32. All incidents and their contexts are different and a standard risk assessment applied to all may be out of context and all stakeholders and related partners and affected systems may not be able to be quickly determined. 34. Every assessment is different but a standard approach, if comprehensive and flexible would make it easier to do well. 35. Only an experienced professional can do it freeform. Done carefully, standardised can reduce the reservation expressed in #5 (A “3” score. Standardising helps ensure consistent quality of the sought information. However, it can mean omission of important detail if it doesn’t fit on the standard report.) to a reasonable level. 37. Standardised risk assessment helps to maintain consistency and perspective when assessing risks. This will allow individuals and lower management to understand what risks they can tolerate and what risks need to be escalated, terminated or transferred. It also allows senior management to understand their overall risk and prioritise activities for risk reduction, or tolerate as necessary. 39. These turn into box ticking exercises and add little value as staff are seen as blockers. 43. Providing there is sufficient room to accommodate "free text" in which subtle nuances can be articulated or clarified. 50. Again my view would be that for major or medium incidents then "yes" it would be beneficial for someone to carry out a risk assessment but probably not worthwhile for incidents deemed as a low category. However it may be that unless the RA is completed then an incident would not be able to be assessed easily. 51. The risk assessment methodology does not really affect the incident reporting process, except where it is perceived as so poor as to be useless and thereby	incidents would make it impossible to standardise a risk assessment covering all types. • diversity of security incidents in our sector (********) would make standardisation difficult. • There are advantages to standardise within a single organisation but not more widely. • Providing there is sufficient room to accommodate "free text" in which subtle nuances can be articulated or clarified. • Standardized across the enterprise, but not necessarily the industry, as numerous methodologies are available. • Including categorisation into "Accidental" or "Deliberate" and "Internal" or "External" source. Also essential to report if the current incident is identical or similar to an earlier incident. • there are possibly too many individual factors and situations to be able to fit into one standard assessment. •

	discourages potential reporting. If the question were broadened to cover critical success factors for incident management rather than just reporting then this factor would become substantially more important. 53. The use of std risk assessment model is required beyond the incident impact. It is the means by which an organisation can measure the current (security) state and plan for an ever evolving future state. 54. Standardized across the enterprise, but not necessarily the industry, as numerous methodologies are available 67. **** (name removed) has a standardised assessment of customer impact. This includes standardisation of serious and non-serious incidents. We do not consider these as risk assessments but impact assessments and the more serious. The less serious being dealt with by the manager and more serious with **** dealing with the incident. 71. Including categorisation into "Accidental" or "Deliberate" and "Internal" or "External" source. Also essential to report if the current incident is identical or similar to an earlier incident. 75. It is up to the specific organisation. They knwo their business and a baseline for RA is not oppertuun (window dressing) 77. A reasonable effort assessment would be useful, but the "interesting" risks are likely to be outside of what any standard envisages. 80. If not consistent then whats the point... The impact certainly needs to be incorporated but to my mind that is different to standardisation. 85. this will ignore the fact that risk is different and unique to each environment. Enterprise and entity. Developing a standard risk assessment would significantly impact its effectiveness, potentially negating the very purpose it was created for. 87. Not quite sure what this means: select from a list of impact ratings or follow laid-down guidance on what rating to apply. 89. Difficult to do consistency is almost impossible. HMG impact levels helped but still remain vague. National ****** information threat model, looks valid from London, and ******** but less so in ******** (smaller locations) 96. Risk assessment does take place but whilst there are currently risk assessment tools that are useful there are possibly too many individual factors and situations to be able to fit into one standard assessment. Sometimes the risks are too organic to fit into a linear template.	

	98. Regular risk assessment reviews help to ensure incident can be identified, and detected and appropriate preventive controls are in place. This can be used to help with impact assessment. Also helps to identify/determine what controls are in place already and what new ones may be required for reactive mode should incident occur. 103. It is important that each incident goes through the same assessment so that it can be graded on its seriousness and impact, or potential impact, on the organisation. 110. Yes, but there needs to be a fudge factor, some things just don't fit the formula and you need to acknowledge that. 115. Risk and impact assessment essential as part of post event and incident management criteria. An initial standard approach will enable comparison of similar incidents and facilitate fact based resolution.	

Round two Comments made by respondents relating to the four CSF's

Critical Success Factors Round 2		
CSF (suggested changes following comments in Red)	**Comments made (respondent number)**	**Notes on comments P = Positive N= Negative O=Other general comment**
1. Original wording (Element 3) ***Rapid, useful, accessible and intelligible feedback to the reporting community*** **1a. Amended wording:** **Rapid, useful, accessible and intelligible feedback to the reporting community[1] recognising:** 1. People will only continue to report incidents if they are acknowledged and, even better, can see that reporting has been useful **or has ensured compliance** 2. Feedback need not be detailed, often a simple acknowledgement of the report and that action is being taken may be sufficient. 3. Staff that have been responsible for **or**	**(2)** Staff in the Police Service can become extremely anxious where they are involved in a security incident due to the potential of involving Professional Standards Departments and timely feedback is essential to alleviate the anxiety **(6)** Two points: - These are more qualifying points rather than improvements per se. - It might have been more useful to score each of the bullets. For instance, I would have given the first bullet a 5, second bullet a 3 and the third bullet a 2. **(7)** Being available to discuss an issue is important; people tend to focus on impact, not always overall risk, and articulating that can be important. **(8)** The constraints are valid, but including them I feel detracts from the message that shared information can benefit all **(12)** Not sure the 'unnecessarily so' statement is necessary as this may demean. **(13)** Bullet points supporting the main wording explain why this is important **(17)** Additional clarification I regard as useful as it will guide implementation of any relevant incident reporting process and supporting system. **(32)** Feedback need not be detailed – This depends on the individual concerned,	**(2)P** **(6) O** **(7)P** **(8) O** **(12) O wording amended** **(13) P** **(17) P** **(32) O**

[1] Community being the one that your organisation may belong to law enforcement, finance, healthcare etc.

involved in a security incident can at times become extremely anxious, sometimes unnecessarily so and it is helpful to discus with them what the risk/**impact** (or otherwise) is and for them to be kept up to date and involved. **4.** Alternative wording for 3 **Staff that have been responsible/involved in a security incident can become anxious. It is helpful to keep them informed and provide support where necessary** **Rapid, useful, accessible and intelligible feedback to the reporting community[2] recognising:** **1.** People will only continue to report incidents if they are acknowledged and, even better, can see that reporting has been useful **or has ensured compliance** 2. Feedback need not be detailed, often a simple acknowledgement of the report and that action is being taken may be sufficient. **3.** Alternative wording for 3 **Staff that have been responsible for or involved in a security incident can become anxious. It is helpful to keep them informed and provide support where necessary**	there are some who may take personal interest and ownership of the problem and like it to be dealt with and regard any corporate involvement as should be in tune with their reasons for reporting the first place. In the context of the amended wording, this potentially contradicts the first point. Staff that have been responsible – If they are at "fault" they may be fearful of their position so unsure whether this point fully encompasses and benefits the individual concerned and you are concentrating on the risk and not taking into account personal side to them. **(36)** Agree with all this. Not sure if you have come across the NIST Draft Special Publication (SP) 800-150, Guide to Cyber Threat Information Sharing - that might be something that interests you - more details at http://csrc.nist.gov/publications/PubsDrafts.html (see SP 800-150) **(37)** This remains highly important as users tend to be the first observers of an incident and as such should be encouraged to raise reports at the earliest opportunity. The provision of feedback both to the individual and the wider community demonstrates the corporate benefit of such reporting and that follow-up activity to resolve the incident does take place. This provides the reporter with a sense of involvement and of 'doing the right thing'. **(45)** While I agree with the statement, there should also be a mechanism for anonymous reporting and anonymous feedback. There are liability issues to be considered with regard to reporting. Obviously with anonymous reporting and feedback there will have to be a vetting mechanism to ensure that the anonymous intelligence is from a reliable source. The reporter of anonymous intelligence should also have the ability to rate the reliability of their source intelligence. **(47)** I feel the revised wording makes clearer what this element is trying to achieve and therefore am happy to amend my original answer to agree this as a Critical Success Factor (50) It is definitely valuable to feedback to those reporting incidents as to what action is being taken to address it and also depending on the nature and	**(36) P** **(37) P** **(45) P Also added suggestion for anonymous reporting** **(47) P Note previously the respondent in Delphi 1 said it was not a CSF and now as a result of the changes has indicated they now**

[2] Community being the one that your organisation may belong to law enforcement, finance, healthcare etc.

	severity of the incidents to ensure that the person/s who caused the incidents are kept up to date of events. **(53)** An initial simple acknowledgement (thanks) with an outcome feedback to all involved is recommended. Engaging with those responsible will happen anyway and it is a matter of corp policy on how softly this is handled. **(55**) I think that the headline wording needs to remain fairly concise. I am happy that it can be qualified (but only when that qualification enhances - not dilutes - the headline requirements. In this case I'm not sure that people will only report if acknowledgements/usefulness is recognised: in some sectors reporting is mandatory, and may be a regulatory requirement **(61)** I would remove or reword the third bullet. It implies to me that the reporter is the person responsible for the incident. I'm not sure this is helpful, as often it is the security community or others in the organisation which make the report. **(62)** Brevity is always good so I would seek to keep the extra sentiments but express them more succinctly - especially the third one, which is a tad verbose. **(72)** I hadn't thought of the third bullet, but it's a good point, directing the organisation towards "no blame" reporting. Given that, I don't think the benefits are limited to "staff that have been responsible…". I've come across too many occasions where "staff that had been involved in a security incident" were reluctant to report because of fears that they'd be blamed. Confidence that messengers won't be shot is important. **(74)** Provides clarity **(76)** Useful for comparison across industry sectors, especially for organisations like CERT-UK that may analyse national security posture. **(77)** " responsible for a security incident" – would adding "causing" reduce ambiguity? **(79)** The first bullet is not strictly true (because self-interest in not making the consequences worse if no report is made is a compelling factor); but the other two are useful. **(85)** Whilst the amended wording does enhance the original wording, the additional bullet points are, in themselves, slightly too long**.** **(87)** This may divide into two streams: 1. Encouraging reporting within an organisation (all bullets).	**agree it is.** **(53) O** **(55)O amended wording to include suggestion ensured compliance** **(61) O In line with other suggestions amended responsible and added involved in** **(62) O Third bullet reduced in line with other comments** **(72) P Amended as above to include involved in** **(74) P** **(76) P** **(77) O Amended as per previous comments** **(79) O** **(85) P with comments re length of comment. Now amended** **(87) O**

	2. Encouraging reporting within a community of organisations (definitely bullet 1; bullet 2 to some extent; bullet 3, not so much). **(89)** Extra words don't necessarily add value **-** in fact they are likely to deter readers and create an adverse impression of our profession. **(92)** The additional wording puts the requirement into context. **(93)** Not sure the 2nd bullet adds anything – mostly covered by 3rd . 3rd bullet suggest removing word extremely **(103)** The 3rd bullet point I do not believe should be included as part of the CSF. **(107)** Feedbacks on action taken could help in preventing further potential incidents. **(113)** Third bullet point could be shortened to "Feedback should reduce any anxiety felt by staff who report incidents" **(116)** Given everything that is written below – is it risk or impact. Interesting risk (!) of confusing or blurring the terminology usage.	**(89) O** **(92) P gives contrary view to others not so keen on changes. Demonstrates support for the CSF but differences of opinion in final wording.** **(93) O** **103) O Mainly refers to bullet 3 which attracted most comments** **(107) P** **(113) O again reference to length of third bullet – amended** **(116) O Added impact to clarify** **Note in Summary. Generally more supportive of changes. Some observations in general and most issues raised with length of or use of some words in bullet three which has now been amended to cater**

		for the comments made.
CSF	**Comments made (respondent number)**	**Notes on comments**
Element 4 Ease of making a report, recognising if incident reporting is difficult individuals will be less likely to submit them. This may particularly affect the reporting of near misses. The reporting process should: • Provide a sufficiently clear level of education and awareness to all staff in how the reporting process works. • Describe what an incident is. • Describe how to report it and what escalation needs to take place. • Sets out levels of expected feedback. • Be clearly set out as part of any governance process. Ease of making a report, recognising that if reporting incidents is difficult, individuals will be less likely to submit incident reports.". Re bullets Replace include with provide Describe no s Amended **Ease of making a report, recognising if reporting incidents is difficult individuals will**	**(2)** Care needs to be taken, if adding guidance to the reporting process, that that guidance itself is not too verbose with the risk of alienating those trying to submit an incident report **(6)** Incident reporting should follow the same process as any operational incident reporting. Start with a simple "Contact Wait Out" which alerts the receiving body, presumably now the NCSC UK, then follow up with a typical incident report – "What, When, Where, to Whom (with contact details), and How or Any Other Comment" Any incident report has to contain these facts to be useful. Don't make it any more complicated. **(7)**There may be many reasons why people do not report an incident; not all are covered here but, in my view, the wording is too long and focused to elicit a broad response. **(8)** The inclusion of near misses is a useful aspect to include in the factor, but the bullets are part of the explanation not the KPI itself **(16)** Without a clear and easy to use process that all personnel are aware of, efficient and effective incident reporting is a non-starter. **(17)** As above additional clarification useful in guiding implementation of any relevant incident reporting process and supporting interface / forms. **(24)** It clarifies it but does not improve CSF. I am also not sure about the reporting to describe what an incident is as by the time one gets to be making a report they ought to already be aware that they are making an incident report. The awareness should already be in place. **(25)** Describes how to report it and what escalation needs to take place. *Suggest only "How to report it" as this should cover all and then recipients should know how/if to escalate* Sets out levels of expected feedback. *Unclear if refers to submission or recipient - &/or acknowledgment of receipt of report or final outcome or both etc. Suggest need to acknowledge (where applicable - ie not confidential line) but minimise expectation of update to submission?*	**(2) O** **(6) O** **(7) O wording too long to be reconsidered** **(8) P** **(16) P** **(17) P** **(24) O** **(25) O** **(26) O Refers to**

be less likely to submit them. This may particularly affect the reporting of near misses. The reporting process should: • Provide a sufficiently clear level of education and awareness to all staff in how the reporting process works. • Describe what an incident is. • Describe how to report it and what escalation needs to take place. • Sets out levels of expected feedback. • Be clearly set out as part of any governance process.	**(26**) Consider also allowing anonymity or at least privacy, where appropriate or necessary to obtain honest and timely reporting	**anonymity as do some others. Need to check how many**
	(27) Do you want to include as part of the education and awareness what the key elements are for reporting an incident in order to have consistent language or have them report it in their own words… no right answer here… just a question	**(27) O**
	(32) What about more on a potential “no blame” culture to learn from incidents and instil an open reporting mechanism, which may mean there will be no comeback on the individuals concerned.	**(32) O Refers to a no blame culture**
	(36) The reporting process should also be flexible. If it is too rigid, people get frustrated trying to report on unusual incidents that don't typically fit a previous incident pattern.	**(36) O flexibility in reporting**
	(37) I agree. Simplicity, supported by a clear governance structure and guidance will ensure that the reporting process will be adopted.	**(37) P**
	(42) First sentence reads slightly awkwardly. It took a while before I understood it! Perhaps it may be useful to alter the sentence, along the lines of: "Ease of making a report, recognising that if reporting incidents is difficult, individuals will be less likely to submit incident reports.".	**(42) O suggested re wording**
	(45) A the end of the day, if reporting is difficult and/or time consuming, it will no occur. The more the process can be simplified and automated, the higher chance of acceptance and therefor success.	**(45) O**
	(**50)** The bullets are indeed critical otherwise staff will potential miss incidents that should be reported and acted upon.	
	(53) I think the key points are understanding what an incident is and how to report. By definition this will require some form of training which will be forgotten by the time of an incident and so Users need to know they are better off making a report if unsure. The incident evaluation process / personnel should then step in with the full procedure as part of the evaluation.	**(53) O**
	(55) I agree need to maintain/establish ease of reporting. I am less convinced that reporters should necessarily be visible to any (detailed) escalation procedures mechanisms	**(55) P +O**
	(61) I think bullet point 3 from the last page (Element 3) could be better placed here. I consider an important part of the KSF to be that that reporters	**(61) O perhaps clarify**

	know they will be taken seriously and the report handled in confidence. I don’t understand “and what escalation needs to take place” means. Does it mean how the incident will be investigated and who will be informed? **(62)** As above **-** I think it depends how the wording will be used. You have the “what” (ease of making a report) qualified by the “how”. Sometimes you only need the former, sometimes the latter. Five words to describe a CSF is pretty digestible! **(72)** This is heading towards “ease of making a high-quality report”. Good ☺ **(74)** Provides clarity **(76)** Listing the purpose of the incident report is a good idea as it is a learning opportunity **(77)** The reduction is due to the text sprawling a little. Present as Element 3, a short statement and then bullets giving context. Grammar is wrong in bullets “should describes”, etc. The education bullet perhaps should be “Provide” not “Include” for clarity. Expected feedback doesn’t make submitting a report easier. **(79)** Far too wordy to have any significant impact except a negative one (83) I am not sure whether bullet 3 is relevant to ease of reporting. Escalation is a different beast from reporting, but I might be missing the context. **(85)** Much like my comments above, the amended wording enhances the original; however, the bullets are, again, too long and could be refined to increase their impact further **(87)** The reporting process needs to be described in a way that is easy to assimilate **-** particularly as it's likely to be consulted under duress.. **(89)** We live in an attention economy: attention is in short supply, and great demand. People are less likely to read something if it is longer. Careful definition is valuable **-** but in my view, that is offset by the time people have to read it. The practitioners need to have a good grasp of the detail; it would be nice if the users had a good grasp but the price is probably too high.	**escalation to show appropriate due to seriousness of the incident** **(62) O** **(72) P** **(74) P** **(76) P** **(77) O clarity and grammar – done based on earlier comments** **(79) N re wordiness amended as per other comments** **(85) P but with comments re length - addressed** **(87) O** **(89) O**

	(92) Mick, doesn't the additional wording relate more to increasing awareness around incidents, rather than the ease of making the report? As such I have said that it doesn't increase the value orginal wording, but rather detracts from it. **(104)** Making it very prescriptive as to what an incident is may mean that some are not reported as it may not easily be related to the description. Better it is reported and for the ISO to determine whether it is an incident. Remain bullets again don't seem to add value. **(107)** Concise and simple report will help staffs submit a report. **(114)** I think that having a good template for the reports would be of great value. The template itself could guide the user thus making it easier to file a report and decide what is expected to be filled in each field. **(116)** Tricky really – would have assumed all of that to be inherent to the process anyway! But of course we know the risks with "assume"... ;)	**(92)O observation but purpose is to ensure staff know what is and what is not an incident** **(104) N feels bullets do not help** **(107) P** **(114) O suggested template may help** **(116) P**

CSF	Comments made (respondent number)	Notes on comments
Element 11 **3. Original wording (Element 11)** ***A recognition by senior management that incidents will happen.*** **3a. Amended wording:** **A recognition by senior management that incidents will happen and that they must play a full and active part in the incident management process by.** • Fully accepting that incident reporting is to be seen positively and not punitive. • Recognising security incidents are part of life and business and, like accidents, the reporting process is part of the prevention strategy. • Supporting a culture which encourages reporting • Recognising an organisation which handles an incident well enhances its reputation **A recognition by senior management that incidents will happen and that they must play a full and active part in the incident**	**(2)** There will undoubtedly be some instances where incident reporting leads to some punitive or disciplinary action on staff and this must be recognised by senior management – this is a tricky balance between the positive promotion of incident reporting whilst retaining the punitive elements of a careless data breach, for example. **(4)** The recognition is in part an indication that Senior Management understand the issues **(6)** This is all about management buy in and gets to the nub of modern security/risk/governance issues. To whom is an incident reported? The organisation's Security division is a good start but to whom do they report it? Time is often of the essence. Most Management won't want anyone to make a decision about external reporting other than the CEO since he is ultimately responsible (for loss of value as well as reputation). But if there was a death, for instance, the organisation would call for help (an ambulance) and for the police. They wouldn't wait for the CEO to tell them to. Cyber incidents can be equally critical – the life or death of the company. Management buy in implies trust in their governance sub-organisation (risk or security) to follow an internal process. There will be a reluctance by management/Board to call the Police/law enforcement. EDPR may help get over this. **(7)** There is a balance between not being punitive and taking action where incidents could and should have been prevented. Perhaps this could be recognised. **(8)** Suggest that this has now become two separate aspects – **one** that incidents will happen (i.e. does that recognition exist) and **secondly** that senior management play a role in resolutions (its not just technical issues) **(25)** Recognising security incidents are part of life and business and, like **H and S** accidents, the reporting process is part of the prevention strategy. • *Suggest no such thing as accident (ie RTA are now collisions as never a mere accident!??!) Replace with "Near miss"??* **(27)** Wording suggestion… that they play an integral part in the incident management process **(28)** Unrealistic expectation – incidents can reveal wrongdoing. There is insufficient disciplinary action taken as is without putting senuior managers	**(2) P** **(4) P** **(6) P with commentary** **(7) O include balance between not being punitive but taking action over recklessness (amended)** **(8) O comment this could now be considered as two aspects Recognition they will happen and active involvement by management** **(25)O good point re the reporting process should be seen as part**

management process by. • Fully accepting that incident reporting is to be seen positively enabling early mitigation action. Whilst recognising in some cases there will be a need to consider action taken where the incident should and could have been prevented. • Recognising security incidents are part of life and business and, like Health and Safety accidents, the reporting process is part of the prevention strategy. • Supporting a culture which encourages reporting • Recognising an organisation which handles an incident well enhances its reputation	under pressure not to act appropriately **(32)** There crux of the issue, management have to support and comments in amended wording echo my above comments. There is an intrinsic link to both points. **(36)** A few comments on this one: - It is also known colloquially as "Don't shoot the messenger" :-) - ...the reporting process is part of the correction strategy, or mitigation strategy... not the prevention strategy. if it was prevented, it would not have occurred and needed to be reported on. - the last comment is a double edged sword... recognising an organisation that handles an incident well, can also indicate an organisation that is experienced in working in incidents (or in crisis!) - that can also harm your reputation if it happens too often **-** but I think the point is you are attempting to provide support for the organisations effort. **(37)** I have found that those organisations where senior management take an active role generally have a positive attitude to security overall. A positive, and not punitive, approach shows a mature attitude that any incident can be used as a learning opportunity to improve the overall security structure. The reporting of 'near misses' really supports this approach, and I believe this ultimately reduces the potential for a serious incident. **(41)** I think it is critical to identify and qualify the term 'senior management.' Whilst senior management from a line management or operational perspective is critical so that incident reporting is seen as the norm and that support is required a crucial factor is whether the 'senior management' can actually be empowered to do something about it. There is a common scenario where IT Security can see the issues arising but are powerless to stop them as they are not empowered nor authorised to spend to prevent. Senior Management needs to play this part otherwise lessons learnt or prevention of re occurrence will not happen. Governenace is critical to the success of reporting. **(45)** Management must accept that incidents will occur. Management must also accept that a learning cycle is absolutely critical to reducing the frequency and severity of incidents. Failure of people and systems if part of	**of the prevention strategy** **(27) O suggested re wording but minor change and current wording unchanged** **(28) N unrealistic however that is the intention of the CSF to improve situation** **(32) P** **(36) P** **(37) P** **(41) P**

	life and often times not controllable. Failure to learn is very controllable. **(50)** Agreed – but this would certainly depend on the nature of the incident. For those incidents that are considered to be very serious then a full incident response Tem should be established to manage and reduce the impact. **(53)** This is a "keeper", best definition I have seen on this aspect. **(55)** Agree entirely **(57)** recognition of the inevitability of incidents occuring assists the security function greatly to follow up on all reports where there may be a feeling that all incidents are, at least partially, due to their own failings. **(62)** Same comment as above. I evidently like the snappier approach more but the additional clauses certainly help explain. **(63)** very important point which it seems to me is missing here is that senior management (leaders?) need to see incidents and near misses as significant learning opportunities so that they are not repeated. If they are repeated, generally senior managers have failed their organisations. Senior managers need to monitor the volume and nature of reports and whether subsequent action/feedback has taken place. What you measure you change - and this is about changing behaviour and the way things have always been done. But is this about reporting or leadership and incident mitigation/resilience? **(74)** Again, provides clarity **(77)** Senior management should also be responding personally to incident management actions relevant to them, supporting by doing. "Fully" and "life and" are unnecessary. **(79)** Almost encourages people to think that there will be no disagreeable consequences for them personally (as distinct from less severe ones if they report incidents and the reverse if they don't). The balance between 'stick and carrot' is difficult to get right, but a too benign management posture is likely to encourage the development of a poor compliance culture. **(85)** As above (Much like my comments above, the amended wording enhances the original; however, the bullets are, again, too long and could be refined to increase their impact further) **(87)** Prompt reporting can result in early and effective mitigation.	**(45) P** **(50) P** **(53) P** **(55) P** **(57) P** **(62) P** **(63) P** **(74) P** **(77) P plus comment to change wording but not changed as supported elsewhere** **(79) P but need to ensure there are actions taken where recklessness comes in (wording amended)**

	(89) We live in an attention economy: attention is in short supply, and great demand. People are less likely to read something if it is longer. Careful definition is valuable **-** but in my view, that is offset by the time people have to read it. The practitioners need to have a good grasp of the detail; it would be nice if the users had a good grasp but the price is probably too high. **(92)** I think the additional wording is important to encourage reporting, and to provide additional information for management to respond appropriately. **(93)** 1st bullet – nut punitive is not a good description. The wording needs to reflect that the if the incident is a first offence and/or not malicious it will not lead to disciplinary action **(113)** At some point there has to be a punitive element. If I as a security manager leave a report on a train I would expect a dressing down. **(116)** Rewording required? That they must play a full ... who is the they? Obviously it's senior management but that could be mis-read (deliberately or otherwise) – be careful! ...to be seen positively and not **punitively** (perhaps??)	**(85) O reduce length of bullets** **(87) P** **(89) P** **(92) P** **(93) again comment re not punitive need balance re reckless (wording amended** **(113) O same again re punitive (wording amended)** **(116) O rewording suggestion and also refer to punitive (wording amended)**

CSF	Comments made (respondent number)	Notes on comments
Element 13 4. Original wording (Element 13) ***Incident analysis that considers root causes and wider systems/processes, not just the initial impact assessment.*** **4a. Amended wording** **Incident analysis that considers root causes and wider systems/processes, not just the initial impact assessment. This is crucial to understanding what actually contributed to an incident otherwise if the true cause is not identified repeat incidents or larger scale impact ones can occur.** **It should be recognised:** • The incident may be just a symptom of a larger organisational or process flaw. • Superficial investigations may be counterproductive in the long term **Incident analysis that considers root causes and wider systems/processes, not just the initial impact assessment. This is crucial to identifying what actually contributed to an incident in order to ensure repeat incidents do not occur.** • The incident may be just a symptom of a larger organisational or process flaw. • Superficial investigations may be counterproductive in the long term	**(4)** Root cause analysis is important in deciding if an event or issue is systemic, but it should only form part of the lessons learned review. Issues can be reoccurring but not systemic.	**(4) P**
	(6) Too wordy and doesn’t add much to the original text.	**(6) N too wordy (amended)**
	(8) In my view, the added explanation does not strengthen the view that root cause analysis is important	**(8) too wordy (amended)**
	(16) Consideration of root causes is vital in learning lessons about security incidents and prevention of re-occurrence/similar incidents in the future	**(16) P**
	(17) Yes clarification useful. Not sure about wording of …“**or larger scale impact ones can occur**” May be better to replace ones with “**incidents**”?	**(17) O suggested re rewording (amended)**
	(25) *Suggest also add to be recognised:* *“Identify / highlight any training development needs or gaps”*	**(25) O suggested re rewording (amended)**
	(27) Wording suggestion … **Incident analysis that considers root causes and wider systems/processes, not just the initial impact assessment. This is crucial to *identifying* what actually contributed to an incident in order to ensure repeat incidents *do not occur.***	**(27) O suggested re rewording (amended)**
	(32) Amended wording does then not imply what identification of root causes will help focus mitigation and education strategies into those areas?	**(32) N**
	(35) Without detailed analysis the true means of attack and the motivation of the attacker may not be known and so future remedial action may not adequately address the treat	**(35)P**
	(36) Another area that should be recognised: - The incident is often a combination of multiple technologies or processes that have built up over time, and only a complex set of coincidences causes the incident (i.e. one that was previously unknown because it either had not happened previously, or not diagnosed previously).	**(36) P and comments**
	(37) I think this adds further clarity to the purpose of incident analysis and the fact that it is a deeper investigation to get to the root of the problem and not dealing with the obvious symptoms.	**(37) P**
	(41) You could equate this to a vanguard attack and concentrating all your resources to tackle that threat whilst missing the flanking manouvres which is the real killing blow or the surgical strike.	**(41) P plus comments**

• Identify/highlight any training/development needs or gaps **or** Incident analysis that considers root causes and wider systems/processes, not just the initial impact assessment. It must recognise that: • **It is important to identify what actually contributed to an incident in order to ensure repeat incidents do not occur.** • **Analysis may** identify/highlight any training/development needs or gaps • **The incident may be just a symptom of a larger organisational or process flaw.** • **Superficial investigations may be counterproductive in the long term**	**(45)** RCA goes to the heart of incident analysis. Knowing the what of an incident is only have of the equation. Knowing the why will reduce reoccurrence and lead to a better understanding how to prevent similar incidents. **(47)** I am not sure if the following: "otherwise if the true cause is not identified repeat incidents or larger scale impact ones can occur." adds any value to the statement. I think this element is covered by the rest of the statement and the two bullet points. (49) ITIL deals with Incident and Problem management effectively therefore the process should be no different when a security incident is raised if this best practise methodology is adopted. **(50)** It is vital that Organisations understand what factors either caused or contributed to the incident in the first place so that future incidents can be prevented. **(53)** The wording is now too long and is covered by my definition of "root cause". I suggest the following is unnecessary, " **This is crucial to understanding what actually contributed to an incident otherwise if the true cause is not identified repeat incidents or larger scale impact ones can occur."** **(55)** Again agree entirely. Root cause analysis represents a step up the maturity scale for a proactive and intuitive incident reporting n methodology; it's a characteristic of embedding it into a culture (61) I think the initial bold text is too long. Can you move part of this into the bullet points below to make the KSF shorter and snappier. (62) This one got too wordy and repetitive for me. (63) Again here, I think that it would be useful to make explicit reference to the need to identify lessons and the action needed to ensure as far as possible that they are not repeated **(72)** I'd prefer to take this in the direction of "Otherwise the organisation will learn nothing to help it prevent future incidents **(74)** As before, provides clarity	**(45) P** **(47) O comment re wording (amended)** **(49) O** **(50) P** **(53) N Too wordy (amended)** **(55) P** **(61) N Too wordy (amended)** **(62) N Too wordy (amended)** **(63) O comments** **(72) O comments** **(74) P**

	(77) Again, structure to focus on short core statement then supporting text. “crucial” may at times be an exaggeration. The root cause might just be different to what was expected, rather than deeper or wider – and if not identified still wastes mitigation effort. “counter-productive” may be too strong – few will make the company worse, some will however waste time and effort. **(79)** The additional commentary strikes me as self-evident. **(85)** Overall, the amended wording is too long; however, the additional bullet points are worth including. I would suggest words to the effect of Incident analysis that considers root causes and wider systems/processes, not just the initial impact assessment. It must recognise that: • The incident may be just a symptom of a larger organisational or process flaw. • Superficial investigations may be counterproductive in the long term **(87)** Some incidents may not merit an in-depth investigation. **(89)** Keep it simple ! **(91)** Differentiate impact between whole system or part of system **(92)** A lack of understanding in identifying the root cause is critcal for responding. **(93)** Wording could be tidier! In main text 2nd bullet need to justify statement **(110**) I dislike the word "just" **(116)** This is duplicative again – given the suggested PIIA below – post incident impact assessment – that’s what this is already suggesting be done. Element 8 and Element 13 therefore need to be revisited with a view to reducing duplication.	**(77) O comment re text** **(79) P** **(85) O wordy but relevant (wording has been amended)** **(87) O** **(89) O may refer to wordiness (amended)** **(92) O** **(93) O comment re wordiness (amended)** **(110) O** **(116) O re possible duplication on CSF 8 and 13 (8 not considered as a CSF so noted)**

Possible CSF		
Possible CSF	**Comments made (respondent number)**	**Notes on comments**
Element 2 ***Collection of reports of near misses as well as actual incidents*** **2a. New wording** **Collection and review of reports of near misses as well as actual incidents. Recognising;** • Much can be learnt from near misses • By doing so can identify the required preventive measures that need to be in put in place to deal with organisational learning and/ or a change in policy & procedure to ensure that such near misses do not, in future become actual incidents Suggested re wording **Collection and review of reports of near misses as well as actual incidents. Recognising;** • First bullet removed as superfluous • By doing so can identify the required preventive measures that need to be implimented to deal with organisational learning and/ or a change in policy & procedure to ensure that such near misses do not, in future, become actual incidents	**(2)** I agree with the second bullet point – I don't think the first adds any value, it is too ambiguous **(6)** What's a near miss? Won't be known until well after the event and until other 'near misses' are analysed. Hence the wording is a non sequitur. All incidents should be reported that have clear negative impact on an organisation. The fact that later it turns out to be a technical anomaly doesn't matter. Organisations stand alone. They probably have no idea what is going on elsewhere. Reporting centres – NCSC UK – do have the breadth of scrutiny and analysis to fulfil this function. Hence why NCSC UK (and its predecessors) should be joined at the hip with Public and Private sector organisations. Perhaps this needs to be rethought – what parameters define the threshold for reporting? Much more about impact on the organisation than , say, 'actual' or 'near miss' ctriteria. **(8)** Near miss information undoubtedly is useful – I would think that the length of explanation is less important than the aspect exists in the full set of factors **(12)** Need to be careful do not hold too much data so would need careful management. **(15)** Could this be rolled in as an additional bullet point of question 2? Meaning element 4 **(27)** Wording suggestion.. By doing so *we* can identify the required preventive measures that need to be ~~in put in place~~ *implemented* to deal with organisational learning and/ or a change in policy & procedure to ensure that such near misses do not, in future become actual incidents. **(32)** And linking together themes of minor near misses which reported in isolation have no enhanced risk but when combined may actually escalate the risk and impact to that of an incident? **(36)** Probably another dot point recognising that the business may decide that a near miss may be within risk appetite -- i.e. the cost to add extra preventative controls may move the organisation to an unacceptable cost point.	**(2) P but feels first bullet superfluous** **(6) O has a point but often near misses are not considered incidents hence the inclusion** **(8) O** **(12) O** **(15)) not really element 4 is about ease of reporting** **(27) O suggested wording (amended)** **(32) P** **(36) O good point (considered for amendment but should be identified in**

Or - By doing so can identify the required preventive measures needed to ensure that such near misses do not, in future, become actual incidents	**(37)** Again, this adds further clarity to the need to report near misses. I think it is important to stress that near misses will continually occur as the threat environment evolves in their attempts to bypass defences. Near misses allow the observation of that evolutionary process and can allow the organisation to adapt to maintain its protective measures.	**incident analysis as accepted)** **(37) P**
	(41) Interesting **-** I think that a combined near miss reporting log could identify a major incident before it happens if used properly. The fear is the near miss could be symptomatic of poor education, reporting etc....	**(41) P**
	(42) While this is a great idea and may be a useful tactic in future, at the moment, I think the priority (for the limited resources) is probably dealing with actual incidents. I didn't know how to rate this one, because on the one hand, I think the wording significantly improves the element, but on the other hand, I don't think it should become a CSF (because it may divert resources away from dealing with actual incidents). If I'm wrong and resources would be available for analysing near misses, then I'd rate this element as a "1".	**(42) P with comment that more important to focus on real incidents**
	(45) The US Federal Aviation Administration requires the recording and reporting of near misses as well as contact incidents. The data can be used to determine changes in processes and procedures that will not only reduce the likelihood of a near miss, but also contact incidents. The data for near misses in cybersecurity incidents would have similar utility. I do not consider it to be a critical success factor, but would rate its utility as high as a non-critical success factor.	**(45) P plus comments**
	(47) I strongly believe that collection and analysis of near misses should be a Critical Success Factor for any Security Incident Reporting system	**(47) P**
	(50) "Yes" this is important data to collect and monitor especially if the near misses are all of a similar nature – however it may be that the processes already in place may be preventing the new miss from actually becoming a full incident. The processes should be reviewed to ensure thay are still appropriate and up to date.	**(50) P**
	(53) First bullet unnecessary. **(55**) Back on culture theme it should be recognised that near misses – or	**(53) O another comment re first bullet**

	Practices Dangerous to Security – are at least as important to identify as actual compromises: lessons learned can help to prevent rather than just react **(57)** Near misses are extremely valuable as they can provide insight into potential vulnerabilities and allow changes to prevent actual incidents occuring. **(62)** I do believe near miss recording and analysis is important but the extra clauses (in fact the second one) detract from the clarity of the original wording, in my view. Too verbose - and to be honest not that well written (*who* can identify…?). **(63)** It follows from my comments above that I think that it is essential that near misses are reported and lessons identified and applied. The ambition here should surely be to mirror the airline industry which loses no opportunity to learn from experience **(72)** Slightly tricky to decide whether this should be promoted, as you also added near misses to Element 4, so they are already included within the list of CSFs! **(76)** Near misses are important as they provide opportunities for learning and perhaps procedural changes. **(77)** 2nd bullet is more an explanation of the first than separate. And doesn't include all possible long term measures – e.g. more tech might help in some cases **(79)** Intelligent analysis of the metrics on near misses can inform the creation of initiatives to address weaknesses in compliance. An example is personal data breaches which may not meet the gravity threshold for notifying the ICO but can point to weaknesses in compliance in individual business areas and the need for bespoke action. **(85)** Whilst I have scored this Element at 3 (on the basis that it should remain where it is and not become a CSF) I think that the amended wording is an improvement on the original. **(87)** I'm not sure how helpful this will be. There are likely to be more 'near misses' than actual incidents. Given the porous nature of layers in a multi-layered defence strategy, each event blocked inside the outermost layer is potentially a 'near miss'. **(89)** The extra words don't add enough value. **(93)** 1st bullet adds nothing not covered by the second	**not needed (bullet now removed)** **(55) P** **(57) P** **(62) O wordiness (amended but not directly as a result of this comment)** **(63) O another comment re mirroring air industry** **(72) O again reference to 4 but this is ease of report not type of.** **(76) P** **(77) O** **(79) P plus comments** **(85) P** **(87) O** **(89) N**

	(96) I think it’s actually impossible to separate “near misses” out anyway. Sometimes what could be originally reported as an incident is later found to be a near miss e.g. an unencrypted disk of sensitive information is thought to have been lost in the post resulting in frantic searching involving Royal Mail as well as the recipients, calls to the ICO, risk mitigation put in place, worsecase scenario Osman warnings when Ooopsy –two weeks later it is found to be still in the “out tray” of the post room after all. Furthermore, an officer might not realise the full consequences of what they might view as a near miss. **(113)** Actually I think it improves it, but doesn't make it a CSF. The same comment applies to the following two questions also **(115)** possibility of risk that to analyse near misses may create additional work. Always good to add the ‘why’ to the ‘what’. Sometimes this type of analysis falls into the too complicated, too challenging, too expensive box. Needs high level recognition to get necessary resource. **(116)** Difficult wording – suggest revisiting to remove clumsiness?	**(93) 3rd comment re bullet 1 now removed.** **(96) O** **(113) P** **(115) P** **(116) wordiness - amended**

Element 7 Mandatory Reporting **7a New wording** **The reporting of incidents should be mandatory. An organisation cannot mitigate any impact or learn from an incident unless there is an awareness something has happened. Recognising:** • A true record of incidents can provide accurate management information which enables amongst other things; trend analysis, a greater understanding of actual rather than perceived threats and risks and more evidence based resource allocation. • Although the decision to report should not be optional the actions taken should be tailored to the incidents severity. For example a manager should have some discretion to deal locally with minor issues such as not locking computer screens or not complying with the clear desk policy. • Staff need clear guidance on what and how to report. **The reporting of incidents and near misses should be mandatory. An organisation cannot mitigate any impact or learn from an incident unless there is an awareness something has**	**(2)** The mandatory reporting of incidents will provide an accurate picture of the information risk. Certainly in my organisation I don't have a clear picture of information risk from security incidents as the reporting is not as good as it should be **(6)** Suggests see comment made by (6) and combine the two **(8)** I'm not a fan of mandatory reporting in general – I think it can be a disincentive and risk creating too much noise **(12)** Totally agree with the second part and struggle somewhat with the mandatory requirement, staff should report as a matter of course and because they want to – but I appreciate why it may have to be mandatory. **(17)** Two areas key: Recognition by senior management that security incidents will occur Recognising that staff may be anxious and that feedback and appropriate action should be undertaken **(25) The reporting of incidents should be mandatory.** *Suggest include* **T**he reporting of incidents **and near misses** should be mandatory. **(26)** I don't consider this to be a helpful or practical stance. It might even be counter-productive. You can't monitor, audit or police it. If reporting is encouraged, easy to do and rewarded, then it will be successful. **(32)** Much better break out **(35)** is this in relation to intra-organisational reporting or extra-organisational. If we are saying that it is mandatory for external reporting the benefits and potential implications must be clear **(36)** Agree with all this. **(37)** I think this adds more depth to the statement, making it clearer that the actions initiated by a report will vary depending on the risk associated to the incident. **(45)** Reporting should be mandatory. With regard to cybersecurity and reporting in particular, I am always reminded that "absence of evidence is not evidence of absence". Put simply, we can not fix that which we do not know is broken. **(47)** I would add "near misses" to the wording, something along the lines of:	**(2) P** **(6) O** **(8) N** **(12) P** **(17) O comment may be wrongly placed in this section** **(25) O suggested wording change (amended)** **(26) N** **(32) P** **(35) O** **(36) P** **(37) P** **(45) P** **(47) P another comment re adding near misses (amended)**

happened. Recognising: • A true record of incidents can provide accurate management information which enables amongst other things; trend analysis, a greater understanding of actual rather than perceived threats and risks and more evidence based resource allocation. • Although the decision to report should not be optional the actions taken should be tailored to the incidents severity. For example a manager should have some discretion to deal locally with minor issues such as not locking computer screens or not complying with the clear desk policy. • Staff need clear guidance on what and how to report.	"The reporting of incidents and near misses should be mandatory."	
	(50) Reporting must be mandatory and that is why it is essential that staff have clear guidance as to what is an incident, breach or near miss etc so that they can report these with ease.	**(50) P**
	(53) Re bullet No 2, this should be tied back to 2a Element 4, i.e. definition of an incident and ease of reporting.	**(53) O comment**
	(55) Not sure that the sense of why something is mandatory is reflected here. Agree however that response and follow up should be proportionate to severity/likelihood of future event/benefit to organisation	**(55) O**
	(61) I think this might be a KSF, however, your comment infers that not locking a screen needs to be reported. I think this is only practical in some environments, not all e.g. commercial / academic. Making such a blanket statement could reduce the value of the KSF for these less security conscious environments. I also suggest that if a manager really needs to report incidents like this, some aggregate reporting like "number of unlocked screens this month" and any serial offenders would be sufficient.	**(61) O Comment suggests not recording unlocked screens but then refers to how many times unlocked. If not reported this cannot be achieved.**
	(62) I like the additional clarity here. There may be something about a severity threshold for reporting though I worry that could be used as an excuse not to report something.	**(62) P**
	(63) I do not think that the comments apply to "Mandatory Reporting" which I took to mean external reporting. The additional wording suggest that this is internal process and is probably covered adequately in the CSFs above.	**(63) O comment re is it internal or external reporting**
	(72) This is all true, but I don't think mandatory reporting is as important as the factors already on the list	**(72) P**
	(74) A process for anonymous reporting for those individuals that feel, for whatever reason, they cannot report in person.	**(74) O suggest anonymous reporting**
	(76) There should be manager discretion regarding the lower grade incidents, otherwise we will be inundated with incident reports, the majority of which will be minor indiscretions.	**(76) O**

	(77) Certainly an improvement, not fully sure a CSF. Some aspects of statement might relate to other than the mandatory nature	**(77) P**
	(79) The bullet points are a touch wordy and reduce their impact.	**(79) O wordiness (amended)**
	(83) I am not a big fan of mandatory rules, believing that it is better to win hearts and minds	**(83) N**
	(85) This is an improvement, sufficient to promote it to a CSF; however, it is again too wordy and could be refined.	**(85) P refers to wordiness (amended)**
	(87) This seems to be leaning towards an impact assessment. There could be a risk of the incident landscape being dominated by minimal-impact events.	**(87) O**
	(89) The extra words don't add enough value.	**(89) N**
	(93) On second bullet it should still be reported upwards perhaps just as a notification with no names/details as knowing that for instance a lots of screens are left unlocked may indicate the need for awareness raising	**(93) O**
	(103) I struggle whether this should be a CSF or not, even with the amended wording. An organisation should have a culture of reporting, not because it is mandatory but because they have awareness of the benefit it will bring to the organisation. Mandatory reporting can give a negative perception. Also - how can it be enforced?	**(103) O re whether a CSF**
	(113) (*Actually I think it improves it, but doesn't make it a CSF. The same comment applies to the following two questions also)*	**(113) P but not sure if a CSF**
	*(***116)** Presumably this is deliberately noted separately from “ease of making a report”? It feels duplicative to raise the issue again here given that if you’ve made incident reporting easier – in doing so, the communication will (or should) have included the fact that it’s not optional	**(116) O**

Element 8 ***Standardised risk assessment (to determine the impact of the incident)*** **8a New wording** **Having Standardised risk assessment (to determine the impact of the incident) whilst recognising:** • There are advantages to standardise within a single organisation or sector but wider standardisation can be a challenge. • Risk and impact assessment are essential as part of post event and incident management criteria. An initial standard approach will enable comparison of similar incidents and facilitate fact-based resolution.	**(2)** How would this standard approach work in the current move from quantitative risk assessment methodologies. A risk assessment approach based on organisational risk appetite at either a local or national level would seem to be sensible **(6)** Don't re-invent the wheel on risk assessment. Follow the Standard. But also, discriminate between risks and issues. Also a CEO should be reporting to his Board on the three most important risks to his organisation each Board Meeting. Most organisation's risk registers don't allow that as they contain a mixture of risk and issue, small to major risk, mitigation and control. Risk Registers are important but they need to focus more on tactical, operational and strategic risk. CEOs will want to know when risks move between categories (T,O,S) and will report on that. **(20)** There will be some improvement within an organisation in a standardised risk assessment process. However a standardised risk assessment process within a whole sector such as the Police Service or even wider, the whole of the Public Sector would allow proper comparison between Police Forces or Public Sector agencies. That cannot be achieved if each single organisation is adopting risk assessment processes which are different and therefore not comparable with similar forces or public services. **(25** (26) This is certainly helpful but it would be a stretch to call it critical for success. **(28)** Here, Here! **(32)** Some things can be dealt with by standard processes, but most incidents have their own individual touch points and only a subset of normal processes may be prudent to follow. I would add in tailoring to the environment and severity. **(35)** The standardisation must be at a sufficently high level to allow for multiple different types of incident or near miss. the danger of a too proscriptive assessment may result in a 'one size fits none' **(36)** Probably another dot point recognising that risk appetite is a lever -- i.e. the cost to add extra preventative controls to reduce the risk may move the organisation to an unacceptable cost point (as above). **(37)** I agree. This statement places a boundary for the scope that risk management can take. It is highly unlikely two organisation, even within the	**(2) O** **(6) N** **(20) O Commnets in general** **(25) O Comment re whether a CSF or not** **(26) O Comment re whether a CSF or not** **(28) P** **(32) O**

	same sector, are likely to view risks in the same way. Therefore, clarifying that the risk management process can only really work at the organisational level helps to give that organisation a consistent view of the risks they perceive to face. It also give a clear picture to those throughout the organisation as to how it views security and wishes it to be treated. **(41)** Commonality of resolution is important especially with business context, the use of which could standardise contingency approaches to the next incident whomever takes the incident on. One of the challenges will be the availability of the information at the time of decision making. Standardisation will rapidly reduce the amount of time of converting data to meaningful outputs. **(45)** An RCA should trigger a remedial risk assessment of the systems of which failed. Dependent systems should also be a part of the remedial risk assessment. This is certainly an area that would be covered by an auditor and/or regulator. **(49)** Rather than standardising the RA, a better assessment method would be to create an approach that was flexible enough to cope with all aspects of risk regardless of the business sector or government organisation and/or their risk acceptance levels. **(50)** Again I would state that Risk and Impact Assessments offer good value depending on the nature of the incident. So for medim and major level incidents “yes” but for minor incidents and breaches “no”. **(55)** Yes re standardised framework – but that framework should be granular enough to allow flexibility and pragmatism in response. **(61)** Consider adding that the risk assessment output should be suitable for automated analysis e.g. can be easily included in a database or excel file. Ideally this would be quantative but in most cases I expect low/medium/high type semi-quantative ratings are most practical. **(62)** I don’t even believe that risk assessment does determine the impact of an incident. An incident has happened; a risk has not. I don’t think this one makes sense. **(63)** is is not a CSF according to my intepretation of the definition. **(72)** As with element 7, it’s all true, but I don’t see this as the same level as the existing CSFs **(74)** Useful for comparison across industry sectors, especially for	**(35) O** **(36) O** **(37) P** **(41) O** **(45) O** **(49) O** **(50) O** **(55) P** **(61) O suggested additional wording (not taken up)**

	organisations like CERT-UK that may analyse national security posture. **(76)** The advantage of standardised risk assessments is that the incident management should be easier to interpret across the organisation making prevention and resolution easier. **(83)** But care must be taken to avoid the ‘tick box’ approach to risk assessment which can creep in with standardisation. **(85) As above (**This is an improvement, sufficient to promote it to a CSF; however, it is again too wordy and could be refined.) **(87)** The true impact of an incident (eg. punitive fine by the ICO) may not emerge for some considerable time after the event. The assessment mechanism may need to take this into account. **(89)** Extra words are justifications, and in my view do not add value. **(107)** The standardised assessment helps in increasing awareness and improving the quality of incident management. **(113)** *Actually I think it improves it, but doesn't make it a CSF. The same comment applies to the following two questions also* **(115)** Mike, not sure if I am missing a point here about the terminology. Risk assessment is something that should happen before an incident in order to reduce or mitigate the potential impact. This is a proactive activity. I would suggest that the post incident activity is an ‘Impact assessment’, which will identify what damage has been done following an event. A standardised impact assessment methodology is essential. This is a reactive activity. **(116)** It seems confusing. Risk assessment of what? Impact of the incident on what? It’s very broad – the whole business? The “bottom line”? I would counsel about confusing risk assessment and impact assessment in this way... it’s a post incident impact assessment that’s required (I feel a new acronym coming on! PIIA). There should already be a risk assessment in place that would have identified the likelihood and impact of the incident occurring; the fact that the incident has now occurred means that the risk assessment needs to be revisited to establish whether someone got the scoring wrong or misunderstood the purpose of the risk assessment.	**(62) N** **(63) N** **(72) O not supporting it as a CSF** **(74) O** **(76) P** **(83) O** **(85) agrees it could be CSF but wordy (already amended due to earlier comments)** **(87) O** **(89) O** **(107) O** **(113) P but not a CSF** **(115) N re use of risk assessments** **(116) N**

APPENDIX 11

CITY OF LONDON POLICE

Ian Dyson QPM
Commissioner

Direct line
xxxxxxxx

19th December 2016

Dear Colleague,

Request for support in research into improving the reporting of information security incidents

As the current Chair of the National Policing Information Assurance Board I have been supportive of the PhD research into information security incident reporting undertaken by Mike Humphrey, Head of Information Assurance at the National Crime Agency. Mike is doing his PhD as a part time student at the Defence Academy of the UK, Shrivenham, Cranfield University.

Mike is an active member of PIAB as well as the Incident Analysis Review Group (IARG), a sub group of the PIAB that review the results of the central reporting of security incidents that you contribute to from your force area.

I have been keen that the police service understands what security incidents are happening. If we do not know what type of incidents are occurring, it is extremely difficult to put in place the appropriate and relevant advice, guidance, controls and countermeasures to reduce or prevent their reoccurrence.

During the last year Mike has conducted a series of research surveys into identifying the Critical Success Factors required to improve security incident reporting. Security professionals from the public and private sector, academia and military across the UK, Europe and further afield took part. The respondents included a number of UK police force Information Security Officers and other police staff.

Cont/ …

Mike is now distributing an Incident Reporting Maturity Model to those who have responded to that research. This contains the details of the four Critical Success Factors identified as most likely to improve security incident reporting within an organisation. The main purpose of a maturity model is to identify a gap that can be closed after following improvement actions.

He is asking those police force information security professionals who took part in that earlier research to also find time to respond to the questions on the Maturity Model.
I would particularly ask that those of you who were not aware of, or unable to take part in his earlier research, to participate this time acting as a control group to review the model. This way he will have views on the maturity model, not only from those who have contributed to its formation, but also those exposed to it for the first time.

May I assure you neither he nor I are asking you to score your force and send in the results. He is asking that you assess the maturity model for its applicability in determining the position of your force in relation to those Critical Success Factors. You are of course at liberty to use it for that purpose for your own benefit.

Mike has attached a short explanatory letter as well as the maturity model and incorporated questionnaire.

I would urge that you find the short period of time from your busy schedules to answer the questions Mike is asking about that maturity model.

Ian Dyson
Commissioner

APPENDIX 12

Copy of email text sent to Police Service Control Group sent 27/12/16 17:34 attachments to this e mail were the introductory letter and a word and PDF version of the IRMM

Dear colleague,

Please find an explanatory letter from Ian Dyson, Commissioner of the City of London Police, regarding my research into the reporting of information security incidents, together with a word and PDF version of a questionnaire.

The contact list, which contains your email address, was supplied to me by [Redacted] with Ian Dyson's permission. For some forces more than one person is listed. As I am only interested in security professionals views, not a forces perspective, more than one response from a force is not a problem.

Some of your colleagues will have already taken part in earlier stages of my research and will shortly receive a separate message regarding this final stage. For those of you who are not aware of what I am researching the below should help you understand the short amount of time that I would ask that you find to assist me in the final stages of my research.

I am a part time PhD student at the Defence Academy of the UK, Shrivenham, Cranfield University. My PhD research focusses on security incident reporting. My day job is that of the Head of Information Assurance at the National Crime Agency. I am a Fellow of the Institute of Information Security Professionals (IISP) and an elected member of the Information Assurance Advisory Councils' (IAAC) management committee.

I had come to a stage in my research where I needed to seek the views from information security professionals on what could be considered the Critical Success Factors required to support the security incident reporting process. During the last year I conducted a survey of information security professionals across law enforcement, central and local government, the private sector and academia from the UK, Europe and further afield. The results of that research have identified four Critical Success Factors which are believed to be key in improving the reporting of security incidents.

From this I have created a Security Incident Reporting Maturity Model. The purpose of the model is for organisations to be able to judge if, and how well, any or all of these critical factors are embedded within their security incident reporting process. The main purpose of a maturity model is to identify a gap that can be closed after following improvement actions.

I am sending the maturity model and questionnaire to those who contributed to that research. However, I also wanted to send the model and questionnaire out to a control group of security professionals who had not, for a number of reasons, been able to take part in the original research. This will enable me to gauge its suitability and usefulness from those who have not been exposed to the rationale and process of determining the Critical Success Factors which provide for the model's content.

The enclosed maturity model questionnaire contains the four Critical Success Factors (CSF) identified through my research that are considered the most likely to improve the reporting of security incidents. I have included them within a maturity model and it is your views on the model that I am seeking. There is also the facility within the questionnaire to add any comments. The maturity model pages are greyed out to show there are no questions on those pages that require answering for my purposes. You can of course use the model for your own benefit.

Completion of the questionnaire should take no more than 15 minutes. For the purpose of this study, as there is no universally accepted definition of a security incident, I am using one I have crafted for my thesis:

An information security incident is either, an actual or potential event that has, or is likely to, cause harm to the confidentiality, integrity and/or availability of data, assets, systems or infrastructure whether caused by people, processes or technology.

I would now ask that you view the enclosed maturity model to comment on if this was provided to your organisation, or those for which you may be assessing, whether it is:

1. Understandable
2. Usable
3. Considered to be of value to asses where your organisation sits regarding the deployment of the identified CSFs

The response form is simple to complete and uses a Likert scale of 5 options and some simple yes no answers. There is a facility for you to add any comments or observations you feel can assist in its final version.

I appreciate you may have both positive and negative views regarding maturity models. I would ask that for this exercise that you judge the maturity model as a potential benefit to any organization to assist in improving the number of incidents that are reported.

The aim of such a maturity model is to identify if the particular Critical Success Factor is in place and, if so, to what extent. It is not an iterative maturity model. In other words you do not have to score well in one before you can score another. They can be assessed individually with regards to the current situation.

I am not asking that you score your organization as part of this survey and send me the response, as this may be very sensitive. You are of course at liberty to do so for your own internal benefit. I recognize that in any template or model the language, terminology and contextual wording required may be different and relevant to the sector (e.g. law enforcement, finance, energy etc.). As a result you will notice the maturity level descriptions have been kept to simple descriptions. Therefore please bear this in mind and, of course, you are free to add any comments regarding the level descriptions in your response.

In addition, I provide reassurances regarding confidentiality of any responses. These are set out in the maturity model questionnaire.

I have enclosed two versions of the maturity model questionnaire, as a word form and as a pdf form (whichever is easiest for you to complete).

Please note; some research respondents had difficulty where they completed previous surveys but did not save it as a separate document and then returned the unsaved one to me. With some versions of mail and office document management, if you complete the form as it arrived without renaming and saving it, when it is sent back to me your response will be blank. So please save your response and then send that saved version.

There is an option of printing the form, completing it, scanning the response and then emailing to me the scanned version. Alternatively you can print and complete it and then post it to me. All these options are open to you.

I would be grateful if you could return your answers to my university email address m.humphrey@cranfield.ac.uk or, if you prefer post to me at the address shown in the questionnaire instructions.

May I thank you in anticipation of your participation. I am really grateful for your valuable professional input into my research.

Please can you complete and return the questionnaire by Sunday the 15th January 2017.

I do hope you can find the time to add your valuable contribution to the research. Thank you for reading this.

Regards,

Mike

Mike Humphrey MSc. F.Inst.ISP

APPENDIX 13

Copy of email message sent to Delphi group regarding participation in the Validation Study

Dear [insert name],

Firstly, may I thank you again for taking the time to be involved in my Delphi study research questionnaire into Security Incident Reporting. I had a very positive response, with many of you adding valuable comments in the spaces provided next to the elements. A large number of respondents also completed round 2 (74%) and equally provided a quality range of supportive comments, suggested alternative wording and other observations.

Your comments, both from round one and round two of the Delphi survey, have been taken into account to assist in the formulation of the final wording of the elements identified as Critical Success Factors (CSFs). As a result I believe I now have a consensus as to the Critical Success Factors to improve security incident reporting and the wording of them.

I did say that once I had analysed the responses I would contact those who did respond with details of my findings. I am now asking that, whether you completed round one or both rounds that you look at the outcome - A Security Incident Reporting Maturity Model.

The aim of such a maturity model is to judge if the particular CSF is in place and, if so, to what extent. It is not an iterative maturity model. In other words you do not have to score well in one before you can score another. They can be assessed individually with regards to the current situation. The main purpose of a maturity model is to identify a gap that can be closed after following improvement actions

I am not asking that you score your organization as part of this survey and send me the response, as this may be very sensitive. You are of course at liberty to do so for your own internal benefit. Also it is recognized that in any template or model local relevant language, terminology and contextual wording would be of benefit to make it more applicable to the relevant sector or organization. Therefore please bear this in mind when commenting.

This maturity model incorporates the top 4 elements of the Delphi survey together with the amended descriptions taken from your valuable comments. Many of you will recognize some of the amendments as being taken from your suggestions.

I would now ask that you view the enclosed maturity model to comment on if this was provided to your organisation, or those for which you may be assessing, whether it is:
1. Understandable
2. Usable
3. Considered to be of value to asses where your organisation sits regarding the deployment of the identified CSFs

The response form is simple to complete and again uses a Likert scale of 5 options. As before there is a facility for you to add any comments or observations you feel can assist in its final version.

I appreciate you may have both positive and negative views regarding maturity models. I would ask that for this exercise that you judge the maturity model as a potential benefit to any organization to assist in improving the number of incidents that are reported.

As in round two I will use an allocated reference number that will ensure I can marry up your responses in round one/two. This also will save you time repeating your details. In addition, I again provide reassurances re confidentiality. These are set out in the maturity model questionnaire. Your reference number is xxxx

I have enclosed two versions of the Maturity Model, as a pdf form and as a word form (whichever is easiest for you to complete). I have again sent them separately as some defences do not like certain types of pdf or word formats, hopefully you will receive one of them.

Please note; some respondents had difficulty where they completed a response but did not save it as a separate document and then forwarded the unsaved one to me. With some versions of mail and office document management, if you completed the form as it arrived without renaming and saving it, when it was sent back to me your response was blank. So please save your response and then send that saved version.

Some of you took the option of printing the form, completing it, scanning the response and then emailing to me the scanned version. Others printed and completed it and then posted it to me. All these options are still open to you.

I would be grateful if you could return your answers to my university email address m.humphrey@cranfield.ac.uk or, as before, if you prefer post to me at the address shown in the instructions.

Again may I thank you for participating and would be really grateful for this last request for your valuable professional input into my research.

Please can you complete and return the questionnaire by Sunday the 15th of January 2017.

I do hope you can find the time to add your valuable contribution to the research. Thank you for reading this.

Yours faithfully,

Mike Humphrey MSc F.Inst.ISP
Part Time PhD Student Defence Academy Shrivenham
m.humphrey@cranfield.ac.uk

Reference no. 1

APPENDIX 14

Validation of a Suggested Security Incident Reporting Maturity Model

Confidentiality, completion and return of the completed questionnaire

This survey will be conducted in strict confidence and your responses kept secure and not shared. I will be the only person analysing the responses. You can either complete as a word document, pdf form or, as sometimes there are compatibility issues, print it out, complete by hand, scan and return. If you do not want to email your response but post it instead the address for posting replies is**:** Mike Humphrey Standards and Security PO Box 8000 London SE11 5EN. My e mail address for the survey responses is m.humphrey@cranfield.ac.uk

You can withdraw from the survey at any time and after the completion of the survey I am happy to provide a de-brief on the results.

Please be assured all responses will be treated with strict confidentiality and the final analysis and any reporting will not identify individuals or companies.

Please look at each of the Critical Success Factors (CSFs) which make up the maturity model set out on pages 2-5. (These pages are greyed out to indicate they are not part of the questionnaire). There are four of them. The identification and wording of these Critical Success Factors have been compiled through consensus of a number of security professionals across the public, private sector, academia in the UK and across the world. There is a description of the CSF, a level which sets out the position within the maturity model and finally a description of what that level might represent in relation to that CSF. The level descriptions have been kept to simple descriptions rather than being proscriptive which may not be universally relevant to all sectors and organisations. Please bear this in mind and, of course, you are free to make suggestions regarding the level descriptions in your response.

The intention is that you look at the CSF then, using the description, decide what level you would allocate to your organisation or one for which you may be reviewing or providing guidance to.

Then please go to page 6 and complete the questions that relate to each CSF and, where you wish to make any comment, use the space provided. Each CSF question has a rating between 1 and 5. There are also further questions relating to the maturity model itself which are a mix of ratings of 1-5 or a more simple yes no option. The layout of the model is not being scored. It is your views on the description of the Critical Success Factor and level descriptions to support the maturity levels that I am interested in. You are of course welcome to make any comments on the layout.

To assist if I have any need to clarify any of your responses it would help if you include a contact email address below.

CRITICAL SUCCESS FACTORS MATURITY MODEL TABLES (Not part of the questionnaire)

Critical Success Factor	Maturity Level	Description (Feel free to amend by suggesting alternative wording)
1. A recognition by senior management that incidents will happen and that they must play a full and active part in the incident management process by. • Fully accepting that incident reporting is to be seen positively enabling early mitigation action. • Recognising in some cases there will be a need to consider action taken where the incident should and could have been prevented. • Acknowledging security incidents are part of life and business and, like Health and Safety accidents, the reporting process is part of the prevention strategy. • Supporting a culture which encourages reporting • Recognising an organisation which handles an incident well enhances its reputation	1. Initial	No recognition by senior management that incidents will occur or of their role in the process
	2. Established	Aware of the fact they will happen and they are to actively participate but only evidence of partial involvement
	3. Business enabling	Recognised by management as important but not consistent across the organisation
	4. Quantitatively managed	The majority of management accept incidents will happen and there is good evidence of regular involvement by managers but not firmly embedded.
	5. Optimised	Considered as part of day to day management responsibilities with strong evidence of consistent active participation across the organisation with proactive rather than reactive involvement of managers
Organisation Score: Level 1 2 3 4 5		
Reason for score		

Critical Success Factor	**Maturity Level**	**Description** **(Feel free to amend by suggesting alternative wording)**
2. Ease of making a report, recognising if reporting incidents is difficult individuals will be less likely to submit them. This may particularly affect the reporting of near misses. The reporting process should: • Provide a sufficiently clear level of education and awareness to all staff in how the reporting process works. • Describe what an incident/near miss is. • Describe how to report it and what escalation needs to take place.	1. Initial	No recognised reporting mechanism in place
	2. Established	A reporting process in place but not well known or used.
	3. Business Enabling	A reporting mechanism is in place and used by most but still has challenges in its use
	4. Quantitatively managed	Well understood processes with majority completing the process as described
	5. Optimised	Second nature to staff on how to report.
Organisation Score: Level 1 2 3 4 5		
Reason for Score		

Critical Success Factor	**Maturity Level**	**Description** **(Feel free to amend by suggesting alternative wording)**
3. Rapid, useful, accessible and intelligible feedback to the reporting community[1] recognising: • People will only continue to report incidents if they are acknowledged and, even better, can see that reporting has been useful or has ensured compliance • Feedback need not be detailed, often a simple acknowledgement of the report and that action is being taken may be sufficient. • Staff that have been responsible for or involved in a security incident can become anxious. It is helpful to keep them informed and provide support where necessary	1. Initial	No feedback provided to anyone who reports an incident. No support offered
	2. Established	Limited feedback to reporters and some support
	3. Business enabling	Feedback provided but not consistently. Some support provided but ad hoc
	4. Quantitatively managed	Feedback in most circumstances. Recognition that support needed for reporters
	5. Optimised	Feedback is consistently given; reporters are kept in the feedback loop. Support mechanisms embedded
Organisation Score: Level 1 2 3 4 5		
Reason for score		

[1] Community being the one that your organisation may belong to law enforcement, finance, healthcare etc.

Critical Success Factor	**Maturity Level**	**Description** **(Feel free to amend by suggesting alternative wording)**
4. Incident analysis that considers root causes and wider systems/processes, not just the initial impact assessment. It must recognise that: • It is important to identify what actually contributed to an incident in order to ensure repeat incidents do not occur. • Analysis may identify/highlight any training/development needs or gaps • The incident may be just a symptom of a larger organisational or process flaw. • Superficial investigations may be counterproductive in the long term	1. Initial	No analysis taking place
	2. Established	A process in place but there is limited analysis of incidents
	3. Business Enabling	Analysis is taking place but not fully investigated to understand root cause and tackle the identified issues
	4. Quantitatively managed	Analysis and learning taking place and lessons learnt in the majority of cases and changes to policy/procedures/process put in place to prevent reoccurrence
	5. Optimised	Full root cause analysis in place for incidents. Learning outcomes adopted to ensure business improvement and future prevention of that type of incident's recurrence
Organisation Score: Level 1 2 3 4 5		
Reason for score		

QUESTIONNAIRE STARTS HERE (Pages 6-12)

Critical Success Factor 1
A recognition by senior management that incidents will happen and that they must play a full and active part in the incident management process

Question	Please rank your answer by selecting as appropriate one of the below boxes as applicable to the key below;	Please use the space below if you wish to comment regarding your answer
1.1 Based on the Critical Success Factor and the level description how easy was it for you to interpret the maturity position of your/another organisation?	1. Very easy to understand ☐ 2. Easy to understand ☐ 3. Neither easy nor difficult ☐ 4. Difficult to understand ☐ 5. Very difficult to understand ☐	
1.2 Based on the Critical Success Factor and the level description how easy would it be to use to judge your or another organisations position in the maturity model?	1. Very easy to judge ☐ 2. Easy to judge ☐ 3. Neither easy nor difficult to judge ☐ 4. Difficult to judge ☐ 5. Very difficult to judge ☐	

<table>
<tr><td colspan="3"><b>Critical Success Factor 2
Ease of making a report, recognising if reporting incidents is difficult individuals will be less likely to submit them.</b></td></tr>
<tr><td>Question</td><td>Please rank your answer by selecting as appropriate one of the below boxes as applicable to the key below;</td><td>Please use the space below if you wish to comment regarding your answer</td></tr>
<tr><td>2.1 Based on the Critical Success Factor and the level description how easy was it for you to interpret the maturity position of your/another organisation?</td><td>1. Very easy to understand ☐
2. Easy to understand ☐
3. Neither easy nor difficult ☐
4. Difficult to understand ☐
5. Very difficult to understand ☐</td><td></td></tr>
<tr><td>2.2. Based on the Critical Success Factor and the level description how easy would it be to use to judge your or another organisations position in the maturity model?</td><td>1. Very easy to judge ☐
2. Easy to judge ☐
3. Neither easy nor difficult to judge ☐
4. Difficult to judge ☐
5. Very difficult to judge ☐</td><td></td></tr>
</table>

Critical Success Factor 3
Rapid, useful, accessible and intelligible feedback to the reporting community

Question	Please rank your answer by selecting as appropriate one of the below boxes as applicable to the key below;	Please use the space below if you wish to comment regarding your answer
3.1. Based on the Critical Success Factor and the level description how easy was it for you to interpret the maturity position of your/another organisation?	1. Very easy to understand ☐ 2. Easy to understand ☐ 3. Neither easy nor difficult ☐ 4. Difficult to understand ☐ 5. Very difficult to understand ☐	
3.2. Based on the Critical Success Factor and the level description how easy would it be to use to judge your or another organisations position in the maturity model?	1. Very easy to judge ☐ 2. Easy to judge ☐ 3. Neither easy nor difficult to judge ☐ 4. Difficult to judge ☐ 5. Very difficult to judge ☐	

Critical Success Factor 4

Incident analysis that considers root causes and wider systems/processes, not just the initial impact assessment.

Question	Please rank your answer by selecting as appropriate one of the below boxes as applicable to the key below;	Please use the space below if you wish to comment regarding your answer
Q 4.1 Based on the Critical Success Factor and the level description how easy was it for you to interpret the maturity position of your/another organisation?	1. Very easy to understand □ 2. Easy to understand □ 3. Neither easy nor difficult □ 4. Difficult to understand □ 5. Very difficult to understand □	
Q 4.2 Based on the Critical Success Factor and the level description how easy would it be to use to judge your or another organisations position in the maturity model?	1. Very easy to judge □ 2. Easy to judge □ 3. Neither easy nor difficult to judge □ 4. Difficult to judge □ 5. Very difficult to judge □	

General Questions on maturity models

It is recognised that not all organisations use maturity models and there are varying views on them. For the purpose of this survey can you please judge the potential use of this maturity model to identify if and how well each of the four identified Critical Success Factors is adopted within an organisation.

Question	Please rank your answer by selecting as appropriate one of the below boxes as applicable to the key below;	Please use the space below if you wish to comment regarding your answer
Do you use maturity models in your organisation or one for which you have reviewed or assessed	Yes □ No □	
Do you personally feel maturity models are useful tools to assist an organisation understand where they sit regarding to a particular situation.	Yes □ No □ No strong view either way □	
Some maturity models set out a larger number of elements to measure against. Is just listing the critical elements a better approach.	Yes □ No □ No strong view either way □	

Specific questions on the Critical Success Factor Maturity Model

The four Critical Success Factors and their wording have been developed through the consensus of a number of security professionals. They have now been set out in a maturity model together with a brief description of the level of maturity appropriate to that CSF. The following questions ask your opinion on the model; it is understandable, useable and whether or not you feel it could be of value.

Question	Please rank your answer by selecting as appropriate one of the below boxes as applicable to the key below;	Please use the space below if you wish to comment regarding your answer
Overall would you consider this maturity model to be of value to your organisation to assess how security incident reporting is handled and managed against the identified Critical Success Factors	Extremely valuable □ Valuable □ Neither Valuable or of no value □ Not very valuable □ Of no value at all □	
If other organisations used the same model would this assist when determining the ability of that organisation to handle incidents? (for example if exchanging data with them or contracting them as a third party supplier)	Extremely valuable □ Valuable □ Neither Valuable or of no value □ Not very valuable □ Of no value at all □	
Once refined would you consider using this maturity model in your organisation or one you would be assessing	Yes □ Possibly □ No □	

Specific questions on the Critical Success Factor Maturity Model (continued) The four Critical Success Factors and their wording have been developed through consensus of a number of security professionals. They have now been set out in a maturity model together with a brief description of the level of maturity appropriate to that CSF. The following questions ask you opinion on the model. Whether it is understandable, useable and whether or not you feel it could be of value.		
Question	Please rank your answer by selecting as appropriate one of the below boxes as applicable to the key below;	Please use the space below if you wish to comment regarding your answer
Would just knowing what the Critical Success Factors are and using an internal method of ensuring a gradual move to ensure they were embedded be a better approach for your organisation	Yes ☐ Possibly ☐ No ☐	
Thank you for your time if you have any other comments on the Critical success Factors, level descriptions or other matter relating to this questionnaire please feel free to add them below.		

Thank you for your time. Please e mail your completed form to; m.humphrey@cranfield.ac.uk Alternatively if you wish to post it please send to Mike Humphrey Standards and Security PO Box 8000 London SE11 5EN

c:\users\mike\documents\phd\thesis commenced feb 2013\chapter 3 methodology\validation of irmm\incident reporting maturity model table questionnaire delphi group version 3 24_12_16.docx

Control Group version

APPENDIX 15

Validation of a Suggested Security Incident Reporting Maturity Model

Confidentiality, completion and return of the completed questionnaire

This survey will be conducted in strict confidence and your responses kept secure and not shared. I will be the only person analysing the responses. You can either complete as a word document, pdf form or, as sometimes there are compatibility issues, print it out, complete by hand, scan and return. If you do not want to email your response but post it instead the address for posting replies is**:** Mike Humphrey Standards and Security PO Box 8000 London SE11 5EN. My e mail address for the survey responses is m.humphrey@cranfield.ac.uk

You can withdraw from the survey at any time and after the completion of the survey I am happy to provide a de-brief on the results.

Please be assured all responses will be treated with strict confidentiality and the final analysis and any reporting will not identify individuals or companies.

Please look at each of the Critical Success Factors (CSFs) which make up the maturity model set out on pages 2-5. (These pages are greyed out to indicate they are not part of the questionnaire). There are four of them. The identification and wording of these Critical Success Factors have been compiled through consensus of a number of security professionals across the public, private sector, academia in the UK and across the world. There is a description of the CSF, a level which sets out the position within the maturity model and finally a description of what that level might represent in relation to that CSF. The level descriptions have been kept to simple descriptions rather than being proscriptive which may not be universally relevant to all sectors and organisations. Please bear this in mind and, of course, you are free to make suggestions regarding the level descriptions in your response.

The intention is that you look at the CSF then; using the description, decide what level you would allocate to your organisation or one for which you may be reviewing or providing guidance to.

Then please go to page 6 and complete the questions that relate to each CSF and, where you wish to make any comment, use the space provided. Each CSF question has a rating between 1 and 5. There are also further questions relating to the maturity model itself which are a mix of ratings of 1-5 or a more simple yes no option. The layout of the model is not being scored. It is your views on the description of the Critical Success Factor and level descriptions to support the maturity levels that I am interested in. You are of course welcome to make any comments on the layout.

To assist if I have any need to clarify any of your responses it would help if you include a contact email address below.

CRITICAL SUCCESS FACTORS MATURITY MODEL TABLES (Not part of the questionnaire)

Critical Success Factor	**Maturity Level**	**Description** **(Feel free to amend by suggesting alternative wording)**
1. A recognition by senior management that incidents will happen and that they must play a full and active part in the incident management process by. • Fully accepting that incident reporting is to be seen positively enabling early mitigation action. • Recognising in some cases there will be a need to consider action taken where the incident should and could have been prevented. • Acknowledging security incidents are part of life and business and, like Health and Safety accidents, the reporting process is part of the prevention strategy. • Supporting a culture which encourages reporting • Recognising an organisation which handles an incident well enhances its reputation	1. Initial	No recognition by senior management that incidents will occur or of their role in the process
	2. Established	Aware of the fact they will happen and they are to actively participate but only evidence of partial involvement
	3. Business enabling	Recognised by management as important but not consistent across the organisation
	4. Quantitatively managed	The majority of management accept incidents will happen and there is good evidence of regular involvement by managers but not firmly embedded.
	5. Optimised	Considered as part of day to day management responsibilities with strong evidence of consistent active participation across the organisation with proactive rather than reactive involvement of managers
Organisation Score: Level 1 2 3 4 5		
Reason for score		

Critical Success Factor	**Maturity Level**	**Description** **(Feel free to amend by suggesting alternative wording)**
2. Ease of making a report, recognising if reporting incidents is difficult individuals will be less likely to submit them. This may particularly affect the reporting of near misses. The reporting process should: • Provide a sufficiently clear level of education and awareness to all staff in how the reporting process works. • Describe what an incident/near miss is. • Describe how to report it and what escalation needs to take place.	1. Initial	No recognised reporting mechanism in place
	2. Established	A reporting process in place but not well known or used.
	3. Business Enabling	A reporting mechanism is in place and used by most but still has challenges in its use
	4. Quantitatively managed	Well understood processes with majority completing the process as described
	5. Optimised	Second nature to staff on how to report.
Organisation Score: Level 1 2 3 4 5		
Reason for Score		

Critical Success Factor	**Maturity Level**	**Description** **(Feel free to amend by suggesting alternative wording)**
3. Rapid, useful, accessible and intelligible feedback to the reporting community[1] recognising: • People will only continue to report incidents if they are acknowledged and, even better, can see that reporting has been useful or has ensured compliance • Feedback need not be detailed, often a simple acknowledgement of the report and that action is being taken may be sufficient. • Staff that have been responsible for or involved in a security incident can become anxious. It is helpful to keep them informed and provide support where necessary	1. Initial	No feedback provided to anyone who reports an incident. No support offered
	2. Established	Limited feedback to reporters and some support
	3. Business enabling	Feedback provided but not consistently. Some support provided but ad hoc
	4. Quantitatively managed	Feedback in most circumstances. Recognition that support needed for reporters
	5. Optimised	Feedback is consistently given; reporters are kept in the feedback loop. Support mechanisms embedded
Organisation Score: Level 1 2 3 4 5		
Reason for score		

[1] Community being the one that your organisation may belong to law enforcement, finance, healthcare etc.

Critical Success Factor	**Maturity Level**	**Description** **(Feel free to amend by suggesting alternative wording)**
4. Incident analysis that considers root causes and wider systems/processes, not just the initial impact assessment. It must recognise that: • It is important to identify what actually contributed to an incident in order to ensure repeat incidents do not occur. • Analysis may identify/highlight any training/development needs or gaps • The incident may be just a symptom of a larger organisational or process flaw. • Superficial investigations may be counterproductive in the long term	1. Initial	No analysis taking place
	2. Established	A process in place but there is limited analysis of incidents
	3. Business Enabling	Analysis is taking place but not fully investigated to understand root cause and tackle the identified issues
	4. Quantitatively managed	Analysis and learning taking place and lessons learnt in the majority of cases and changes to policy/procedures/process put in place to prevent reoccurrence
	5. Optimised	Full root cause analysis in place for incidents. Learning outcomes adopted to ensure business improvement and future prevention of that type of incident's recurrence
Organisation Score: Level 1 2 3 4 5		
Reason for score		

QUESTIONNAIRE STARTS HERE (Pages 6-12)

Critical Success Factor 1
A recognition by senior management that incidents will happen and that they must play a full and active part in the incident management process

Question	Please rank your answer by selecting as appropriate one of the below boxes as applicable to the key below;	Please use the space below if you wish to comment regarding your answer
1.1 Based on the Critical Success Factor and the level description how easy was it for you to interpret the maturity position of your/another organisation?	1. Very easy to understand □ 2. Easy to understand □ 3. Neither easy nor difficult □ 4. Difficult to understand □ 5. Very difficult to understand □	
1.2 Based on the Critical Success Factor and the level description how easy would it be to use to judge your or another organisations position in the maturity model?	1. Very easy to judge □ 2. Easy to judge □ 3. Neither easy nor difficult to judge □ 4. Difficult to judge □ 5. Very difficult to judge □	

Critical Success Factor 2 **Ease of making a report, recognising if reporting incidents is difficult individuals will be less likely to submit them.**		
Question	Please rank your answer by selecting as appropriate one of the below boxes as applicable to the key below;	Please use the space below if you wish to comment regarding your answer
2.1 Based on the Critical Success Factor and the level description how easy was it for you to interpret the maturity position of your/another organisation?	1. Very easy to understand ☐ 2. Easy to understand ☐ 3. Neither easy nor difficult ☐ 4. Difficult to understand ☐ 5. Very difficult to understand ☐	
2.2. Based on the Critical Success Factor and the level description how easy would it be to use to judge your or another organisations position in the maturity model?	1. Very easy to judge ☐ 2. Easy to judge ☐ 3. Neither easy nor difficult to judge ☐ 4. Difficult to judge ☐ 5. Very difficult to judge ☐	

Critical Success Factor 3 **Rapid, useful, accessible and intelligible feedback to the reporting community**		
Question	Please rank your answer by selecting as appropriate one of the below boxes as applicable to the key below;	Please use the space below if you wish to comment regarding your answer
3.1. Based on the Critical Success Factor and the level description how easy was it for you to interpret the maturity position of your/another organisation?	1. Very easy to understand ☐ 2. Easy to understand ☐ 3. Neither easy nor difficult ☐ 4. Difficult to understand ☐ 5. Very difficult to understand ☐	
3.2. Based on the Critical Success Factor and the level description how easy would it be to use to judge your or another organisations position in the maturity model?	1. Very easy to judge ☐ 2. Easy to judge ☐ 3. Neither easy nor difficult to judge ☐ 4. Difficult to judge ☐ 5. Very difficult to judge ☐	

Critical Success Factor 4 **Incident analysis that considers root causes and wider systems/processes, not just the initial impact assessment.**		
Question	Please rank your answer by selecting as appropriate one of the below boxes as applicable to the key below;	Please use the space below if you wish to comment regarding your answer
Q 4.1 Based on the Critical Success Factor and the level description how easy was it for you to interpret the maturity position of your/another organisation?	1. Very easy to understand □ 2. Easy to understand □ 3. Neither easy nor difficult □ 4. Difficult to understand □ 5. Very difficult to understand □	
Q 4.2 Based on the Critical Success Factor and the level description how easy would it be to use to judge your or another organisations position in the maturity model?	1. Very easy to judge □ 2. Easy to judge □ 3. Neither easy nor difficult to judge □ 4. Difficult to judge □ 5. Very difficult to judge □	

General Questions on maturity models

It is recognised that not all organisations use maturity models and there are varying views on them. For the purpose of this survey can you please judge the potential use of this maturity model to identify if and how well each of the four identified Critical Success Factors is adopted within an organisation.

Question	Please rank your answer by selecting as appropriate one of the below boxes as applicable to the key below;	Please use the space below if you wish to comment regarding your answer
Do you use maturity models in your organisation or one for which you have reviewed or assessed	Yes ☐ No ☐	
Do you personally feel maturity models are useful tools to assist an organisation understand where they sit regarding to a particular situation.	Yes ☐ No ☐ No strong view either way ☐	
Some maturity models set out a larger number of elements to measure against. Is just listing the critical elements a better approach.	Yes ☐ No ☐ No strong view either way ☐	

Specific questions on the Critical Success Factor Maturity Model

The four Critical Success Factors and their wording have been developed through the consensus of a number of security professionals. They have now been set out in a maturity model together with a brief description of the level of maturity appropriate to that CSF. The following questions ask your opinion on the model; it is understandable, useable and whether or not you feel it could be of value.

Question	Please rank your answer by selecting as appropriate one of the below boxes as applicable to the key below;	Please use the space below if you wish to comment regarding your answer
Overall would you consider this maturity model to be of value to your organisation to assess how security incident reporting is handled and managed against the identified Critical Success Factors	Extremely valuable ☐ Valuable ☐ Neither Valuable or of no value ☐ Not very valuable ☐ Of no value at all ☐	
If other organisations used the same model would this assist when determining the ability of that organisation to handle incidents? (for example if exchanging data with them or contracting them as a third party supplier)	Extremely valuable ☐ Valuable ☐ Neither Valuable or of no value ☐ Not very valuable ☐ Of no value at all ☐	
Once refined would you consider using this maturity model in your organisation or one you would be assessing	Yes ☐ Possibly ☐ No ☐	

<table>
<tr><td></td><td></td><td></td></tr>
<tr><td colspan="3"><b><u>Specific questions on the Critical Success Factor Maturity Model (continued)</u></b>
The four Critical Success Factors and their wording have been developed through consensus of a number of security professionals. They have now been set out in a maturity model together with a brief description of the level of maturity appropriate to that CSF. The following questions ask you opinion on the model. Whether it is understandable, useable and whether or not you feel it could be of value.</td></tr>
<tr><td>Question</td><td>Please rank your answer by selecting as appropriate one of the below boxes as applicable to the key below;</td><td>Please use the space below if you wish to comment regarding your answer</td></tr>
<tr><td>Would just knowing what the Critical Success Factors are and using an internal method of ensuring a gradual move to ensure they were embedded be a better approach for your organisation</td><td>Yes ☐
Possibly ☐
No ☐</td><td></td></tr>
<tr><td colspan="3">Thank you for your time if you have any other comments on the Critical success Factors, level descriptions or other matter relating to this questionnaire please feel free to add them below.</td></tr>
<tr><td colspan="3"></td></tr>
</table>

Thank you for your time. Please e mail your completed form to; m.humphrey@cranfield.ac.uk   Alternatively if you wish to post it please send to Mike Humphrey Standards and Security PO Box 8000 London SE11 5EN

APPENDIX 16

IRMM Survey Responses Comments

CSF 1 Comments and reference number of respondent
1.1 Based on the Critical Success Factor and the level description how easy was it for you to interpret the maturity position of your/another organisation?
(**12)** I would suggest changing the wording from ‘ Health and Safety accidents’ to ‘ Health and Safety incidents’ in order to match the terms used elsewhere and not, potentially, raise a belief that security incidents may all be ‘accidents’. (1) **(21)** suggest including more information or examples about the role of managers, such as regular conversations with staff about security incidents, briefing the team as well as the individual to reduce the risk of it ha[ppening again, or evidence that managers promote honest and full reporting. (2) **(29)** Purely down to the size of the organisation, evidencing level 5 could prove hard (1) **(37)** I liked the fact that there are general CSF descriptions to further explain the CSF itself, as well as a brief description against each level. The descriptions are clear, allowing me to make a judgement regardless of sector the organisation is in. (1) **(42)** It was very easy to understand the distinctions between the 5 Maturity Levels. (1) **(45)** I recommend using, “Recognising there will be a need to consider action(a) taken where the incident should and could have been prevented.” Instead of, “Recognising in some cases there will be a need to consider action taken where the incident should and could have been prevented.” If an incident is reported, this consideration is a critical part of the RCA (2) **(49)** The organisation has a well-defined and established incident management policy with supporting procedures (2) **(50)** The Organisation has a well-defined reporting system, there is also a very good educational process in place to prevent security incidents. However senior management do accept that incidents will occur and when major or critical incidents occur then Gold groups are established to ensure appropriate action is taken. (2) **(61)** I feel emphasis on the “no blame” part of the process has been somewhat lost and is harder to draw out. The explanatory bullet points are long. (2) **(63)** You might want to include "that" after "Recognising" in the fifth CSF descriptive bullet. (1) **(70)** Level 4 might be better as “… not firmly or consistently embedded”. (2) **(72)** All at least 2, except for the second bullet, which I can’t make sense of, so 5. “…incident could and should have been prevented” implies that action was *not* taken, but “consider action taken” suggests that it was? (3) **(87)** Lack of experience of the incident reporting process implies lack of evidence of the extent of management involvement. (3) **(89)** “positively enabling…mitigation” may be capable of causing confusion: I would suggest more direct language. Similarly

“Recognising…prevented”. (3)

(92) The wording is clear, but I found it difficult to score. Probably because I was thinking along the lines of CSF 4 when I was trying to assess the maturity. (3)

(93) Subject to some wordsmithing! (2)

(103) A simple statement that will be interpreted correctly. (1)

(107) Suggestion to change the description of initial maturity is to :

No recognition by senior management that incidents will occur or incident handling will be of their role in the process (2)

(115) Questions are simple and unambiguous with defined maturity statements.(1)

(CG7) Clear and explicit but provided you now your subject matter. Not sure that this would be of use by Internal Audit as they would not have the breadth of knowledge required. (2)

(CG11) Easy for my own organisation because I am involved in the process however if auditing another organisation I would need evidence to support the scoring. (2)

(CG12) The description suggests a smaller organisation. I would not expect all senior management to have an involvement only relevant individuals. (2)

(CG13) There needs to be some sort of recognition that there may be a turnover could be an inhibitor so I’d like to see some reference to induction/training. The ICO would also be interested in this aspect in the event that an incident required notification to that regulator. Size/scale of the organisation is also a factor that needs to be considered here. (2)

1.2 Based on the Critical Success Factor and the level description how easy would it be to use to judge your or another organisations position in the maturity model?

(7) Not sure there is a clear distinction between 3 & 4 as both talk about either a lack of consistency or not being firmly embedded. (2)

(8) The difficulty I think will be on what to base a judgement on – you could ask an organisation and get one answer but whether they had documented processes or auditable evidence might be another question.

Any assessment of awareness can be coloured by the presence of the question. So if you ask a CEO “Are you aware of the risk of security incidents?” then they immediately have a level of awareness simply from being asked the question.

However I don’t think its necessary to create an audit checklist – BUT it may be useful to think about, list or include the kinds of evidence you would expect against each answer. (2)

(17) Need to be either involved in the incident reporting process or interview appropriate management personnel.(2)

(29) Very easy to judge our own, perhaps slightly less easy to judge the level of in another organisation without sufficient evidence (2)

(37) Same comment as given for CSF1 (I liked the fact that there are general CSF descriptions to further explain the CSF itself, as well as a brief description against each level. The descriptions are clear, allowing me to make a judgement regardless of sector the organisation is in. (1))

(38) To judge any organisation including you own a high degree of familiarity must exist or the output will be inaccurate. (2)

(40) Easy to judge as a security practitioner, less easy for a senior manager to accept, especially at the lower end. (2)

(42) Maturity Levels 1 and 5 will be easy to judge. The intermediate levels will take more work, to establish how much IM activity takes place and how it is distributed across the organisation. (3)

(52) Difference between the two questions 1.1 and 1.2 (and for the other CSFs) is rather subjective **-** had to read it twice and then I can't really differentiate my answers.(1)

(55) I think there will always be some room for “interpretation” – aka an ability to err towards what might be seen as an acceptable score. This is of course inevitable; can be tempered by having an element if independence/moderation is assessing scores/position. Example: when we scored ourselves against IAMM our result ranged from a healthy(?) 2 to a more realistic 0.7! (2)

(63) It would depend on the consistency with which the assessment is made but the requirement is explicit. (2)

(70) Basically easy, but it will depend on the complexity of the organisation, and there could well be a difference of perception between senior managers themselves and other in the organisation of their level of recognition – but of course that is the point of having a model like this, but it does highlight the importance of getting the right person to assess.(2)

(72) All at least 2, except for the second bullet, which I can’t make sense of, so 5. “…incident could and should have been prevented” implies that action was *not* taken, but “consider action taken” suggests that it was? (3)

(73) In theory should be easy but MoD are not good at being clear about what needs to be reported. (2)

(74) Senior Management do not have a uniform set of values or characteristics. Those closer to the organisation’s security team tend to get it. (4)

(86) Having an understanding of the approach taken by the organisation reviewed, in conjunction with a clear maturity scale and associated level definition, I feel it would be easy to judge. (2)

(87) As per previous box (3) *Lack of experience of the incident reporting process implies lack of evidence of the extent of management involvement.*

(89) In my experience the main difficulty is in expressing the maturity of a large and complex organisation – that has thousands of members, dozens of sites, tens of specialisms, ten ranks, sworn and unsworn staff, volunteers and almost as many cultures. It is not easy to take an overall view, or should one consider worst case, or best outcomes ? (2)

(92) As 1.1, easy to understand but levels are not so clear cut. I wonder if this question should actually be asked last? It can then be reviewed in context. (4)

(96) The reporting/ recording process may have to factor in to what extent senior management (as opposed to line management) have been involved in the management process. Whilst the critical success factor might be at the optimal level it might be difficult to judge this in an audit-able way unless senior management were copied in to incidents or summaries on a regular basis. (3)

(103) All of the examples are subjective...which is difficult to evidence. It would perhaps be useful if there were ways of evidencing the score...i.e. Senior managers take a proactive role in the incident management process by have a standing agenda item on their weekly executive meetings' or something similar? (4)

(115) This would be dependent upon the security culture and attitude of the organisation being assessed. (3)

(CG7) Ditto (2) *Clear and explicit but provided you now your subject matter. Not sure that this would be of use by Internal Audit as they would not have the breadth of knowledge required.*

(CG9) Would require the responder to have genuine knowledge and probably wide experience of the organisation to answer accurately (3)

(CG11) It would be difficult to determine another organisations maturity based on the questions alone. It would need a full evidence based assessment to be carried out to determine the senior management involvement in incident management. (2)

CG12) As above – that said I would take it as the senior management I thought would need to have an involvement and judge accordingly. (2) *The description suggests a smaller organisation. I would not expect all senior management to have an involvement only relevant individuals*.

(CG13) same comments fro previous answer 1.1 There needs to be some sort of recognition that there may be a turnover could be an inhibitor so I'd like to see some reference to induction/training. The ICO would also be interested in this aspect in the event that an incident required notification to that regulator.Size/scale of the organisation is also a factor that needs to be considered here. (3)

CSF 2 Comments and ref number of respondent

2.1 Based on the Critical Success Factor and the level description how easy was it for you to interpret the maturity position of your/another organisation?

(8) As an observation, as I work in the security industry I can easily make sense of this – the survey probably needs input from non security practitioners (1)

(12) I would suggest the sentence 'Describe what an incident/near miss is' has the phrase 'in non-technical terms' in order to clarify the need for ease of use and common understanding. (1)

(21) Just a suggestion to include in the bullet point list that the incident reporting process and the form required should be easy to find (2)

(29) As with Factor 1, evidencing of level 5 could be difficult in our large organisation (1)

(37) Same comment as given for CSF1 (I liked the fact that there are general CSF descriptions to further explain the CSF itself, as well as a brief description against each level. The descriptions are clear, allowing me to make a judgement regardless of sector the organisation is in. (1))

(42) It was very easy to understand the distinctions between the 5 Maturity Levels. (1)

(49) Templates and reporting guidelines are well publicised. (2)

(50) There is a well-defined security incident/breach process in place backed up with policy and procedures. (2)

(55) Yes: I've used this table to match against an internal scoring mechanism we used last year to compare ourselves at different points along our road to implementing an internal/BT-partnered SOC. (1)

(63) Is "second nature" universally understood? Might this
be expressed as: "Reporting is fully embedded in the
culture and processes of the organisation and its people (1)

(70) But I felt there were a couple of missing points:

- consistency of reporting of different types of incident.
- need for 'no blame' culture in incident/near miss reporting to encourage openness. (2)

(72) A proof-reading comment that you switch from talking about "reporting processes" and "reporting mechanisms". If that was supposed to have some significance then I missed it, if not it's a distraction by making me think it might have some significance! (1)

(86) The levels of maturity may be take into account the reporting mechanism itself, i.e. manual form filling may deter individuals from reporting given the effort required (relatively speaking). More automation e.g. Intranet based web reporting forms may aid uptake and are likely to indicate greater levels of maturity. (2)

(87) Reporting criteria, forms and details of where to send them to are readily available on the intranet. There are also phone points of contact. (1)

(89) Again, I would suggest the use of very direct language. Particularly my attempt would be "Ensure that staff are aware of the reporting process and how it works". (3)

(107)
Suggestion to change the description of optimized maturity is to :
Well understood processes reporting recognized incidents as described
Reason) to understand clearly. (2)

(115) See 1.1response *Questions are simple and unambiguous with defined maturity statements*(1)

(CG5) The ability of the individual to report incidents in a simple and straightforward manner is critical to the success of the reporting mechanism and this CSF is probably the key tenet of the maturity model, sadly one that has been overlooked in this organisation. (1)

(CG7) Ditto (2) *Clear and explicit but provided you now your subject matter. Not sure that this would be of use by Internal Audit as they would not have the breadth of knowledge required.*

(CG11) Easy for my own organisation because I am involved in the process however if auditing another organisation I would need evidence to support the scoring. (2)

(CG12) I found I needed to read the CSF (bit in bold) a couple of times before I understood it fully (3)

(CG13) I found it very easy to understand. The descriptions would benefit from recognising that hopefully users would at best only be occasional users so the focus ought to be on awareness of what to do in the event of recognising that a security incident has occurred and what they need to do next ie report the incident on the intuitive reporting tool. (1)

2.2. Based on the Critical Success Factor and the level description how easy would it be to use to judge your or another organisations position in the maturity model?

(8) The issue above would be less of a problem as a reporting process and evidence of its use is more likely to be tangible and present or not. The only issue might be that if there hadn't been many incidents (or "detected incidents") the volume of data might be low. (1)

(17) Need to be able to review appropriate material and processes.(2)

(29) Very easy to judge our own, perhaps slightly less easy to judge the level of in another organisation without sufficient evidence (2)

(37) Same comment as given for CSF1 (I liked the fact that there are general CSF descriptions to further explain the CSF itself, as well as a brief description against each level. The descriptions are clear, allowing me to make a judgement regardless of sector the organisation is in. (1))

(38) An intimate understanding if the organisation is essential to use these scales and I can confidently use it for my own organisation but would be concerned using it to judge another organisation that I did not know as well. (2)

(40) As with all incidents reporting schemes it is difficult to judge the take up as you 'don't know what you are not told'. This would be easier in smaller organisations based in a couple of buildings, potentially in the same country. Difficulties when numbers increase into the 1000's, buildings into the 100's and potentially global organisations. Not sure if there is any other research concerning differences socially across a global organisation with some cultures being more open and some more secretive? (4)

(42) This will be easy to judge, as it will be possible to examine the entries into the reporting process/mechanism, to assess how widespread its use is. If an area of the organisation is under represented, it will be easy to investigate that area.
Incidentally, I’ve assumed that there’s no difference between an IM Process and an IM Mechanism. If the use of different words is important and intended to enable distinctions between Maturity Levels to be made, more explanation will be required.(2)
(45) This could be more quantifiable than subjective if you describe year on year reporting statistic using some defined KPI’s. (2)
(49) Sometimes the need to just raise a report overshadows the quality and content of the actual report. This can hamper any investigation and also skew any analysis being conducted. (4)
(50) As above. *There is a well-defined security incident/breach process in place backed up with policy and procedures*. (2)
(54) Can be a selective judgement, as to ‘what good’ looks like, or the nature and extent of documentation (4)
(72) At any level above 1 there should be evidence/records to support the judgement (1)
(74) It must be difficult just now because we now have a behaviours team to understand culture around policy breach and reporting. (4)
(103) How can this be judged? I would like to think my organisation is quantatively managed, but the reality may be different. Again it would perhaps be good to have some metrics to quantify the scoring (but acknowledge this is very difficult to achieve!).(Not scored)
(115) This is easier to judge as the questions in the CSF can be asked of several staff at different levels in an audit. (2)
(CG7) Ditto (2) *Clear and explicit but provided you now your subject matter. Not sure that this would be of use by Internal Audit as they would*)*not have the breadth of knowledge required.*
(CG8) For our organisation, we would need to canvas the opinions of all staff before we could judge our own MM position. I do believe that unfortunately there will also be a number of staff who would prefer to try and “brush the incident under the carpet” then of course we may never get to hear about the incident (4)
(CG9) Measuring the ease of reporting would still need to be followed by people actually using it. (2)
(CG11) Easy for my own organisation because I am involved in the process however if auditing another organisation I would need evidence to support the scoring (2)

CSF 3   Comments and ref number of respondent (score in brackets)
3.1. Based on the Critical Success Factor and the level description how easy was it for you to interpret the maturity position of your/another organisation?
(1) Subjectivity with this section may be an issue as 'useful' is difficult to perceive to another organisation.(3)

(15) It was not entirely clear what the word “accessible” means in this context in the question. (2)
(17) Need to be either involved in the incident reporting process or chain or allowed to review the reporting process and reported incidents (and associated information) and interview appropriate personnel. (2)
(24) Normally the person reporting an incident is owns the incident and so is in the loop of its status. So in some cases this CSF may not be applicable.(2)
(25) As per suggested amendments above **-** unclear as to whether aimed at individual person reporting incident or holistic awareness to units/teams etc or both (4)
(26) The headline question uses the term “community” yet the explanation and the answers are all about the reporter? Feedback to the community is a different process from feedback to the reporter. The reporter should always be given feedback, but there are many good reasons that feedback to the community is not necessary or appropriate, so should remain a choice, not a requirement. (4)
(29) Given those involved in providing incident support would likely be the ones who provide the feedback to the reporting community, this would be easier to evidence than the other factors. (1)
(37) Same comment as given for CSF1 (I liked the fact that there are general CSF descriptions to further explain the CSF itself, as well as a brief description against each level. The descriptions are clear, allowing me to make a judgement regardless of sector the organisation is in. (1))
(42) It was very easy to understand the distinctions between the 5 Maturity Levels. (1)
(45) Solid definitions of what is meant by “Rapid, useful, accessible and intelligible” Regardless of definition, I would replace “rapid” with “timely”. (3)
(49) The feedback and reporting loop to the incident manager is very immature and inconsistent. (2)
(50) This would very much depend on the nature of the security incident/breach. Providing early feedback can help to calm or inform the reporter that action is being taken. However if it is a major or critical incident then sometimes more facts will need to be gathered before any feedback can be provided. (3)
(61) Intuitively, to me “reporting community” means organisation. I wouldn’t expect incidents to be routinely shared outside of my organisation except in a summary/aggregated format, or useful details e.g. threat signatures. I’m not sure if you are suggesting that incident details should be routinely shared with the wider industry base, or if you mean a CISP-style sharing community partnership (3)
(63) I am not sure whether this is a comment on CSF 2, 3 or 4 but the sense that an essential pre-requisite for staff
to report incidents and near misses is confidence that they will not be blamed may not come through as clearly as it should. Rather, it is failure to report that will be penalised. The organisational culture should view helping others to avoid similar situations as commendable behaviour. This is fundamental to aviation safety where anonymous reporting arrangements, often through third parties, have proved themselves. (2)
(70) And this largely answers my points at Q2.1 above. (2) *But I felt there were a couple of missing points:*
consistency of reporting of different types of incident.
need for ‘no blame’ culture in incident/near miss reporting to encourage openness.
(87) No experience of using the reporting process **-** lack of reportable incidents. (3)
(115) See 1.1 response (1) *Questions are simple and unambiguous with defined maturity statements*
(CG7) Ditto (2) *Clear and explicit but provided you now your subject matter. Not sure that this would be of use by Internal Audit as they would not have the breadth of knowledge required.*

(CG11) Easy for my own organisation because I am involved in the process however if auditing another organisation I would need evidence to support the scoring (2)

3.2. Based on the Critical Success Factor and the level description how easy would it be to use to judge your or another organisations position in the maturity model?

(8) There are a couple of factors here – if the feedback/support is given (auditable) – you would ideally also want to measure whether it was understood or even acted upon by the recipient (i.e. would it change behaviour or increase vigilance).
The other distinction you probably need is between specific and general feedback. Its very easy to give an overly standardised or general message "Thanks you for your report. We are dealing with it" might be counter productive and appear like an unattended mailbox of there is no case-specific feedback. (2)

(17) As above - Need to be either involved in the incident reporting process or chain or allowed to review the reporting process and reported incidents (and associated information) and interview appropriate personnel (2)

(29) Very easy to judge our own, perhaps slightly less easy to judge the level of in another organisation without sufficient evidence (2)

(37) Same comment as given for CSF1 (I liked the fact that there are general CSF descriptions to further explain the CSF itself, as well as a brief description against each level. The descriptions are clear, allowing me to make a judgement regardless of sector the organisation is in. (1))

(40) I would suggest there is an issue here of risk assessment. You may be at level 2 for low risk incidents, but at level 4/5 for high risk incidents. A large number of similar low risk incidents should be picked up in Factor 4 below, but may not need to be dealt with individually. (4)

(42) Assessing feedback directly will depend on whether and how the feedback is provided and recorded.
Feedback may be provided electronically and so be recordable (e.g. emailed to individuals or groups, or disseminated to all employees via Intranet or newsletters). Alternatively, it may be delivered face to face, in which case examining it afterwards will not be possible.
The amount of feedback provided may also vary widely. It may be a simple email acknowledgement or a series of face to face meetings (if support is required).
In order to judge the Maturity Level, rather than assessing feedback directly, it may be easier to interview staff who have been involved in incidents, to get their opinion on the feedback they received. (3)

(54) Use of metrics would assist the process, so established for example would mean x events are reported on and managed by the business, based on what are the important success criteria as defined by the business (4)

(55) Similar comments re consistent use/trust in who had carried out the assessment/when/etc (2)

(72) As above, these processes should create their own evidence (1) *At any level above 1 there should be evidence/records to support the judgement*

(74) I would need to dip sample responses from a number of teams to make a value assessment. Although we have a relatively new and common case management system I am not confident that all case notes would necessarily detail feedback. Not straightforward. (4)

(87) As per previous box (3) *No experience of using the reporting process - lack of reportable incidents.*

(115) Again I see this as dependent upon the culture and attitude of the assessed dept. (3)

(CG7) Ditto (2) *Clear and explicit but provided you now your subject matter. Not sure that this would be of use by Internal Audit as they would not have the breadth of knowledge required.*

(CG9) Should be able to quite easily evidenced by production of incident records (2)

(CG11) Easy for my own organisation because I am involved in the process however if auditing another organisation I would need evidence to support the scoring.
(2)

CSF 4 Comments and ref number of respondent

4.1 Based on the Critical Success Factor and the level description how easy was it for you to interpret the maturity position of your/another organisation?

(26) I would question the wording of Answer 2 (“A process is in place”). This response belongs in Answer 4 or 5. An immature organisation which does not analyse incidents well is unlikely to have a process in place to do so. (4)
(37) Same comment as given for CSF1 (I liked the fact that there are general CSF descriptions to further explain the CSF itself, as well as a brief description against each level. The descriptions are clear, allowing me to make a judgement regardless of sector the organisation is in. (1))
(42) It was easy to understand the distinctions between the 5 Maturity Levels. (2)
(45) Spot on (1)
(**50)** I would add that based on evidence I have seen and been involved in at my Organisation for major/critical incidents of a data loss or similar type event, a senior gold group is established under the Deputy SIRO to look into root cause analysis and wider system processes to ensure improvements are put in place. (2)
(54) For the company this was straightforward as a lot of time has been invested in the processes. However, for other organisations this may prove challenging (2)
(63) Again here, it is essential that it is failure to report and therefor to risk situations repeating themselves that
should be unacceptable and the subject of censure. It is right to focus on training and development needs and to organisational or process flaws but these must be seen
as failings of management and leadership - which takes one full circle to CSF 1! I am also very wary of language like "lessons learnt" and which suggests that anything
can be prevented (level four). The proof of whether they have been learned is whether or not they are repeated. "...lessons identified...and changes made to policy/
procedure/process to reduce the risk of reoccurence" might (3)
(70) Understandable and clear – yes – but this is likely to be the hardest area to assess. (3)
(72) In three places you imply that the aim is for incidents to be “prevented” or “not recur”. That may be too absolute for many business risks – e.g. loss of laptop can only be prevented by not issuing laptops and insisting that staff only work in the office. I tend to talk about reducing risks to the acceptable level for that business. But there’s probably an official ISO etc. phrase. (2)
(87) The intranet offers a Security Breach Matrix that allows line managers to assess the impact of an individual breach. I have no indication of the extent of its use. (3)
(89) Only the sophisticated and mature practitioner is likely to have much idea of what analysis is called for, and how output might be useful. Case studies are a useful tool for briefing users and management; statistical facts are also useful for briefing (4)
(92) In my thinking, this was tied in with CSF 1 (1)

(115) See 1.1 response (1) *Questions are simple and unambiguous with defined maturity statements*

(CG7) Ditto (2) *Clear and explicit but provided you now your subject matter. Not sure that this would be of use by Internal Audit as they would not have the breadth of knowledge required.*

(CG11) Easy for my own organisation because I am involved in the process however if auditing another organisation I would need evidence to support the scoring. (2)

(CG13) Whilst easy to understand it is complicated by the fact that we adopt a risk based approach whereby certain incident types are subjected to a very detailed investigation. (2)

Q 4.2 Based on the Critical Success Factor and the level description how easy would it be to use to judge your or another organisations position in the maturity model?

(8) One would hope that for a given incident, the root cause/issues leading to it/contributing factors had either been identified or not. There would be some use in making sure that trends were also captures – i.e. data across incidents that indicated recurring problems or common origins (1)

(17) Need to be either involved in the incident analysis, investigation and remediation process or chain or allowed to review the supporting evidence and information for those events where analysis was required. (3)

(29) Very easy to judge our own, perhaps slightly less easy to judge the level of in another organisation without sufficient evidence (2)

(37) Same comment as given for CSF1 (I liked the fact that there are general CSF descriptions to further explain the CSF itself, as well as a brief description against each level. The descriptions are clear, allowing me to make a judgement regardless of sector the organisation is in. (1))

(40) This would all depend on the competence of your analyst and potentially their security knowledge. There may be a split here with specialist security professionals carrying out risk assessments, and specialist analysts carrying our analysis. Again the risk assessment process is critical together with your risk appetite. (4)

(42) Root cause analysis will almost certainly be documented, in order to capture lessons learnt that can be followed through. It should be easy to look at the results and check what's happened, in order to assess the Maturity Level. (2)

(45) Spot on (1)

(47) I have answered every question at 1. Very easy. This may be because I have been involved in this evaluation process from the beginning. I expect you will have considered, but you may obtain more useful feedback from people who have not seen the Critical Success Factor matrix before (1)

(54) For other organisation, as stated earlier, what are you comparing it to? Your own standards? Or defined metrics which can be quantified? (4)

(70) As above. (3) *Understandable and clear – yes – but this is likely to be the hardest area to assess.*

(72) Assessing the completeness of investigation might involve a bit of work to partly re-analyse and work out whether the conclusions reached/actions taken were reasonable (2)

(73) Difficult to judge due to complexity of organisation and lack of robust commercial arrangements. (4)

(74) Post Incident Review is embedded into our processes for major incidents. (2)

(89) There is room in our world for a more detailed guide on the analysis of incidents. I would rather have a superficial investigation than none; and a superficial investigation could well indicate that there is nothing to be learned from this one. Sometimes we have to prioritise. I remember when we used to investigate all crimes – no matter how much they were non-starters. Now we investigate almost none. The knack of it is picking the winners !

(4)

(103) This will always be difficult to judge as it is more about understanding long term change as to how an organsiation is learning from its mistakes. There perhaps should be something in here around evidence that the business has adopted the change. (4)

(115) This may be a complex analysis process based upon the type and complexity of the incident. An organisation may be well versed in dealing with a specific type of incident or range of incidents, but when something comes in from left field, it may cause problems. (4)

(CG7) Ditto (2) *Clear and explicit but provided you now your subject matter. Not sure that this would be of use by Internal Audit as they would not have the breadth of knowledge required.*

(CG9) In depth knowledge of incident records, actions taken, changes to processes etc would all be involved. Assessing overall performance would therefore require research and then a yardstick to measure what ‘good’ looks like. (3)

(CG11) Easy for my own organisation because I am involved in the process however if auditing another organisation I would need evidence to support the scoring. (2)

(CG12) In some cases I believe there may be difficulties in enforcing actions that come out of lessons learned. So even though the process is completed it may not be effective. (4)

(CG13) Need awareness of the business risk appetite. (3)

General Answers on Maturity Models Comments and ref number of respondent

Do you use maturity models in your organisation or one for which you have reviewed or assessed

(8) Not so much in current role, but have in the past. (Yes)

(12) Maturity models are used sporadically and as a supplemental tool rather than a required assessment method. (Yes)

(17) Have provided advice on the choice of available maturity models and the content of assessment mechanisms to HMG organisations. (Yes)

(20) We use maturity models for Information Assurance. (this appears to be 2 different questions and I am not sure that the question makes sense. Is there a word missing?) (yes)

(37) My own organisation is an SME and as such we do not use MMs as they tend to be too cumbersome and rigid in their application. Equally, I have not had the opportunity to apply MMs during an assessment of another organisation .(No)

(40) We have in the past they became far too complicated and were not able to be accurately used by large and small teams. (No)

(42) I have some experience of using Maturity Models (did not score)

(49) Although an IAMM is not formally used, its context and content has been adopted in various aspects of risk assessment and management. (Yes)

(50) In all honesty I am unsure whether or not a maturity model is in place for security incident reporting, but there is a well defined process. (Yes)

(52) BT, GCHQ spring to mind - both large organisations with time and staff to spare who do this sort of thing (Yes) **(54)** As we are ‘accredited’, we are subjected to a number of independent audits by the MOD accreditor which happens on an annual basis. Of course the success ‘criteria’ are clearly defined as compliance requirements are clearly laid out. (Yes) **(74)** SIM3 (Yes) **(77)** Not personally, but I’ve seen discussions of others using them (Yes) **(86)** Maturity modelling, with well defined definitions of each level, are a good method of highlighting the delta between the now and the future. (Yes) **(87)** [Redacted] is effectively a lodger unit within [Redacted]. Although involved in infosec across the police community, we are seldom involved with it in Home Office. (No) **(89)** Maturity models have been mandatory for the police service for at least five years. (Yes) **(93)** IAMM and DIAN (Yes) **(96)** Not as far as I'm aware (No) **(103)** Originally used the IAMM - however are no longer using this. This Incident Maturity will be useful to gauge our current standing and how we can improve. (Yes) **(107)** In Korea, there is a certification scheme for information security readiness assessment that is to measure maturity for an organization. Please see at http://www.kfict.or.kr/board/index.html?board_id=business2&action=list. Sorry for being written in Korean. (Yes) **(116)** One client is currently using ISF – but the Information Security team are answering the questions without full recourse to the experience of the business themselves and are thus positively responding irrespective. Marking one’s own homework is never a guarantee of security nor success. (Yes) **(CG7)** The College uses ONE3M [HO model] and have and do use IAMM as a point of reference. (Yes) **(CG9)** The principles described for security incidents are all known and aspired to. Other IA areas where maturity models could feasibly assist have been broadly covered through the previous IAMM, but which finally outlived its usefulness as a constructive tool. It is hard to see where such models could have significant value in the future.(No) **(CG10)** Previously used the IM Maturity Model when it was an accreditation requirement from [Redacted] (No)
Do you personally feel maturity models are useful tools to assist an organisation understand where they sit regarding to a particular situation
(1) Mixed with this one. I have known organisations to massage figures to score more highly than perhaps they should. This, of course, is an integrity issue, and one that is difficult to allow for, but is noteworthy nevertheless (No strong view) **(4)** As long as in addition to defining requirements they provide a vehicle for submission of supporting evidence (Yes) **(8)** Normally they work best if there is some comparative data from the wider industry or same sector upon which to compare. An organisation might have medium maturity, but be streets ahead or behind other similar business – hence for a give rating is the action to strive to improve, or accept that you are relatively OK. (Yes) **(12)** If they are short, sharp and simple to follow – as per this example here I feel they can be very useful. (Yes) **(15)** I think it is dependent on the organisation size and maturity! As an SME with relative mature internal processes, then I do not find them useful. However, as a tool where the level of maturity is lower, then they are good at helping set priorities (No view either way) **(21)** I believe how organisations deal with security incidents are integral to an effective security culture and in some cases maybe one of the few times a member of staff engaged with the security team, so a maturity model is most welcome. (Yes)

(36) Maturity models, baselines, etc. are a good way for measuring, maturity, compliance, etc. especially where you work in large organisations that rely on third parties to provide managed services i.e. it enables all parties to converse with the same terminology, thereby ensuring consistency, repeatability, & traceability. (Yes)

(37) I personally believe that MMs have a use so long as they are used within the wider context of the operating environment to provide an internal understanding of the organisation's current capability within that environment. From anecdotal evidence, I understand that organisations have a tendency to use a MM assessment as a 'scorecard' to deliver a security goal or to achieve a particular 'standard', which once achieved results in no further improvement. (Yes)

(40) If they are simple they can be more use than if they are complex. They can give an indication of an area of concern, but not necessarily pinpoint the exact issue.(No strong View)

(49) As long as the model used is relevant to the organisation’s business and stated risk outcomes. (Yes)

(50) Yes, I believe that the use of a maturity model would very much assist the Organisation is dealing with major and critical security incidents and breaches. (Yes)

(52) Depends how seriously the outcomes are taken - eg: Board or Audit Committee level, Harder for SMEs. (No strong views)

(54) Yes, organisations should understand where they sit with peers, so in the market segment should they spend more of less?
Of course, also driven by regulatory requirements (Yes)

(70) Actually my personal view is Yes with a strong caveat, hence the tempering of response. They are very useful where they are used properly, but there is a danger of them being used either as confirmation of perceived goodness or as sticks, rather than as genuine assessments to inform activity. (no strong view)

(73) They are a good benchmark but only as good as on that day and area you assess (Yes)

(89) They are helpful in generating a little self appraisal; they are flawed by the lack of objectivity. And there is a competition for effort/resources – between doing the day job (in my case Policing), dealing with the practicalities of IA, and reporting IA. I would suggest that one report/return annually, or even biannually, does the trick. (Yes)

(94) I am an advocate of maturity models. For me one of the key elements of any maturity model is that the results lead to an action plan (as a result of a gap analysis) so that improvements can be made where the model shows weaknesses. It is also important that the model may be applied iteratively to demonstrate progress, or the lack of it(!), and that comparable analysis with previous results can be shown to management. (Yes)

(107) Definitely, the maturity model is very important to improve the posture of organization for the information security. (Yes)

(116) Only because it is usually a self-assessment response and one provided in isolation so there is little measurable value to be gained. Years of experience breeds scepticism unfortunately. (No)

(CG4) Senior management need to take the lead and push outstanding issues through. Should be done independently (No strong views)

(CG6) As long as they are direct, concise and do not take up a disproportionate amount of time to complete. The effort cannot outweigh the desired outcome.(Yes)

(CG7) They are incredibly important to review your maturity and take out the personal factors which can distort views. (Yes)

(CG8) Personally, my first review of a MM, one that I found both useful and informative. It gives confidence that the critical elements that need to be considered are just that, considered. (Yes)

(CG10) As long as it is understood what the maturity model is there to do for the organisation and ensure there is a consistent understanding across the

profession if they are using it for a common purpose (Yes)
(CG11) It is a useful tool to show senior managers where they sit within the maturity model and provides the information needed to support future progress and strategy. (Yes)
(CG12) I believe they can but you can easily interpret the question to make you sound more or less mature than you are. Or you may score highly but there are still issues which are then ignored due to the score being high. (No strong views)
(CG13) They can be beneficial provide the benefits are recognised at a senior level. They also need to be used over a period of time to identify the organisation’s direction of travel/trajectory. (Yes)

Some maturity models set out a larger number of elements to measure against. Is just listing the critical elements a better approach.

(1) Subjectivity is limited as much as possible by using only critical elements. (Yes)
(7) This prevents the model becoming a ‘tick list’ and requires greater understanding to implement a system. (Yes)
(8) The shorter any questionnaire/survey/assessment is the easier and more likely it is to be adopted.(Yes)
(12) More complex and complicated models take more time and in most organisations this a much valued resource. (Yes)
(17) Critical elements should be concentrated on. However a more granular approach may enable an organisation to better show progress (or lack of progress) in addressing identified gaps. (No strong views)
(20) Listing the critical elements is a good starting point to achieving a base line minimum standard as quickly as possible. However, when that is done there may be opportunity to increase the number of elements to seek to achieve thus enhancing the standard above 'base line' (No strong views)
(21) The key to any good model is to keep it simple. I believe four is about right. (Yes)
(26) Both approaches have merits, depending on how much detail is required and how much time the participants have available
(No strong views)
(29) In my opinion just listing base line critical elements, with yes/no answers, provides a narrower less helpful view (No)
(36) Too many elements leads to complexity, variability & so on. Listing the critical elements is a common-sense approach that is not overly draining (Yes)
(37) On the whole I would say 'Yes', as this would make it easily scalable for different sized organisations. For example, you have covered the 4 key aspects of incident management and any size organisation should have these in place. An SME could use this MM with little worry, or drain on resources, and still achieve a managerial understanding of its capability just as a larger organisation could. (Yes)
(40) However, you may wish to go down to the lower level if you are scoring low (1.2 in your example), but there would be no need if you were at 4/5. 3 would always be a discussion based on appetite. (Yes)
(42) Listing the critical elements is a better approach for organisations at the lower maturity levels, as it will enable them to focus on the most important factors.
Including further elements may be useful for organisations that are already at a medium or higher level. I would expect the law of diminishing returns to effectively determine a level, beyond which is not cost-effective to go, for each organisation. **(**no strong views)
(45) That very much depends on the individual situation and what benefit you are looking to derive out of the CMM. (Yes)
(49) Many organisations only have appetite or resources to manage the critical elements however they need to be cognisant of the wider elements and

impact in order to fully understand where they sit within the scale. The key is how this is presented and in what order. i.e. critical elements first with the remainder as an appendix for reference as necessary. (Yes)

(50) Again this would depend on the nature of the security incident/breach, maybe there should be different variations of the maturity model. (No strong views)

(51) complete listing of detailed elements allows a maturity model to form the basis of a workplan for improvement, but the critical elements approach allows a rapid comparison against best practice and/or other bodies. (No strong Views)

(52) Interest can be hard to sustain doing a mega-questionnaire with similar but not identical questions (Yes)

(54) Time is money, so all automation of processes is beneficial, as well as the ability to complete compliance statements via the intranet supports the process and buy in (Yes)

(55) I think you need some substance behind the headline statements – certainly for lay, non-expert practitioner use
(Ticked No strong views and No)

(57) Previous iterations of security related maturity models have been very long and laborious with organisations choosing to move away from their use. Whilst the overall results and assessments can be very useful in providing indications of areas for improvement, the complex models tend to be avoided. (Yes)

(61) Measuring against sub-criteria adds value but also complexity. (No strong View)

(72) Number of elements depends on the scope of the model, and the extent to which factors are common to all organisations. E.g. the Security Incident Management Maturity Model (https://www.trusted-introducer.org/SIM3-Reference-Model.pdf) has more factors because it covers a wider area. I suspect that incident reporting is both a narrower area and one where you'll get into more-than-one-way-to-do-it if you dig much deeper. (No strong View)

(74) A common standard for maturity models may be useful where security teams from disparate organisations need to interact for the common good of security. Each team may then know what to expect in terms of capability from others, where each has been accredited against a particular model. (No)

(85) I think it is important to understand the client or audience involved and adapt accordingly. (No strong view)

(86) Simplicity is important, but as mentioned above, clear definitions for each level (which may itself include a number of measurements) will enable more specific assessment.(No strong view)

(89) More than two A4 sheets of questions starts to feel oppressive. May well outreach the attention span of senior management.
(No strong view)

(92) Definitely, otherwise there is a danger of focusing on the process and losing sight of the main goal. (Yes)

(93) Many maturity model are too complex and hence resource intensive. (Yes)

(115) It's the same as lessons *learned* vs lessons *logged*. If all that happens is a list if events is listed, nothing changes and an organisation will consistently fail to improve (No)

(116) I want a "sort of" option! Looking at one element in isolation ultimately only means more work to pull together all the other elements that should be being considered. (No)

(**CG4)** Time consuming but the Force would have a better understanding.
(No strong views)

(**CG5)** I think that it very much depends on the criticality of the matter under review, any maturity model should be designed to focus on analysis of a

known (desired?) maturity level by use of a consistent set of questionnaires and scoring. (No strong views)
(CG6) See answer above. There is a balancing act between being too generic and being too granular. Getting that element right is the key to making a Maturity Model work for an organisation.
(No strong views) *As long as they are direct, concise and do not take up a disproportionate amount of time to complete. The effort cannot outweigh the desired outcome.*
(CG7) Possibly! Listing can be bland but with the IAMM there is an opportunity to expand. Personally the IAMM is an excellent tool with both listing and comment. (Yes)
(CG8) Absolutely, if only the critical elements are considered then I would suggest this would give some clarity to organisations, the less critical elements would, in some cases, be unique to that business and can be considered separately if required. (Yes)
(CG9) Setting out, or even in some case prioritising, principles could add value in some cases – and perhaps benefit people who are new in some business areas. (Yes)
(CG10) As an initial measure to build on – once embedded you may wish to identify priority areas that require more specific elements to measure against (Yes)
(CG11) Some maturity models can be very bureaucratic therefore critical elements is a good way forward. However it may require additional evidence column to support scoring. (Yes)
(CG13) Yes but senior management need to see that there are real benefits to any such review. Also not everyone would wish their results to be publicly available. (Yes)

Specific questions on the Critical Success Factor Maturity Model

Comments and ref number of respondent

Overall would you consider this maturity model to be of value to your organisation to assess how security incident reporting is handled and managed against the identified Critical Success Factors

(8) Current company is quite small, but the model looks useful based on past clients I've worked with (2)
(12) Carrying out this in my own organisation, perhaps even required by our national accreditors, would be a good way of highlighting any shortcomings to senior management.(2)
(15) … but limited value.
We have an incident response plan, and are aware of the frailties.
Also, having answered the questions, it lacks the "so what" factor. (2)
(17) The criteria set out are very clear and easy to interpret – *good piece of work Mike :-)* (2)
(21) is that a mature incident reporting model needs some 'teeth' at times. Whilst recognising that the 'open hand' approach usually works better than the 'closed fist', I feel there needs to be clearly defined strategy for dealing with people that are ambivalent or seek to disrupt the security programme. (2)
(37) I like the straightforward nature of this MM, in which it describes the key elements of incident management that can be easily understood by non-technical management and can be evaluated in real-world terms. It is concise which can give a quick look overview that would be applicable to most

sizes of organisation.(2)

(42) An assessment could point towards areas that could be improved. These could then be assessed, to determine whether improvements may be cost-effective for the organisation.

It would also be useful to have information on how other companies are distributed among the Maturity Levels, although I realise that this research isn’t aiming to provide this information. (2)

(49) It clearly and simply defines what success factors are relevant and why and how they are to be scored. (2)

(50) Yes, I could definitely see the benefit of using this or a similar maturity model. (2)

(52) I'm thinking of [Redacted](where I am a NED) - an SME - as an easy way to help them start thinking about maturity. (2)

(55) Although, if we hadn’t already done it, then it would have been v useful – we had to create our own metrics (2)

(61) I see how this is useful as a talking point to management but believe that a sample process/checklist would be more useful to guide implementation. (3)

(63) This depends entirely upon what is done with the output and whether it informs the delivery of better outcomes. If it is not used by senior management, and communtiacted to the wider organisation as a vital metric, it will decay into just a box ticking exercise.(3)

(72) As below, I hope these points are already included in our ISO27001 processes, so main value would be to check we’ve not missed anything and as evidence that we’re not being unreasonably demanding. (3)

(74) Because it is relatively brief, unlike SIM3, it is more likely to gain the attention and engagement of the seniors. It may also be a catalyst for further exploration of the organisation’s security posture and readiness for dealing with incidents. (2)

(77) After a strong mechanism and campaign round its introduction, we have effectively got to roughly the right place on incident reporting, and these CSF don’t particularly help with the final polishing.

They would have been useful five years ago for us, or for any company who had not been on this journey. (3)

(86) Assessed the majority of the questions above as Easy to Understand, but overall, the approach would be extremely valuable. (1)

(87) The unique position of [Redacted] in [Redacted]means that I'm less able to assess this question. (3)

(94) Where I would find this model and the 4 CSFs particularly helpful would be in highlighting to the SIRO where I see vulnerabilities in our current incident reporting mechanisms. In some quarters in my organisation there seems to be a belief that, “We’re the Police. We’re good at responding to incidents.” Unfortunately that doesn’t always play out in practice but I have no concrete method to showcase my concerns except by risk briefings and anecdotal evidence. This model would give me a tangible vehicle to highlight where I see immaturity and where we could improve (2)

(103) would look to use this model to understand how Incident Management is embedded into the organisation and what areas I need to improve to have a more efficient process. (2)

(115) When can I start using it? (2)

(116) As a lone consultant, it depends on the projects and organisation as to what is already in existence. In a great many organisations, incident management is handled outside of the remit of security and traction is extremely difficult. (2)

(CG2) Once I started thinking about the critical success factors, it prompted me to think about small changes to improve our current process. (2)

(CG6) It fills the space between the Security Policy Framework requirements for incident reporting and the desired outcomes. (2)

(**CG7)** Allied with ONE3M and IAMM this could be used to influence in and point out that the others may be HO but this is broader. (2)

(CG10) We are currently looking at Tri-Force Collaboration and a model such as this could make identifying the stage each force is at easier (2)

(CG11) Once finalised it will be valuable. (2)

(CG12) I don’t think that it would pull out the issues we have with our reporting process. (4)

If other organisations used the same model would this assist when determining the ability of that organisation to handle incidents? (for example if exchanging data with them or contracting them as a third party supplier

(7) This would depend on the level of understanding and detail behind the reason for the scores.(2)

(8) Definitely, but also it would allow cross-industry/cross-sector comparisons to be made which would really focus attention.
I think a measure of “relative maturity” is possibly more useful than just “maturity”(1)

(12) We rely heavily on some third party organisations for handling some areas where security incidents would be included and knowing where they sat in relation to this would be extremely useful to compare, contrast and gain confidence. (1)

(15) We’d look towards 3rd party audited 27001, and not the specifics in this area.(Neither /nor)

(20) As your example suggests, exchanging/sharing information with partner agencies (not contractors) is often 'accepting' of a notion that the partner has a suitable structure to handle data. Few would have time to put that to a test! (1)

(22) A lot of the scoring is subjective and open to interpretation. Whilst this is of value to me internally in my organisation it would be insufficient to make any judgement on another organisation. (4)

(29) Our information sharing agreements ask that any external organisation we share with has incident management processes but we do not (usually) go any deeper than that at present. Knowing the maturity level of an organisation would be helpful in some sharing cases (particularly those where more sensitive data is being exchanged) but not necessarily a deciding factor in some of the less sensitive arrangements. (2)

(36) Yes – as per my comments in the General Questions table above ☺ (1)

(37) I think there is value in understanding the current capability, so long as it is not looked at in isolation of the wider operating environment. MMs should be used in context to provide a 'part' of a balanced view of the operating capability of an organisation. (ie an organisation may score low on a CSF, but it may not be critical to its operation or ability to recover from a situation).

(38) If it were answered honestly and by someone who knew the organisation well.(2)

(40) Only in areas with a similar appetite and physical make-up (numbers, buildings, locations) (4)

(42) The value of using the model would depend on whether findings had been independently assessed. If findings were independently assessed, an organisation's use of the model would be valuable to other organisations. If not, an organisation's use of the model would not be very valuable to other organisations e mail 10/1/17 0948 gives above amendment to answer and replaces sentence below
~~The value of the model would depend on whether findings had been independently assessed.~~
It would not be wise for an organisation to rely on another organisation’s self assessment. (did not score)

(49) A common approach across all organisations is the nirvana of maturity models. However, with the SPF based on outcomes this is becoming less likely. (1)

(50) As above. If Organisation used the same or a similar model then yes this could certainly prove beneficial to Organissations. (2)

(55) Yes – if it became a standard comparison? (1)

(61) Difficult to assess simply as part of an assessment (e.g. ISO27000 series) as many of the criteria require a lot of data to validate. For example we conduct around 50 supply chain audits a year and cannot spend the time to understand how many staff know of the existence of a reporting process. We would have to rely on data from the audited company. (3)

(63) See comment above. It should be of assistance but it takes two to tango. *This depends entirely upon what is done with the output and whether it informs the delivery of better outcomes. If it is not used by senior management, and communtiacted to the wider organisation as a vital metric, it will decay into just a box ticking exercise* (3)

(70) My concern is the difficulty of consistency of assessment, even with a relatively clear and simple model like this. Although it is clearly worded, how do I know that your assessment of your organisation has been as honest as mine of my organisation? Or even, as one MM response I once saw suggested, that you had even understood the question! An independent assessment would offer more value here.(3)

(72) Of more value when assessing software/service vendors. At present we informally assess what their approach to vulnerability handling is, but this could make that more formal (as well as giving those tendering a clearer idea of what we expect). (2)

(74) As per my comments earlier about a common standard. (2) *A common standard for maturity models may be useful where security teams from disparate organisations need to interact for the common good of security. Each team may then know what to expect in terms of capability from others, where each has been accredited against a particular model.*

(77) It's more we want our partners to have good incident handling processes, and if this model helped them, it would be good. (2)

(86) At a minimum it would highlight the areas for improvement**.** (1)

(89) Yes but consider also some dynamics of reporting – some of us report low, with the intention of obtaining funding/resources; while others report optimistically for reasons of ego and reputation. I think that the top of the league table is a tricky place to be – because others want to knock you off, and management see yours as a problem that is no longer needy, and promote a more needy problem for the purposes of allocating funds/resources.
I tend to be pragmatic – a perfectionist would be disgusted by my reporting ! Standards are a problem with self assessment. (2)

(115) Standardisation is always beneficial (2)

(116) There are already too many questionnaires and assessments required in order to evaluate the performance of third party suppliers therefore the likelihood of value being realised from asking for this to be completed is potentially reduced. (3)

(CG6) Anything that helps a partner organisation understand and interpret another's IA Maturity is to be welcomed. More commonality would reduce risk. (2)

(CG9) In my experience, the tool could be of value to some partner organisations where IA principles are not sufficiently followed, or understood. (2)

(CG10) It would give you some baseline evidence and you could ask further questions or not dependant on the risk level (2)

(**CG11)** It would be valuable however from experience it is very difficult to get partners or suppliers to engage in the process unless it is specified in the contract. (2)

(CG12) It would act as a level of confidence and if the classification of information was OS and below I think this would be perfectly adequate. (2)

(CG13) I would however be sceptical about whether or not other organisations would be prepared to be as candid as they might be if they knew the information/results were published. (2)

Once refined would you consider using this maturity model in your organisation or one you would be assessing

(12) I would need to get the cooperation of the organisations senior management and a commitment to working with the results.(Possibly)

(15) Possibly, tending toward no. (Possibly)

(17) Consistency regarding the choice of model is necessary if an organisation is to measure its' own progress or rank its' maturity against the maturity

of other organisations. If this model where appropriately adopted I would be perfectly happy to use it. (possibly)
(37) I would definitely consider using a version of this MM as part of any wider evaluation as I like the concise nature, simplicity of use and the focus on the key requirements of the capability. (Yes)
(45) This would be a good model to use and develop. I would be interested in developing it further for use in our consultancy practice. (Yes)
(52) As above – [Redacted] *I'm thinking of [Redacted] (where I am a NED) - an SME - as an easy way to help them start thinking about maturity. (Yes)*
(72) I suspect it's already covered by our ISO27001 processes, but would suggest that our Quality Manager compare ours with yours to see if we've missed anything (Possibly)
(74) We have used SIM3 recently. (Possibly)
(77) Not my role to do this sort of thing, and as above "we've made most of the journey already" (No)
(85) I am not in a position to authorize adoption (possibly)
(89) I am just a contractor – I will do whatever my customers want me to do, within ethical parameters. (no answer given)
(115) I have already started to apply some of the knowledge that I have learned through the review of this model. (Yes)
(CG2) But only at my level, in order to make slight adjustments/improvements to the process. (Possibly)
(CG6) Yes. See above two answers. (Yes) *It fills the space between the Security Policy Framework requirements for incident reporting and the desired outcomes. Anything that helps a partner organisation understand and interpret another's IA Maturity is to be welcomed. More commonality would reduce risk*
(CG7) I can never predict what senior managers will do. That said this would be a good step forward. (Possibly)
(CG9) I would only see as adding value in non-policing organisations
(Possibly)
(CG11) I am a supporter of MM therefore would use this to promote better reporting and management of incidents. (Yes)
(CG12) It feels that the maturity model is aimed at small organisations. I feel it would be beneficial re third parties. (Possibly)

Would just knowing what the Critical Success Factors are and using an internal method of ensuring a gradual move to ensure they were embedded be a better approach for your organisation

(1) My organisation is very change resistant. Slowly but surely would definitely be an advantage. (Yes)
(7) They would be a good basis to develop systems and understanding further but on a risk/return scale 'optimised' may not be seen as the desired level when considered against the wider security needs and tasks.(possibly)
(8) Sadly, it is often the case that the adoption of any given improvement (or model in this case) is often driven by a past issue, by a mandated compliance driver or by peer comparison – rather than actual business need or value. (possibly)
(12) This is more likely to succeed in my organisation but, again, I would need to ascertain buy in from senior management.(Possibly)
(21) There should always be scope for organisations to adapt models to meet their needs, but this is certainly a good starting point. (possibly)
(26) I didn't fully comprehend this question. For example, "...be a better approach" than what? (possibly)
(36) I think accepting these as the definitive CSFs is a better approach. Using an internal method & gradually moving to the CSF's has the potential to create the worst possible outcome for all organisations. I have seen time & time again where project managers have "invented" CSF's that lacked

consistency, were bloated (i.e. too many CSFs), catered for the project specifically & not the organisation overall, such that they became unusable on the next project or elsewhere in the organisation.

As an example, these 4 CSFs could be thought of like the ISO31000 5x5 Risk Matrix – well known throughout many organisations. (No)

(37) I think that identifying the CSFs provides focus on the areas to concentrate efforts, especially for less resourced organisations such as SMEs, whilst level descriptions helps management to understand their current capability and assess their risk. I do not think a MM should describe 'how' (or even 'if') an organisation should develop their capability but provide evidence towards an informed view and so allow informed decision-making to be made on future development within their operational environment.(Possibly)

(40) Form filling is fine for collecting information (maybe for benchmarking), I'm not sure it does a lot to focus future actions. Completely depends on the culture of the organisation**.** (Possibly)

(42) I think a commitment to self assessment and improvement, where necessary, would encourage actual improvement.

Just knowing what ought to be done probably wouldn’t help enough. It wouldn’t necessarily reveal exactly where the problems are. (possibly)

(45) Securely sharing aspects of the data and lessons learned external would allow for better implementation, use and maturation of the model. (Possibly)

(49) This would provide the end state for an organisation to achieve but allow them the flexibility and their own choice in how they might achieve it. (Yes)

(50) I could certainly see the benefit of a more gradual implementation and ensuring that it is properly understood and implemented correctly, rather than just playing lip service which often happens when teams, managers and staff are under pressure. (Possibly)

(52) Will test on [Redacted] as the year progresses (Possibly)

(57) Would be more likely to use the maturity model as is rather than extracting the CSFs and assessing against them independently using other criteria. The CSFs themselves could be useful in providing high level Input to board briefings on this subject and security more widely to indicate areas of focus. (No)

(61) I think the most benefit would be combining this model with some implementation guidance, whether a process map, checklist or similar.(No)

(63) See comments above. Simply having a maturity model and a score is of no value unless it is acted upon and reflected in behaviour at every level in the organisation. Absent committed and visible leadership from the top -
including all members of the Board - the CSF Maturity Model will be of no more than academic value.(Possibly)

(70) I have answered not necessarily as better than implementing the model (question above) but as an alternative approach which I think is of value. (Yes)

(72) Useful to have specific targets, rather than just “more embedded” (No)

(77) I suspect many organisations would prefer to do things according to their internal culture, so adapting any given model (rather than just accepting as given) is common. (Possibly)

(89) If management are allowed much discretion, they can be expected to exercise it by reducing costs/efforts. (No)

(92) But senior management may be better persuaded by the standard IRMM tool. (Possibly)

(93) I would suggest that some examples of what good looks like for each would assist the development of an improvement plan. (Possibly)

(94) I’m not sure how “ensuring a gradual move” could be measured. If (as regularly happens to me in other contexts) I’m challenged by senior management with, “Is there a risk?” and I answer “Yes, sir” then invariably the next question is, “How big is it and what do we need to do about it?” If

I were to highlight a vulnerability in our incident reporting mechanisms a maturity model approach gives me a means to measure, evidence and qualify my concerns then demonstrate progress to address any identified gap. (No)
(CG6) It is preferable to have a line in the sand to work towards and measure against. This also helps towards commonality between third parties and the understanding of IA Maturity. (No)
(CG8) Yes, Having sight of the CSF's would give us strong foundations that we could use to develop our internal processes and procedures, one particular area that springs to mind is staff awareness training, both initial, and ongoing training.(Yes)
(CG10) But I strongly believe that a consistent approach that enables organisations to know that they are comparing themselves to others on a like-for-like basis helps all parties understand the ir own and others positions. (Possibly)
(**CG11)** The MM can be used to identify current level then used as a strategy model to reach the next level based on resources and risk appetite. Experience also tells me that organisations don't like to be bottom of the league therefore are encouraged to progress. (Yes)
(CG12) I think that would allow you to ask the right questions for your organisation. (Yes)

Additional comments

(1) My only comment is the subjectivity of incident management itself. Commercially, if contracts rested on a high level of maturity (as they may do in supply chain protection) then there may be a natural bias, probably at board level, so interpretation to play a part in the scoring. As mentioned above, the integrity of the scheme will always be difficult to ensure so if, from an implementation point of view, the scheme was used by external auditors (in the same way as ISO27001) to gauge maturity rather than internal to the organisation then this may produce better results. From a scheme point of view however, I think that limiting to the CSFs is perfect for both brevity and clarity. People can get quite bored with endless streams of questions especially if they are similar in appearance.
(**6**) Finally got round to this. My response is attached. Hope it can be read. My one main criticism of Maturity Models – and I used to use and like[redacted] IAMM which got fairly wide adoption but use has now tailed off – is that the output is too textual. Boards like data in simple to absorb forms. This means pictures. In [redacted] we used [redacted] BEATO tool. This was a stack of spreadsheets seamlessly integrated by some simple BASIC software which could absorb IAMM (and therefore your MM as well) but was mainly configured for ISO 27K stuff and assessed people/organisations using KPIs in much the same way your MM does. The difference is that the output was a chart/charts, immediately generated, that showed where the organisation was on its own and also compared to others (Department by Department). [xredactedx] only ever used it in [xredactedx] but I tried (and failed) to get [xredactedx] Services to use it. That's when I came across in depth inertia in many of the Boards who talk the talk but shy away from doing anything, mainly because of auditors anal devotion to the ISO 27K process (two year cycle). Hence getting auditors to provide instant outputs illustrating the Cyber/IA maturity is not just 'game changing' for a Board but can also make them more competitive as they can demonstrate their cyber security awareness at the top as a selling point (as opposed to ISO27K and similar reports that only happen every two years or so).
(17) One minor comment is that I find the "Times New Roman" font not the clearest font where used to on-screen documentation.
(20) Please let me know if this hard work of yours gains acceptance. I would be happy to use it to bench mark our 'as is' maturity and then use it further to improve the standards in an attempt to achieve 'optimised' in all CSFs
(26) I expected to be asked something about presence or absence of formal methods and systems for capturing, responding to and learning from incidents. For me that is also part of the maturity of the organisation. An immature organisation fails to capture, store and learn from this information, because there is no application or system. A mature organisation has a system which prompts for the necessary information at each stage and prompts the analysts for learnings, then makes the whole body of knowledge searchable and allows management reporting.

(36) Please see the visualisation I included in my email (Note respondent sent a colour coded version of the IRMM in his email to show it in another possible format)

(63) Mike **-** this is a great initiative but it will be apparent from my comments above that without a genuine commitment from the top of any organisation and evidence of impact on the culture and on behaviour at all levels, its impact will inevitably be limited.

(77) Your statements and scales look sensible and credible, and consistent with each other, so I ranked them equally rather than trying to tease out differences.

(79) I am an experienced user of maturity models in the IA sphere, and have contributed to ther content of a number of them. My responses are perhaps influenced by my enthusiasm for this sort of mechanism to establish clear benchmarks by which organisations can assess and decmonstrate their standing.

(86) A really useful approach; which I feel my organisation would definitely benefit from to improve its approach to security incident reporting.

(107) I personally believe that four Critical success factors identified in the study could be valuable for organizations.

(CG6) Mike, really good work IMO and I can see a real benefit for policing and partner organisations in adopting this. It strikes the right balance in effort and outcome and this has not always been the case in some Maturity Models (the IAMM being a prime example).

(CG7) A very useful exercise. Thank you.

(CG8) Very useful document Mike, will prove to be a real asset for measuring our own MM position.

(CG11) I think similar organisations could use the score information in a league table to assist in promoting their security profile and for partners to develop sharing protocols.

APPENDIX 17

List of Security Conferences where the incident reporting research was socialised.

Econique Information Security and Risk Management Conference November 2011

IAAC Symposium September 2012 Poster Session (This lead to request to present to National Audit Office by the Chair of NAO)

NISC (National Information Security Conference) May 2012,

SUAC (Sunningdale Accreditors Conference) September 2012,

SASIG October 2012,

SUAC (Sunningdale Accreditors Conference) October 2013

Nuclear Inspectorate Infosec Forum   January 2014

CISO Security Summit Singapore November 2014

Sofia East West Defence and Security Co-operation conference April 2015

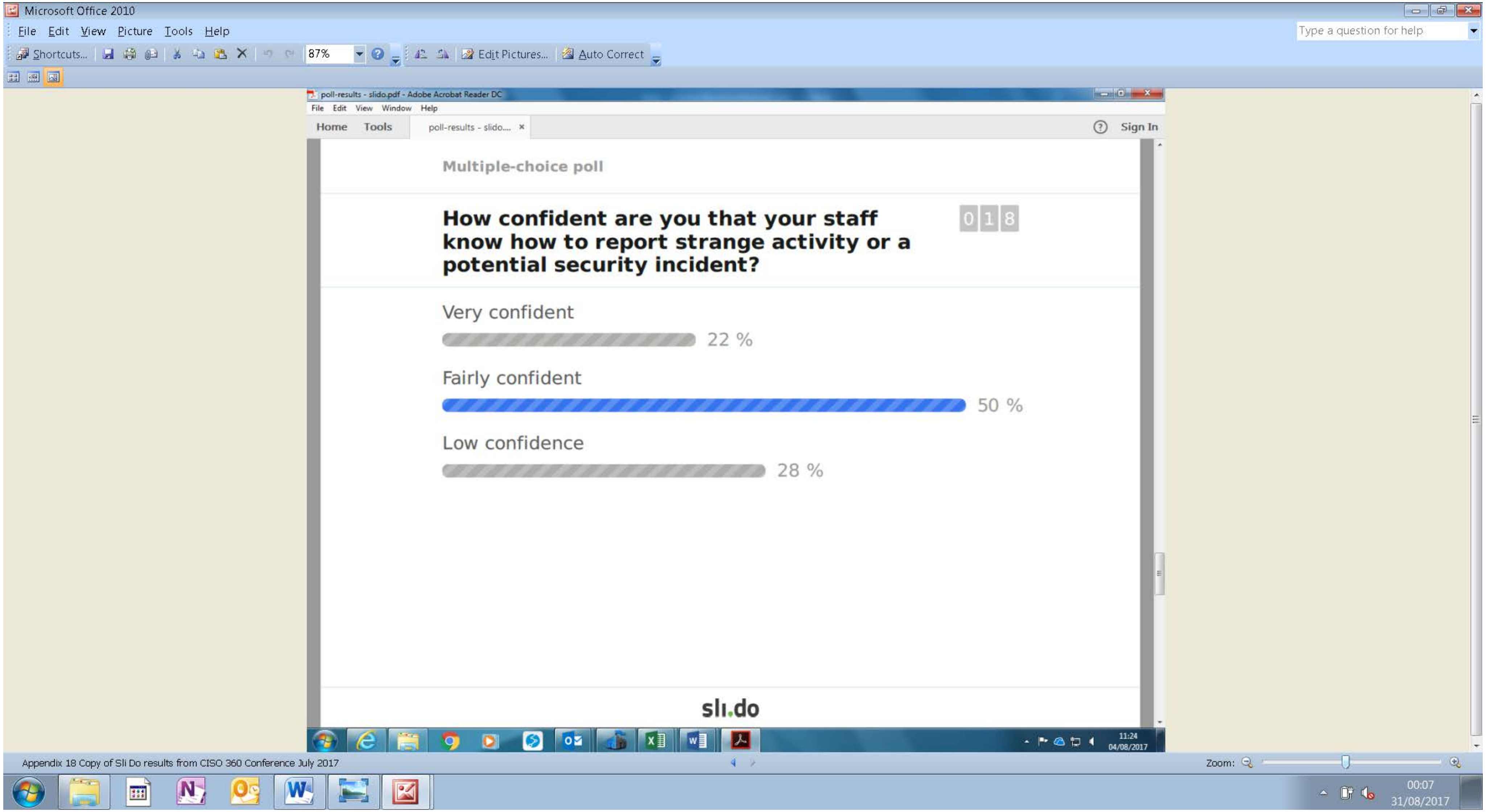
IISyG Quarterly Special Interest Group presentation House of Lords July 2016

IAAC Symposium - Poster - September 2016

Defence Academy Symposium – Poster November 2016

CISO 360 Barcelona July 2017

APPENDIX 18
On line poll of CISO’s at Barcelona CISO Conference July 2017



Multiple-choice poll

How confident are you that your staff know how to report strange activity or a potential security incident? 018

Very confident	22 %
Fairly confident	50 %
Low confidence	28 %

sli.do

Appendix 18 Copy of Sli Do results from CISO 360 Conference July 2017