HI-Risk: a Socio-Technical Method for the Identification and Monitoring of Healthcare Information Security Risks in the Information Society

Nicole Emerentiana van Deursen

A thesis submitted in partial fulfilment of the requirements of Edinburgh Napier University, for the award of Doctor of Philosophy

March 2014

Abstract

This thesis describes the development of the HI-risk method to assess socio-technical information security risks. The method is based on the concept that related organisations experience similar risks and could benefit from sharing knowledge in order to take effective security measures. The aim of the method is to predict future risks by combining knowledge of past information security incidents with forecasts made by experts. HI-risks articulates the view that information security risk analysis should include human, environmental, and societal factors, and that collaboration amongst disciplines, organisations and experts is essential to improve security risk intelligence in today's information society.

The HI-risk method provides the opportunity for participating organisations to register their incidents centrally. From this register, an analysis of the incident scenarios leads to the visualisation of the most frequent scenario trees. These scenarios are presented to experts in the field. The experts express their opinions about the expected frequency of occurrence for the future. Their expectation is based on their experience, their knowledge of existing countermeasures, and their insight into new potential threats. The combination of incident and expert knowledge forms a risk map. The map is the main deliverable of the HI-risk method, and organisations could use it to monitor their information security risks.

The HI-risk method was designed by following the rigorous process of design science research. The empirical methods used included qualitative and quantitative techniques, such as an analysis of historical security incident data from healthcare organisations, expert elicitation through a Delphi study, and a successful test of the risk forecast in a case organisation. The research focused on healthcare, but has potential to be further developed as a knowledge-based system or expert system, applicable to any industry. That system could be used as a tool for management to benchmark themselves against other organisations, to make security investment decisions, to learn from past incidents and to provide input for policy makers.

Acknowledgements

Many people have contributed to the completion of this thesis and I wish to express my appreciation to all of them.

The nature of the discussions between my supervisors and me over the years could not have been a better example of the different approaches to the social and the technical conceptions to information security and the need for a socio-technical foundation. Professor Alistair Duff, associated with the Centre for Social Informatics, guided me through the various stages of my research and encouraged me to study information security from unexpected angles in society. This study would not have been started nor finished without the support of Professor Bill Buchanan in the Centre for Distributed Computing, Networks and Security, pointing my attention to technological trends and future possibilities. The combined supervision from these different perceptions proved to be highly beneficial and inspirational to the creation of a socio-technical approach. I also wish to thank the panel chair Dr Phil Turner for his supportive supervision of the progress.

Finally, this research would not have been possible without the collaboration of the panel of experts, survey respondents and the people in the case study organisation, and I am grateful to all of them.

Table of contents

List of tables

List of figures

1 Introduction

1.1 Introduction

The research described in this thesis investigates information security in healthcare and proposes a new approach to assess information security risks. This chapter describes how the research topic was chosen and what the research aims to deliver. Furthermore, it is stated why the scope focused on healthcare specifically. The research process steps and how they relate to the arrangement of the text in the thesis are briefly outlined, as well as how engagement with other researchers and professionals contributed to the results.

1.2 Motivation

The researcher initiated the research project after working for several years as a consultant in information security for a diversity of commercial and non-profit organisations. From this experience, it was learned that in many cases, the number of information security incidents does not diminish after the implementation of detailed policies, consistent auditing, and certification of organisations against international security standards. The experience also learned that incidents tend to occur unexpectedly for an organisation and that organisations often are not adequately prepared to respond. However, many incident scenarios are not unique and also materialise in similar organisations. In a competitive market, businesses do not usually share security incident information, which may lead to situations where one keeps reinventing the figurative wheel and spending budgets on preventive and corrective measures of control that may not be effective. The motivation to start the research was grounded by this experience and it was the aim of the researcher to investigate the idea that organisations could benefit from sharing information security knowledge, especially about security incidents.

Several trends in the field support this line of thinking. During the course of the research, the European data breach notification regulation for electronic communication service providers was further strengthened with specific rules in 2013 (European Commission, 2013). These rules contain practical guidelines to ensure that in the event of a data breach, customers are informed, the authorities are notified and that the problem is solved at a pan-European level. Further calls have been made, for instance by the European Privacy Association, to expand this notification regulation to other sectors as well (Cleghorn, 2013), although, as pointed out by the World Law Group

(2013), the patchwork of laws around the world regarding data breach notifications is challenging. The notification of data breaches to the public and authorities could contribute to knowledge of how to organise the response to security incidents across an industry.

Another indicator of the interest in shared information security incident intelligence is a growing popularity in the use of risk and threat landscapes. Parallel to the research, several reports from respected organisations were published of this kind. These reports have in common that they try to map threats and risks on a scale that goes beyond one single organisation or region. One example is a technology focused threat landscape report from the European Network and Information Security Agency (ENISA) (ENISA, 2013) and the other is the Global Risk Report from the World Economic Forum (2012). Both reports have different scopes but they both support the thought that shared data about risks and incidents provides important knowledge to information security professionals.

ENISA published their threat landscape report early in 2013. This report is based on 120 reports from security industry and publicly available data and provides a view on observed technological threats, threat agents and threat trends. A threat landscape differs from a risk landscape. A risk embraces threats, vulnerabilities, likelihood and impact and is on a much higher level of abstraction. The global risk landscape from the World Economic Forum (2012) not only shows aggregated risks, but also shows how these risks relate to each other. One of the maps in the report shows a critical connection between technology risks and society and geopolitics. The forum considers cyber security as a key risk. It states that “cyber security is not a problem that any one organisation, private or public, can solve alone” (p. 46), which is a statement that has guided this research.

The underpinning philosophy of this thesis is that multi-sourced threat landscapes, when combined with assessments of other risk factors such as vulnerabilities and lessons from past incidents, have the potential to contribute to the reliability of risk landscapes and forecasting. Therefore, organisations should not keep information security incidents as their secrets. Sharing knowledge and lessons learned will improve everybody’s resilience to threats and this in turn is essential to contain global cyber unrest. This thesis aims to contribute to knowledge in this upcoming field of information security risk and threat intelligence.

1.3 Aim and objectives

At the outset of the research, the aim was the generic goal of exploring information security risks and to contribute to the knowledge of information security risks by producing a new method to analyse information security risks. The main aim of the research was to investigate the possibility of stepping away from traditional information security risk assessment approaches, which are aimed at individual organisations and systems, and to design a novel approach that would make a contribution to the knowledge of information security risks industry-wide. The approach should enable organisations to learn lessons from each other and to unite in the prevention of recurring information security breaches that could harm individuals.

The experimental approach of this research, the extensive literature review presented in chapters 2 and 3, and the engagement with experts and other researchers during the course of the research, led to further refinement of the general aim into specific objectives of the novel risk assessment method:

1. To gather and to evaluate information security incidents that occurred in multiple organisations and to discover the most frequently occurring scenarios. Knowledge about information security incidents must be included in the risk analysis because sharing lessons from the past contributes to the general knowledge of information security (Lips, Taylor & Bannister, 2005). Furthermore, sourcing risk information from multiple locations has shown an improvement in reliability or the forecast in other methods (Elevant, 2011). On top of that, it is assumed that systems and organisations do not exist in isolation. Assets and their social, physical, technical and human environment are entangled and pervasive and therefore the scope is unlimited (Rouse, 2008). Risks should therefore be reviewed in relation to the wider network.
2. To analyse the contribution of social, technical and environmental risk factors to information security incidents. The causes of risks and incidents are not limited to certain elements and are likely to occur in combination with each other (Crinson, 2008, PerAda, 2010).
3. To involve experts to identify and evaluate future risks and trends, as expert elicitation is a proven method for scenario building and forecasting (Padma et al., 2009; Rowe & Wright, 2001).
4. To express risks in a manner that can be used for policymaking and management decisions. The presentation of risks in scenarios proved capable of contributing to

the understanding of the risk by those involved in the risk assessment and therefore is preferred above the presentation in words only (Gürbüz et al., 2009; Lund, Solhaug & Stølen, 2011).

The novel method should be applicable to different industries, but for this thesis the focus was specifically on healthcare.

1.4 Scope

Healthcare was chosen as the main domain because it is a very diverse industry that comprises a wide range of processes and information. Healthcare is at the heart of the most innovative technological research and development and its security should protect the most private and vital information of all of us.

Information security in healthcare and in other industries concerns us all. We (as patients, as healthcare consumers, as family and friends of patients) need to have trust in the level of respect, protection and quality of care that our information receives from the people and organisations that we share it with. Our daily life is becoming inseparable from our digital selves when we pay electronically for medication, goods, and services, or when we communicate online or seek information. Our digital identity is a valuable asset that we would like to protect.

In healthcare and beyond, information security is also an economic issue: security incidents cost money. The 2013 information security breaches survey report, commissioned by the Department for Business Innovation & Skills (2013), estimates that small businesses suffer an average of £35,000 to £65,000 per incident, while in large organisations the average cost goes up to £850,000 per incident. According to this report, the median number of breaches suffered by large organisations in a year is 113, so the total costs could be millions of pounds each year. These numbers suggest that information security incidents are expensive and measures to prevent these incidents are worth the investment.

Information is critical for many processes within healthcare. Issues with confidentiality, integrity and availability of health information could affect us all, as it can lead to damage to health, life and trust in care. As perceived risks of confidentiality breaches increase, patients might avoid care (Myers et al., 2008). Patients could become concerned that a breach of confidentiality may lead to embarrassment, stigma or discrimination. A published example of this is the banker who also sat on a county health board in the U.S. and who gained access to patients' records. He identified several people with cancer and called in their mortgages (Patientprivacyrights, 2013). Furthermore, issues with the integrity and correctness of patient information could lead to medical errors. For instance, a study of the implementation of a computerised physician order entry system, discovered that users create workarounds when encountering usability problems with the system (Niazkhani et al., 2011). These workarounds influence the integrity of the data. The researchers observed that at the time a decision needed to be made, the user relied on memory about the patient to write out prescriptions and not on the data in the system, leading to an increased number of errors. Finally, patient information and healthcare information systems need to be available and accessible for healthcare staff to provide care. Healthcare infrastructure is considered as a critical infrastructure: an essential asset that needs to be available for the functioning of society. Baker, Waterman and Ivanov (2010) state that all over the world, critical infrastructures are under constant cyber attack. These attacks can cause disruptions in healthcare information systems. According to the conclusions of the American Medical Informatics Association’s health policy conference, these “disruptions in care and security challenges […] could result in the loss of public trust, a loss that may extend beyond the government to healthcare institutions and even providers” (McGowan, Cusack & Bloomrosen, 2012, p. 462).

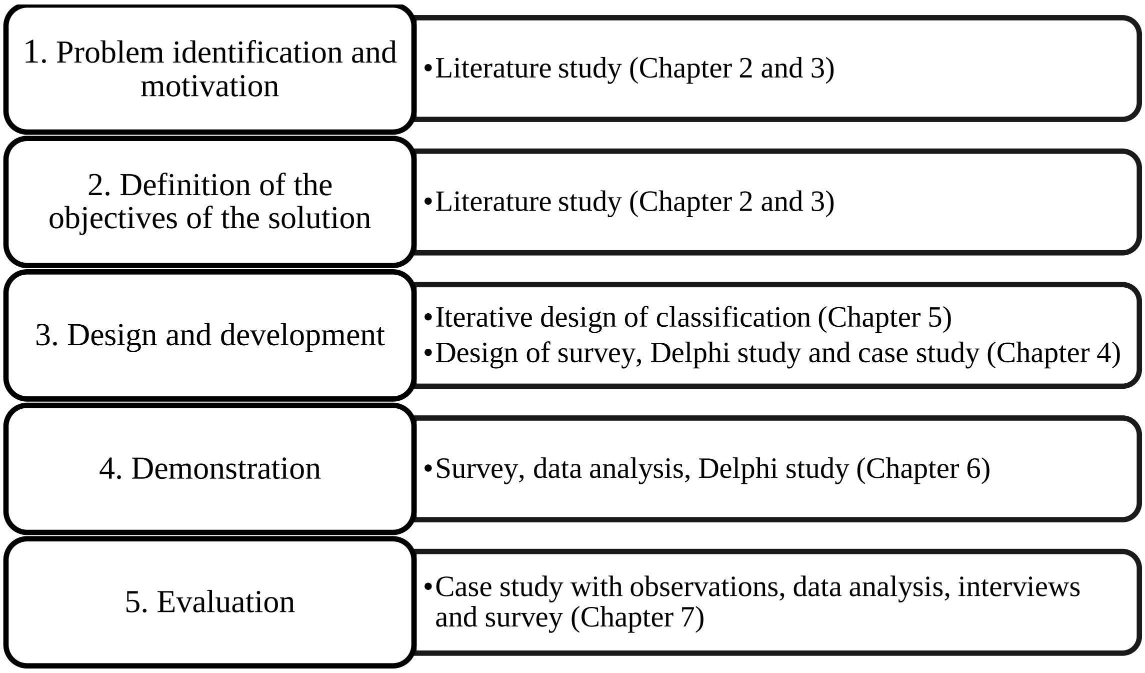
Correct and accessible information about a patient, in electronic or other forms, can save lives (NHS National Institute for Health research, 2013, Hillestad et al., 2005). Advances in technology have made it easier to provide and share medical and health information, but at the same time have raised questions in society about confidentiality, integrity and unauthorised access (Appari & Johnson, 2010, Meingast et al., 2006). Approaches to information security and information security risk analysis have so far not led to systems and processes that are free from security issues, resulting in on-going media and industry reports of security breaches.

Many methods to manage information security risks exist, but only a few have been developed specifically for healthcare. Furthermore, risk analysis methods for healthcare organisations have only sporadically been researched and are limited to “anecdotal evidence” (Appari & Johnson, 2010, p. 300). As will be argued in this thesis, these methods can be criticised for being time-consuming for participants and for not extending beyond the imaginary boundaries of a system, department or organisation. The relationship with contextual risk factors is often ignored, with some exceptions for legislation and compliance. These discrete-entity or contained-system methods provide little help in explaining or predicting the occurrence of security incidents. It has long been recognised that problems with information systems occur often because of social relations and dependencies with users, resource controllers and other actors who appear outside the boundaries of the entity (Kling, 1987). However, risk analysis methods have not evolved alongside that belief and seek individualistic explanations of risks, even for complex, connected and distributed information processing activities. Furthermore, these methods include neither the lessons learned from past incidents, nor future expectations of experts in the field.

The main deliverable of the research reported in this thesis is the Health Information (HI)-risk method to assess (identify and monitor) information security risks in healthcare. HI-risk provides insight into the most frequently occurring information security incidents and gives an indication of future trends in information security risks. This information contributes to the knowledge of individual organisations and policy makers on a regional level.

1.5 Research overview and thesis structure

The research process was organised following the process for Design Science Research (Peffers et al., 2008). The process contained 5 steps as illustrated in Figure 1-1. The design started with the identification and definition of the problem and the search for possible solutions. Issues with traditional perspectives on information security in general, and suggestions for wider socio-technical approaches of information security were researched by means of a literature study, which is presented in chapter 2. This chapter explains the different views on information security risks and controls. These differences cause confusion about what information security entails and why it continues to deliver unsatisfactory and partial solutions. It is argued that information security is a multi-disciplinary and socio-technical topic of study, characterised by the entanglement of people, organisations, information and communication technology (ICT), and the environment (e.g. physical environment, geographical environment, politics, and society).



1. Problem identification and motivation	•Literature study (Chapter 2 and 3)
2. Definition of the objectives of the solution	•Literature study (Chapter 2 and 3)
3. Design and development	•Iterative design of classification (Chapter 5) •Design of survey, Delphi study and case study (Chapter 4)
4. Demonstration	•Survey, data analysis, Delphi study (Chapter 6)
5. Evaluation	•Case study with observations, data analysis, interviews and survey (Chapter 7)

Figure 1-1 Research steps and reference to thesis chapters.

In addition, specific healthcare information security problems and directions for solutions were researched and reported in chapter 3. This research step studied the literature on healthcare information security governance, information security policy, risk assessment methods, and the risks associated with confidentiality, integrity and availability of information. It is shown that risk assessments are: often performed based on the traditional philosophy of contained systems; do not share knowledge across organisations within the same network; and are not fit for the modern complexity of healthcare. This causes a gap in knowledge about the actual information security risks in healthcare. Furthermore, it suggests that the foundations of risk controls, i.e. governance and policy, are suffering from inconsistency and from a low acceptance level.

The third research step, the design and development of the method, are presented in chapters 4 and 5. The design of the mixed methods approach to develop and implement the HI-risk method is specified in chapter 4. The methods included a survey, data analysis, a Delphi study and a case study with interviews and observations.

Chapter 5 presents the HI-risk method and demonstrates the strengths from existing methods on which it was developed. The method contains: an incident register; an analysis of scenarios; expert forecasting; and the final output is a risk map that shows the expected information security risks in healthcare.

The design of the *incident register* builds further upon existing security threat and vulnerability classification models. Existing models focus usually on a specific knowledge area or specific types of security problems. In the HI-risk method, classic computer security taxonomies from authors such as Parker (1998) or Howard and Longstaff (1998) are combined with a classification of human error categories (Liginlal et al., 2009), an overview of target patient information elements (Asaro et al., 1999), a typology of confidentiality breaches in healthcare (Brann & Mattson, 2004) and patient safety elements of organisational culture (Carthey & Clarke, 2010). This combined classification of socio-technical security risk and incident factors supports the structure of a database that holds an information security incident register.

From this data, calculating the co-occurrence of incident factors results in a list of the most frequent incident *scenarios*. These scenarios are presented to a panel of healthcare and security *experts*, and they state their opinion about possible future occurrence of these scenarios in a three-round Delphi study. They also add important insight into new risks that are likely to occur in the future. The knowledge from the incident scenarios is combined with the experts' insight into a forecast for the future. This forecast is presented on a *risk map.*

The fourth step in the research was the demonstration of the method. Chapter 6 presents the results of how the method was put to practice. During this phase, the proposed steps in the method were performed. Data about information security incidents in healthcare was collected from NHS Care Trusts or Health Boards in the United Kingdom by means of a Freedom of Information request. This approach delivered information about 2,108 incidents. The incidents were added to the combined incident register, and the expert panel reviewed the most likely scenarios during the Delphi study. This resulted in an information security risk forecast for healthcare.

The fifth step in the research was the evaluation of the method. In chapter 7 the results from a case study validate the reliability of the risk forecast. It is shown how the forecast on the risk map compared to the actual incidents that happened in a healthcare organisation.

The final chapter 8 discusses the results, the study's contribution to knowledge and suggestions for further research.

1.6 Engagement with the research community and produced papers

During the course of the research, there were several opportunities to present the research and to engage in relevant discussions about the research topic. These discussions provided valuable insights from scholars from different academic backgrounds and from different countries.

The first collaboration occurred within the faculty with a research project that focused on technological risk assessments within healthcare. The researchers took the opportunity to work as a team to design a survey to collect data about information security incidents in healthcare. This collaboration is described in more detail in section 4.4.2.2 of this thesis and resulted in a joint paper (Smith, Buchanan, Thuemmler, Bell & Hazelhoff Roelfzema, 2010)[1] on information governance and patient data protection.

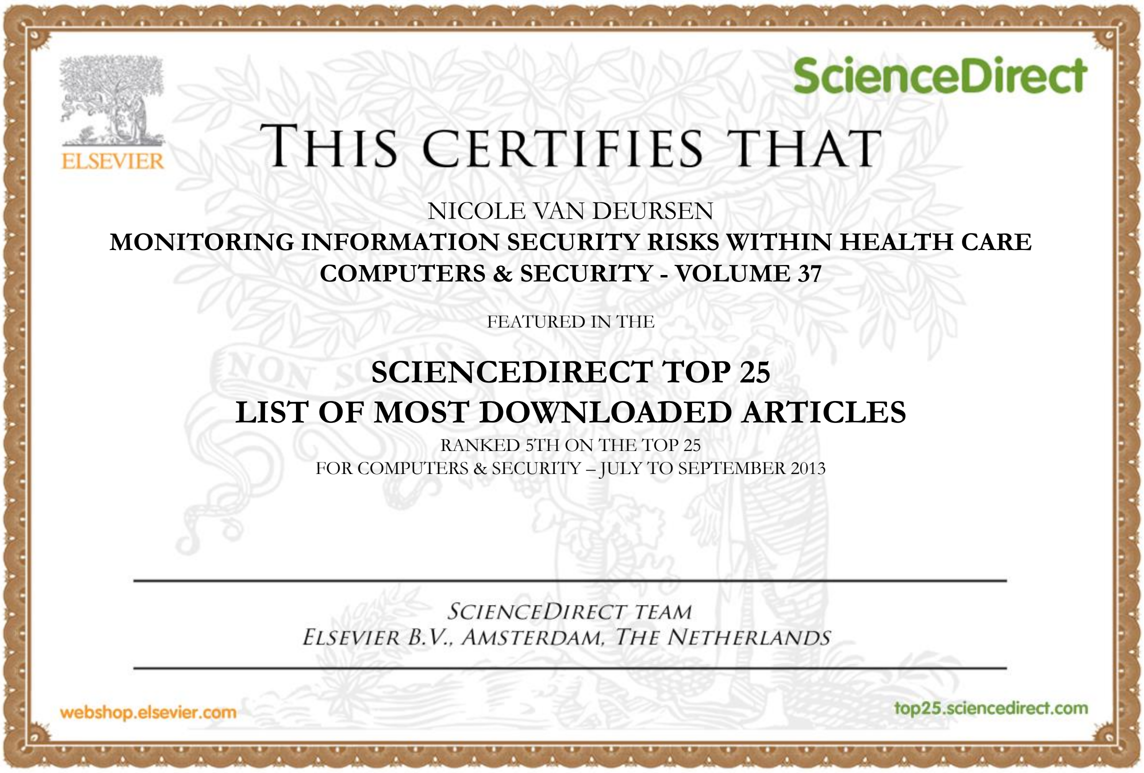
A second opportunity came through an invitation to participate in a workshop of the Pervasive Adaptation (PerAda) project, funded by the European Commission under the 7th Framework Programme for Research and Technological Development (FP7). PerAda is part of a project which aims to integrate, coordinate and increase the visibility of research carried out in the fields related to collective adaptive systems. The aim of the event was to determine key challenges in security, trust and privacy as they relate to pervasive adaptation. The presentation focused on the socio-technical information security risks and the human factors (PerAda, 2010). Feedback from other participants and information gathered from the presentations of other speakers proved inspirational for the comprehension of the magnitude of the scope of information security risks, which are omnipresent in today's society of pervasive systems. The workshop contributed to the understanding of the limitations of the performance of risk assessments within pre-defined scopes, as will be further discussed in section 3.6 of this thesis.

Indications of possible research directions to improve the reliability of information security risk forecasts were taken away from the E-society conference in 2011. At the time of the conference, the research into existing methods and their strengths and weaknesses had just finished, and a paper about this was presented at the conference (Hazelhoff Roelfzema, 2011). The aim of attending this conference was to gather requirements for the HI-risk method. In particular the research presented at the

[1] This paper was published using the researcher's married name Hazelhoff Roelfzema.

conference that was related to collaborative data gathering (crowd sourcing) of current events, in order to analyse trends and to predict the future direction of these trends, was used in the development of the HI-risk method. Details can be found in chapter 5 of this thesis.

Finally, a paper related to the research results was produced after the Delphi study (as detailed in chapter 6 of this thesis) (Van Deursen, Buchanan & Duff, 2013). This paper made it in the top 5 of Elsevier's most downloaded articles and was awarded with a certificate as shown in Figure 1-2.



ELSEVIER

ScienceDirect

THIS CERTIFIES THAT

NICOLE VAN DEURSEN

MONITORING INFORMATION SECURITY RISKS WITHIN HEALTH CARE

COMPUTERS & SECURITY - VOLUME 37

FEATURED IN THE

SCIENCEDIRECT TOP 25

LIST OF MOST DOWNLOADED ARTICLES

RANKED 5TH ON THE TOP 25

FOR COMPUTERS & SECURITY – JULY TO SEPTEMBER 2013

SCIENCEDIRECT TEAM

ELSEVIER B.V., AMSTERDAM, THE NETHERLANDS

webshop.elsevier.com

top25.sciencedirect.com

Figure 1-2 ScienceDirect certificate of most downloaded articles

1.7 Conclusion

This chapter introduced the research and provided some background into the project. The next chapter aims to clarify the concept of information security, and describes in more detail how information security is perceived differently by researchers and professionals from different backgrounds. Chapter 2 leads to a conceptual framework that defines information security in the light of this thesis. Thereafter, in chapter 3, the concept of information security will be related to healthcare and its specific issues.

2 Conceptions of information security in the information society

2.1 Introduction

This chapter is a background chapter to explain the concept of information security that underpins this thesis. It was deemed necessary to include this chapter because information security is a topic of study in different disciplines, which approach different aspects and work from different conceptions. However, as will be argued in this chapter, it requires multi-disciplinary collaboration to solve shared security problems. This chapter combines the different perspectives into the socio-technical theoretical framework that forms the foundation of the research. A more specific literature review on healthcare information security issues is presented in chapter 3.

2.2 Traditional conceptions

Information security became a common research topic at the end of the 1960s and early 1970s when the first publications relating to computer security and data security appeared. Before that, most papers were produced under government contract as reports, rather than conference papers, and therefore these were not widely disseminated among the general computing community (NIST, 2002). In the following decades, discussions about security spread outside the computing community to organisation and management disciplines, social and behavioural sciences, and sociologists. Nowadays, it is a central item in the public media, a topic of international relations and warfare, and it causes global anxiety amongst governments, organisations and the public alike.

Many regard the publication of the Rand Report R609-1 from the RAND Corporation as one of the seminal works in the early days of information security. The Task Force which wrote this report, under the authority of the U.S. office of Defense Research and Engineering, had the assignment to study and recommend hardware and software safeguards that would satisfactorily protect classified information in computer systems (Ware, 1970). The security philosophy in the report was based on closed environments: “cleared users working with classified information at physically protected consoles connected to the system by protected communication circuits”” (p. vi). The vision was that assets needed to be protected from uncontrolled access and information should not get out either. The aim of information security was to protect equipment from theft, damage or modification. The risks were mere technology risks, and controls aimed to protect the data in the systems. Furthermore, the report stated that security was best left to the experts:

> The security problem of specific computer systems must, at this point in time, be solved on a case-by-case basis, employing the best judgment of a team consisting of system programmers, technical hardware and communication specialists, and security experts (p. v).

In the 1980s and 1990s the innovations in communication technology changed the way that organisations were connected to each other and to their employees. E-commerce, remote working or outsourcing of services require a corporate ICT network to be accessible from outside of the logical boundaries of the organisation. Many publications about the role of people in the security of systems appeared from the 1980s onwards. However, Hitchings reported in 1995 that his survey amongst the top 1000 businesses and all local authorities in the UK found that although organisations were becoming more security conscious, there had been no advantages to the management of security techniques and the understanding of the role of human factors (Hitchings, 1995).

Many studies of human security behaviour followed from then. For instance, Straub and Welke used behavioural theories in their much-cited work about coping with security risks in systems (Straub & Welke, 1998). They found evidence that training and supporting reference material positively contributes to the awareness of managers and staff on how to properly protect and manage information assets. Awareness and behaviour of employees in organisations remains a popular research topic ever since.

When ICT systems started to connect to each other, information security practitioners promoted the opening up of the organisation’s computer networks in order to allow controlled and secured communication instead of keeping it closed and secured. In the U.S. General Accounting Office guidelines (1998), it is stated that:

> Security is increasingly being viewed as an enabler: a necessary step in mitigating the risks associated with new applications involving Internet use and broadened access to the organization’s computerized data. As a result, security is seen as an important component in improving business operations by creating opportunities to use information technology in ways that would not otherwise be feasible (p. 23).

Opening up connections between networks makes it difficult to maintain the traditional philosophy of containment. Dhillon and Backhouse (2001) argue that “maintaining a security perimeter around information processing activities” (p. 145) creates problems when organisational structures become more entangled with each other, as it is hard to define the boundaries of each organisation. However, classifications related to human behaviour and organisational culture persist in differentiating between insider behaviour and external attackers. It is frequently claimed that insiders are the biggest problems of information security (Baker, 2008, Baker et al., 2011, BERR, 2008, CSI, 2011, Verizon, 2012).

Recent developments in areas such as outsourcing of ICT services, mobile technology, cloud computing or management of large and complex data sets, have raised government and public discussions about boundaries, legislation, warfare, ethics and responsibilities. Information security is no longer an exclusive activity for computing experts. It has become a multi-disciplinary topic in which, as suggested by Von Solms (2010), the role of information security experts may change towards facilitating and educating governments and the public about risks and controls.

2.3 Socio-technical conceptions

Socio-technical studies receive growing attention within information security studies. In socio-technical approaches, it is believed that social constructs and technical infrastructure constantly respond to and shape each other. Socio-technical approaches envision that organisations should be designed as a balance between:

1. The technical subsystem: the technology to produce work -hardware, equipment, and technology- but also the techniques, methods, configurations, procedures and knowledge used by organisational members to acquire inputs, transform inputs into outputs and provide outputs or services to clients or customers.
2. The social subsystem: employees, knowledge, skills, attitudes, values and needs, reward systems and authority structures.
3. The environment: customers, suppliers, rules and regulations, which govern the relations of the organisation to society at large.

Adler and Docherty (1998) state that classical socio-technical systems approaches, focus on the stable internal aspects of the system with a lack of interest in the external environment. However, as Heller (1997) points out, the original studies from a socio-technical perspective focused predominantly on the micro level of systems, but the meso level (an industrial sector) and macro level (which could be a range of phenomena) were never disregarded. The socio-technical system was described as an open system with boundary roles that have to be sensitive to the external world. The environment should be an integrated part of sociotechnical studies. The social part of socio-technical is not limited to the managerial and organisational practices, but refers to the influences of technology and informatics on the entire economy and ways of life.

In a socio-technical system, the technical, social and environmental subsystems need to work in harmony. When changes are made to the social system (i.e. the reporting structure, cultural changes, etc.), the technical system is impacted through things such as information sharing or training. These changes may also affect the organisation's role in the community as well as the relations between customers and suppliers. Because technical changes are the most popular form of organisational improvement, their effect on the social system and the environment has been well observed. Communication and reporting structures in the social system can be changed dramatically by changes to the technical system. Socio-technical research is important to the management of information security as it acknowledges the importance of *social* and *human* factors in security management. The security of the technical system is created and challenged by the social system through users. The security of technical systems is also influenced by the environmental system through legislation and customer demands. When a security incident affects a technical system, the social and environmental system can be affected as well: staff will not be able to perform their tasks, the customers will not receive their service or the public will lose trust in a provider.

Orlikowski and Scott (2008) relate difficulties with the sociotechnical approach to technology in organisations to the assumption that humans and organisations are separate dimensions from technology. They argue that a new stream of research is coming to the fore to enhance the socio-technical approach, which they call relationality. In this view, humans/organisations and technology exist only through their intra-relating entanglement. They suggest that examples of this kind of research approaches are Actor Network Theory (ANT) and sociomateriality. ANT (Latour, 2005) is not a theory to explain why networks are formed as they are, but a method to explore the relations within heterogeneous networks, including the social as well as the technical. It maps relations that are simultaneously material (between things) and semiotic (between concepts). ANT assumes that many relations are both material and semiotic. Sociomateriality (Orlikowski, 2010; Orlikowski & Scott, 2008) challenges the assumption that technology, work, and organisations should be conceptualized separately, and advances the view that there is an inherent inseparability between the technical and the social. Leonardi (2012) defines sociomateriality as "the enactment of a particular set of activities that meld materiality with institutions, norms, discourses, and all other phenomena we typically define as *social*" (p. 43).

A few recent information security studies can be classified in this research stream. For instance, Hedström, Dhillon and Karlsson (2010) used ANT to analyse a computer hack in an organisation. They state that their findings reveal not only the usefulness of ANT in developing an understanding of the (in)security environment at the case study organisation, but also the ability of ANT to identify differences in interests among actors. They found that by using ANT, it was possible to see the heterogeneous network around a security breach, embodying human as well as non-human actors. Furthermore, it made it possible to identify the associations that link the different actors together forming the network.

Crinson (2008) advocates the sociomaterial understanding of information systems and points out that security risks are evolving and conditional, and that is where security analysts should engage. The focus should not be on separate technical and human factors, but on how the demands of working with information systems impact upon, and in turn are reconfigured themselves by, material practice within a particular organisation. He criticises the socio-technical approaches, as in his opinion, they remain focused on the insider-outsider duality. Furthermore, he argues that these studies tend to interpret the term socio-technical as the interaction of people with information systems security or the interaction between people and organisational policies. According to Crinson, by definition these approaches are falling short when analysing threats to security because they separate the human from the technology and exclude many external (macro-level) variables. Assessing threats to the security of information systems is not an evolving process based upon a rational process of risk assessment of a component's technical features and predicted human operator responses, rather it is a complex and highly unpredictable process that has to be alert to emerging practices.

Sociomaterial approaches are also criticised. Mutch (2013) doubts the value of certain aspects of the sociomaterial approach as opposed to more traditional approaches. He states that what is needed is a refreshment of existing knowledge of socio-technical systems rather than seeking new approaches. He refers to the formative work of Trist (1963) that shows sensitivity to broader social and cultural structures. This point has also been made by Heller (1997) who argues that socio-technical systems have always been seen as open system, existing within and interacting with its environment.

The new streams of research approaches are perhaps a response to the underdeveloped attention to the external systems of the socio-technical concept. The new relationality approaches try to fill in the gaps in knowledge that they see in socio-technical approaches. In that respect, the traditional and modern approaches complement each other and do not necessarily replace each other.

2.3.1 Conceptions of risks and controls in the technical subsystem

Developments in technical security mechanisms and artefacts ran parallel with the developments in computer and communication technology. These artefacts can be pieces of hardware or program code within a single machine, distributed systems or networked systems and the applications that run on them. Some examples include logical access systems, audit trails, encryption systems, antivirus software, firewalls, and intrusion detection systems. The innovative research and development of these artefacts is mainly the domain of mathematics, software engineering, computer science and management information systems.

Security practitioners recognise that the security of systems needs to be managed during the development stage of an artefact and that it needs maintenance after the implementation. Dhillon and Backhouse (2001) surveyed the methods for risk analysis and for selection of measures to control those risks that are used by security practitioners. They concluded that professionals use mainly checklists, risk analysis, and evaluations to design and maintain technical security controls. Checklists help to identify every possible control that may be implemented. Checklists are strongly related to audit, evaluation and standards. Many checklists were developed for analysts to check the system and to determine the necessity of existing controls and the possibility of implementing new ones. Risk analysis methods suggest that negative events can be prevented and information systems can be made secure if countermeasures are developed and implemented in a logical sequential manner. Evaluation methods aim to measure security against standards in order to give the system in scope a grading or a certificate.

Different international guidelines for information security management have been proposed, including the ISO/IEC 15408-1: Evaluation Criteria for Information Technology Security (2009), Control Objectives for Information and Related Technology (COBIT) 5 for Information Security (ISACA, 2012), ISO/IEC 21827: Systems Security Engineering Capability Maturity Model (2008), and the ISO/IEC 27000 series (2009), and its derivatives. They have in common that they aim to help organisations with their security certification processes. The implementation of these generic standards in organisations assumes that they are valid across multiple organisations and industries and pay little attention to the environment of the individual organisation. Such standards do not address the organisation’s own, and unique, information security needs, but prescribe universal or general procedures (Siponen & Willison, 2009). This creates the risk that information security is not applied in areas where it is needed. Furthermore, these standards and guidelines are based on the assumption that the implementation of technical security controls and procedures will fulfil the requirement of organisations to experience less security incidents. Some evidence supports this idea (Abdullah Al-Awadi, 2009), but it requires thorough monitoring, auditing and surveillance of the systems and its users.

Normative literature emphasises the importance of periodic reviews and audits of the security controls. Some researchers suggest that regular monitoring of information security controls can improve the overall effectiveness of an organisation’s information security policy (Ransbotham & Mitra, 2009; Steinbart et al., 2012). However, the effectiveness of audits has also been criticised for testing only the compliance to the organisation’s own security framework and for not testing the quality of the security itself. It has even been stated that “information security standards focus on the existence of processes, not on their content” (Siponen, 2006). Furthermore, it has been stated that periodic audits do not take into account the temporal dimension, focus heavily on system controls and do not include observation of users or comparison of results over time. Members of the organisation learn over time how to bypass technical controls (Colwill, 2009) and how to pass compliance assessments and adapt their organisational practices, causing gaps between the framework and the actual practices (Coles-Kemp, 2009), which in return will go unnoticed.

The technical approach to design and implement security controls traditionally considered that a system has strict boundaries. The conception was that if a subsystem is secure, it allows the rest of the system to be secure as well. However, recent publications demonstrate the on-going advances in security solutions, which focus on system-boundary crossing technology. Examples are solutions for computer and network abuse and misuse (Buchanan, 2011); for privacy issues caused by mobile technology (such as location tracking) (Buchanan, Kwecka, & Ekonomou, 2012); for the sharing of sensitive information between networks (Uthmani et al., 2010); or for the protection of data in cloud computing (Fan et al., 2011). These technological controls shape our view on security, and in turn these technologies are shaped by our political, cultural and philosophical standpoints (Coles-Kemp, 2009) and should not be researched and developed in isolation, but embedded in their wider social context. This has impact on the scope of risk analysis and on the applied methods.

2.3.2 Conceptions of risks and controls in the organisational and business subsystem

The organisational and business perspective on information security draws from management studies to describe economics, security management or governance (Anderson, 2001; Anderson & Moore, 2006; Coles-Kemp, 2008; Coles-Kemp, 2009; Collmann, 2001; Fitzgerald, 2012; Gerber & von Solms, 2005; Keller et al., 2005), and from human-behavioural studies to improve awareness and training (Herold, 2011; Khan, et al., 2011; Shaw et al., 2009; Straub & Welke, 1998).

From a business view, the information in the networks needs to be secured because this information and the related knowledge (or intellectual property) of the organisation have an economic value. Information security risks are seen as business risks, which can be measured, e.g. in terms of stock prices. Several studies found that information security has the power to affect company value (Campbell et al. 2003; Goel & Shawky, 2009; Khansa et al., 2012; Morse, Raval, & Wingender Jr., 2011).

Information security controls from the business perspective include the traditional personnel and administrative-procedural safeguards, as defined in the earlier mentioned RAND report, which nowadays are part of the Information Security Management System (ISMS) (ISO/IEC, 2009; Whitman & Mattord, 2010). The widely used BS ISO 27000:2009 (ISO/IEC, 2009) standard for information security describes how security should be managed through an ISMS. In terms of the standard, "management of information security is expressed through the formulation and use of information security policies, standards, procedures and guidelines, which are then applied throughout the organization by all individuals associated with the organization" (p. 8). Furthermore, central to the ISMS is the continuous organisational process (Plan, Do, Check, Act cycle). In this process, the organisation first establishes objectives and makes plans (sets targets). Then, the organisation sets to do what was planned. Subsequently, the achievements are measured and compared to the planned objectives. Finally, corrective and improving measures are taken to ensure better compliance with the plan. The ISO standard promotes a "*holistic management* of information security" (p.11), however, it does not explain what is meant by holistic, nor does it provide a definition of the term holistic management.

Coles-Kemp (2008) performed a range of case studies of these ISMSs across the public and healthcare sectors over a five-year lifespan. She identified that information security management literature generalized a number of “assumptions that did not always hold true” (p. 40). For instance, “it was assumed that an ISMS is structured top-down, both in terms of its organisational hierarchy and in terms of its policy structure” (p. 40). This top-down approach “is designed to manage structure, stable environments which can standardize the majority of their activities and fits with the ownership hierarchy that is typical of such an environment” (p.40). In reality, as Coles-Kemp found in her case studies, organisations are rarely stable and information security can be managed bottom-up as well. She found in her field studies that in Public Key Infrastructure (PKI), the root of the PKI hierarchy creates the certificate policy and has therefore control over the security and makes the information security management decisions. A second assumption in the literature is that strategic decisions are “only made at the top of an organisation” (p. 42). However, the study found that strategic direction is not necessarily introduced top-down, and that an organisation should accommodate strategic, operational and administrative security decisions at a variety of levels within an organisation. The third misconception is that any changes to the policy must be processed by the ISMS so that the changes can be calibrated and that the organisation remains secure. In the operational environment, as was observed in the research, it is not always possible to use a formal change control process. Furthermore, not all forms of ad hoc decision-making result in wrong security controls. The case studies demonstrated that in some instances ad hoc decision-making was a valid way of managing security. The findings of the case studies demonstrate that ISMS implementations suffer from simplified views of power, decision-making and control. Coles-Kemp concludes that the design of an ISMS can be unfocused and that the link between the external context (the organisation and society) and the internal context (the information security mechanism) is often overlooked and marginalized in favour of a focus on the information security mechanisms. The reality of emerging security practices based on ad hoc decision making calls for more research in order to provide a better understanding how humans and security management frameworks interact. The constantly emerging security controls suggest the adaptability and regulation of information security mechanisms.

2.3.3 Environmental subsystem risks and controls

In the socio-technical approach, the environmental subsystem is often related to legislation, government or customers. The requirements of these actors can influence the way the organisation operates and what it produces. Additionally, in information security approaches, there is some attention to the physical surroundings of an organisation. The environment can limit and shape the organisation's information processing. For example, the geographical location of an organisation defines the possibility of acts of nature influencing the ability to communicate and process information. This, in turn, defines requirements for the security of the built environment and for the security of the underlying technical infrastructure. Furthermore, the environment in terms of social-geographic and demographic figures, has the ability to influence the social and technical subsystems in terms of possibility of robbery, theft, burglary and so on.

Physical and environmental security is an element of information security, which is not often discussed in depth in information security studies. The scope of physical security is to protect the physical surroundings of information processing activities. This means the people; the building and its facilities; the hardware and communications; and the environment around the building. Physical security also extends to the employee's home. Working from home on the business network and mobile working create requirements for security controls at the remote location. The handbook of the National Institute of Standards and Technology (NIST), an agency of the U.S. Commerce Department, describes how physical controls aim to protect against interruptions in computer services, physical damage, theft, unauthorised disclosure of information and loss of control over systems (NIST, 1996). Methods to select controls to protect against these risks are often based on checklist or risk assessments. The international standard ISO/IEC 27001 suggests that physical controls include backup power supplies, fire controlling equipment, access control to the building, and clear desk policy. These controls are meant for a specific perimeter, and do not include the wider environmental and socio-geographical context. Some risks remain uncontrolled when following only this standard's suggestions.

The social environment is an element that is not often included in information security risk analysis methods. Local crime rates in the neighbourhood could influence the risk of staff being robbed of their information carrying devices (laptops, tablets, smartphones) at the car park or whilst walking to their transportation. Cozens, Saville and Hillier (2005) reviewed the core findings from place-based crime prevention research and found that a growing body of research supports the assertion that crime prevention through environmental design is effective. The architecture of the built environment and urban planning could have a direct relationship with crime and security and defines the security risk and the fear of crime in the community where an organisation is placed.

Moral laws and information ethics are becoming new areas of interest for information security researchers studying environmental controls. This is where academic fields such as psychology, philosophy and sociology could contribute to the understanding of the handling of secrets by persons and social groups and how people are affected by the loss of secrets (e.g. by loss of face, embarrassment, loss of trust, loss of membership of a group, stigma, loss of image and so on).

Thompson and Kaarst-Brown (2005) use examples of socio-cultural studies that studied the role of secrecy in different social groups and secret societies such as Native Americans and the Ku Klux Klan. These studies show that individuals within these societies feel that the information about the group must not be known to outsiders. Obtaining access to secrets is a sign of trust in the individual member and the information serves as social lubricant to maintain the cohesiveness of the unit and to signal identity in the group. The betrayal of the secrets is a major offence and could lead to termination of the membership. These type of studies have not been extensively researched in relation to information security, which could be a satisfactory line of inquiry for the future as it may provide insights into compliance to policy and perception of security.

Dourish and Anderson (2006) explored the social context of privacy and security. They argue that people have constantly changing information needs, which are subject to on-going revision and re-interpretation. Information management, in their view, is a way in which social actions are achieved. Therefore, any privacy and security requirement must be grounded in an understanding of the specific social and cultural context within which the activity is taking place. Furthermore, they propose that the concerns for risk, danger, trust, secrecy, identity, morality, and power are collectively giving meaning to information activities. They state that “security and privacy are ways in which people collectively understand the world” (p.338). They are social products rather than natural facts. In their approach, they do not seek to automate security in technological artefacts, but “to support the human and social practices through which the whole complex of phenomena –privacy, security, risk, danger, secrecy, trust, identity, morality, power, and so forth- are managed and sustained" (p. 338).

The environmental and social context of information security expands to governments and relates to topics such as information policy, diplomacy and international relations (Choucri, 2012; Choucri & Goldsmith, 2012; Gady & Austin, 2010; Mueller, Schmidt & Kuerbis, 2013). For example, the resilience of critical infrastructures is a matter of national security. President Obama stated that: "Organizations should cooperate more with each other and with governments, and even governments should work together internationally to secure information held in computer networks and to protect critical infrastructures" (Obama, 2011). However, international cooperation on this front is still in its infancy and is mainly military funded. Particularly in countries that have experienced significant downsizing of (conventional) military forces, cyberspace has attracted a considerable interest in the new opportunities for the military to play in what has become framed as "information warfare and information operations" (Eriksson & Giacomello, 2007, p. 178). In a way, this resembles the early days of information security when computing was mainly a military problem.

Examples of international collaboration are the NATO Cooperative Cyber Defence Centre of Excellence, an organisation that originated from military initiatives and aims to coordinate help after a major cyber attack, or Computer Emergency Response Teams (CERTs), who aim to handle incident response. The first CERT was developed by the U.S. Defence Advanced Research Project Agency in 1998 and now the system has expanded worldwide, with more than 250 organisations dealing with Internet security problems. Europe's Convention on Cybercrime is one of the more formal initiatives to foster international cooperation by harmonising criminal laws, and investigative and prosecutorial procedures around the world. Although it has not yet managed to have all member states sign the convention, it represents a cooperation that had not previously existed. The G8 sub-group on High-Tech Crime is another large-scale international network that maintains network of contacts for high tech crime and an international Critical Information Infrastructure Protection (CIIP) directory, but this initiative does not operate within clear legal frameworks, making it difficult to cooperate (Hathaway et al., 2012; Helms, Constanza & Johnson, 2012).

Global cooperation and Internet governance is problematic, yet vital for information security. According to Beck (2007), such cooperation "must be constructed" (p. 186), as he states that it will not automatically appear. However, the emerging international security discourse, conferences, research centres, and so on, may suggest a wide interest in cooperation, without the power struggles. Here lies a role for information security experts to act professionally, to support governments and to inform the public (von Solms, 2010). Beck calls this macro-ethics: “Social groups and firms coordinate their activities, offer competing assessments of risk and create new identities, laws and international organisations in economies, society and politics” (p. 15).

Van Dijk (2012) relates information security issues to politics and power, by discussing them in a book chapter with that name. He finds it remarkable that discussions about computer network vulnerabilities are reduced to aspects of technical security and the protection of confidentiality and privacy, as he states: “It is about the stability of the entire social system working with new ICTs” (p. 96). He argues that “the most fundamental values of society are at stake: social equality, democracy, freedom, safety, quantity and quality of social relations and the richness of the human mind” (p. 3-4).

Maybe, as a result of the slow pace at which governments are able to organise themselves in this area, or as a result of the need for knowledge or even fear, many initiatives arise from the industry, academia and public sector organisations. As many organisations struggle with the security of their data individually, although sometimes seeking help from branch organisations, institutions, consultants or international standards, the calls for more regional and national cooperation are getting more frequent, indicating that information security is an international issue in our modern society and should be researched, approached and governed as such.

Information security controls in the environment are also related to public policy on human interaction and the risks to privacy, freedom of speech, equality, fairness, dignity and other human rights. Braman (2011) sees information policy as the strategic solution to frame and understand the effects of the laws and regulations involving information. Furthermore, according to Orna (2008), information policy also provides the essential context for organisational information policies, which cannot be understood without it.

Questions have been asked on how society will control these issues. On a national level, steering and policy are lacking (Choucri & Goldsmith, 2012; Duff, 2012), and the law is unclear on how to handle cyber crime (Hathaway et al., 2012; Helms et al., 2012). Furthermore, discussions about information ownership and liability for fraud and confidentiality breaches are only just beginning.

Duff (2012) even argues that information policy could possibly play an important role to protect democracy and equality by ensuring equal access to information. According to Duff, the state has been allowing a free market in information, which has implications for society and the democratic rights of individuals to access information. He proposes the implementation of certain political and moral principles to ensure a just state that prevents inequality within society (a disparity between information-rich and information-poor) and to ensure an equal access to and a justified storage of personal data. The state should represent the moral convictions of people about how they wish to have their selves and their digital selves treated.

In contrast, Castells (2011) expresses his opinion against Internet policy (p.115) and his disappointment in networks regarding the topic of global Internet governance. He observes that governments are trying to regulate control over the Internet and to enforce that control through traditional categories of law and order. Castells argues that controls over the Internet are not likely to be effective when they are not directed towards specific corporations or organisations. He argues that the liberalisation and deregulation of Internet is based on capitalism and state control, and has led to the formation of global multimedia business networks where "business interest prevails over state interest" (p.116).

Governments have to play a crucial role. Information policy is an important component in the deliberations of national governments and international public bodies, yet it is much less immediately visible than other areas of public policy (Rowlands, Eisenschitz, & Bawden, 2002). At its highest level, information policy comprises all the laws, regulations and public policies that encourage, discourage or regulate the creation, use, storage and communication of information. Historically, information policies have evolved in direct response to the emergence of specific technologies, such as print, telephony, radio or value added and data services. For example, as was observed by Porat (1977), privacy policy is often "reduced to decisions regarding control of and access to information technologies" (p. 211). To improve this, he states that neither the policy (or ideological) perspective nor the technology perspective alone can solve privacy problems, but that the two must work together.

Related to information security, the process of international cyber security diplomacy proves to be delicate. States with a major influence on international relations such as the U.S., Russia, China and the European Union, considered in this connection as a 'super state', accuse each other of hacking, attacking and spying on citizens. The Internet, which has traditionally been governed from a market principle and self-regulation, has become the centre of international power struggles. The protection of critical infrastructures depends now on global policy versus self-regulation and global hierarchy versus collaboration. The traditional laissez-faire principle now leads to discussions about state control, responsibility and information policy.

Perhaps in the future, our society and politics can evolve towards or can construct a “global solidarity” (Beck, 2007) to protect information. A unified and adaptive global ‘management’ of states, formed by a coalition of different groups from society and businesses provides an opportunity for information security experts to gain influence and to become part of a secure digital future. If our globalizing society can manage to keep trust in its people and institutions, by changing the social, moral, reputational, and institutional pressures as well as the security systems, then, in the future, governance and compliance may be substituted by ‘trustworthiness’ and security by ‘trust’ (Schneier, 2012).

Information policy discussions are thriving at the time of writing of this thesis. The media are currently covering the alleged worldwide spying of the U.S. government on citizens through the Planning Tool for Resource Integration, Synchronization, and Management (PRISM). It is currently the centre of an international diplomatic row, and time will tell if this issue has the potential to stimulate a new wave of security discourse, information policy and citizen empowerment.

2.4 Information society

To the best of the researcher’s knowledge, the literature on information security has not made an explicit step towards an information security risk analysis outside of the technical, business, and legal context. It was therefore necessary to explore information society literature, to make sense of information security risks associated with the environmental subsystem. These large-scale theories help to better understand the relationship between technology and social changes. The goal of the following exploration is not to engage in the discussion about whether or not we live in an information society (or whether this term is the correct expression to describe modern ways of life), nor is it pursued to provide an extensive literature review of all the great society thinkers from the last century. The aim of the next sections is to point out some sociological discussions, often indexed under the term information society, which can contribute to the understanding of the social risks of weaknesses in information security, as a contribution to where the traditional views run short. Three schools of thought were considered important sources to relate information security to society: Ulrich Beck's work on the Risk Society, Manuel Castells' analyses of Network Society, and sociological views on Surveillance.

2.4.1 Risk society

In the late 1980s, it was thought that the safety of the information society was at stake. Society became fragile because it was at the mercy of technology. Questions were asked about preserving the accumulated knowledge of mankind and protecting against the risks coming from mankind itself. The German sociologist Ulrich Beck (1992, 2002a, 2002b, 2006, 2007) was searching for answers to these problems. Beck recognised a paradox in modern society. He stated that risks may be increasing due to technology, science and industrialism rather than fading away as a result of scientific and technological progress. Our society is a world risk society, created by modernity. Although Beck's work is not explicitly about information security, he provided thoughts on risks and how new risks were forming in society which can contribute to the discussions about information security in society.

Beck saw risk as the new form of wealth. Modern society in his eyes did not focus any more on the creation and distribution of wealth, but on the creation, distribution and mitigation of risk. Where the industrial society was structured around economic inequality and wealth, the risk society is structured around risk. In Beck's vision, risk affects all members of society, but only the rich are able to buy their way out of risk, by fleeing from affected areas, buying more expensive, safer foods, and safeguarding their interests against risk.

The United Nations (2013) reported that 80% of cybercrime acts originate in organised and specialised activity, and the organisation of cybercrime reflects patterns of criminal groups in the conventional world. Risks are buyable; an attacker who has gained access to a company network may decide to sell the access credentials to another attacker who has a specific interest in this organisation. As suggested by KPMG (2012), there exists an underground economy that contains 'hackers for hire', which offer their specific knowledge to any party that requires it for an advanced attack. In this online underground economy passwords and (software) tools are traded. Furthermore, knowledge of risks can be seen as a resource that is being traded in, exchanged, moved, used and abused in our economy and politics. The threats of organised cybercriminal groups and organised ideologically/politically motivated cyber groups that aim to incite hatred, violence, and intimidation through the Internet present a real risk to the economic and social stability of society.

Risk affects social structures in several ways. Beck uses the example that risk goes over borders (global warming does not respect national boundaries) and can affect remote parts of the world, just as sheep in Wales were contaminated by radiation from Chernobyl. From this view, it is possible to draw a parallel to the entanglement of computer systems with society. For instance, when a computer virus in an email system starts spreading itself to all the contacts stored in that system, other computers in distant geographical locations can be affected, and can be disrupted as well. This becomes especially important when considering the risks associated with critical infrastructures. Much information security literature explores the security of critical infrastructures such as communication (Ericsson, 2010), water (Sterbenz et al., 2010) and electricity supplies (Farrell, Zerriffi, & Dowlatabadi, 2004). The infrastructures are vulnerable because they are highly dependent on networked information systems. On top of that they are interdependent; should one infrastructure fail because of an accident, a natural event, or an intentional act, it could bring down other infrastructures as well. The impact of such events on national and economic security and the potential effect on global economic areas such as banking and finance, oil production, road and air transportation is far reaching (Rinaldi, Peerenboom, & Kelly, 2001). Risk society thinking can help to understand the way information security risks affect more than just the system component that is under review or under attack.

In Beck’s perspective, positions in society are influenced by the means and possibilities to avoid risks, to cope with risks and to create risks. According to Anderson (2003) information security experts could potentially gain a lot of power as state security advisors as well as in criminal organisations when they have the knowledge to use risks as a weapon. For example, the Stuxnet worm has infected at least 50,000 computers, mostly in Iran, India, Indonesia, and Pakistan. It has shown up in an Iranian nuclear plant in Bushehr and a uranium enrichment facility in Natanz, which got some experts speculating that the worm was built specifically to sabotage the Iranian nuclear industry. It was noted by Chen and Ubu-Nimeh (2011) that the sophistication of the malware and the insider knowledge of the systems affected lead to agreements amongst all reports examining Stuxnet on the likelihood of at least one government’s involvement in its development.

Technological developments have made it possible for people to perform actions without being able to understand the consequences. The meltdown and explosion of the Chernobyl nuclear generating facility, for example, had consequences far beyond any emergency scenarios imagined by the engineers who designed and built the plant, having an impact upon not just local citizens but on entire populations across national borders and inter-generationally, with the incalculable cost of deformities and birth defects. Stuxnet affected many other networks in different countries than the intended targets. Information security incidents have the potential to accidentally affect many different assets and actors in the world.

Beck observes a paradox of deepening scientific progress on the one hand, but greater risk on the other. Advances in science and technology simultaneously increase the technical controls over certain hazards while, at the same time, these same advances can lead to the emergence of global and far-reaching risks. The loss of control over these risks in terms of their social management potentially poses the greatest social harm and could threaten our very social order.

2.4.2 Network society

Castells' trilogy *The Information Age* (1996, 1997, 1998) presents his observations and analysis of the society that we live in. Castells points out, without claiming to be exhaustive in his description, that one of the key features of society is the "networking logic of its basic structure" (1996, p.21). He defines a network as a set of interconnected nodes. These nodes can be anything: a stock exchange market; a state; a mobile phone; or a location. The distance (or intensity and frequency of interaction) between two points (or social positions) is shorter (or more frequent, or more intense) if both points are nodes in a network than if they do not belong to the same network. Important nodes absorb more relevant information and process it more efficiently. Distance (physical, social, economic, political, cultural) for a given point or position varies between zero (for any node in the same network) and infinite (for any point external to the network). This means that networks could be connected on a planetary scale. The boundaries between networks are constantly changing and these changes influence social practices and organisations; they could even redefine society. Social networks have always existed in society, but what Castells sees as revolutionary for modern times, is the technology. This technology enables digital communication networks and thus organises society to reap the benefits of new technology.

When exploring information security in society from Castells' point of view, there are some features of the network society that are particularly relevant. Amongst these are the changing identity of individuals, the flexibility of employment, the power within networks, and globalization.

In the network society, networks cooperate or compete with each other (Castells, 2000). Castells states that networks are:

> appropriate instruments for a capitalist economy based on innovation, globalization, and decentralized concentration; for work, workers, and firms based on flexibility and adaptability; for a culture of endless deconstruction and reconstruction; for a polity geared toward the instant processing of new values and public moods; and for a social organization aiming at the supersession of space and the annihilation of time (p. 502).

Cooperation between networks is based on the ability to communicate between them. This ability depends on the existence of codes of translations and inter-operability between the networks and on access to connecting points (switches). "Switches connecting the networks (for example, financial flows taking control of media empires that influence political processes) are the privileged instruments of power" (p. 502). Competition depends on the ability to outperform or disrupt competing networks. Competition may also take destructive forms by disrupting the switchers of competing networks and by interfering with communication protocols. The inclusion or exclusion in networks configures the dominant processes and functions in our societies. In the vision of Castells, the power lies with those who decide the rules for inclusion and exclusion. He states that the convergence of information technologies has created a new material basis for these processes and "this material basis […] shapes social structure itself" (p. 502).

Because organisations are networked with other organisations, they can create productivity growth through technology and transformation of labour. Outsourcing of services leads to changes in employment. Employees are flexible, change jobs more often and become mobile. Castells suggests that, even where the corporation is a transnational giant, hierarchies are being pulled down, and power is shifting to those information workers who operate on the networks, fixing deals here and there, working on a project that finds a market niche, owing more commitment to people like themselves than to the particular company which happens to employ them for the time being. Flexible workers and working conditions are created through outsourcing and subcontracting, facilitated by technology.

This observation has implications for information security. Flexible working and job-hopping employees could impose a risk to the security of the valuable assets of an organisation. The diminishing of the segregation of work and private life caused by the use of electronic devices, could easily lead to the storage of company information on personal devices. These devices are taken to the home, into the social life and to the next employer. Furthermore, investments in security controls such as training of employees in security procedures and awareness are expensive and could be perceived by management as a waste of funds if the staff is likely to change employment soon. Controlling information security within the organisations of outsourcing partners, located in different geographical environments, in different cultures and operating under different laws is a challenging task.

Castells observes that organisations operate in networks and their systems and networks tend to integrate. KPMG (2012) identifies an example of a typical information security risk in these integrated networks in the form of a chained attack. These are attacks performed by cyber criminals when they attack an organisation in order to gain access to another organisation via a trust relationship. Organisations that are attacked may not be the end target; they are used as a stepping-stone to get to the end goal. Furthermore, after or even during a security breach, the speed at which the news travels (through Internet, mobile phones or mass media) can quickly damage the reputation of an organisation or government and could even lead to quick mobilisation of groups of people, hacktivists or hobbyists to even further damage the information technology networks.

The Internet has facilitated richer and faster communication throughout the globe. Citizens, organisations and governments are getting more and more connected. This communication is not secure, nor private, unless specific controls are used. Meanwhile, the knowledge and technology to intercept, access, read, steal, monitor or delete information from computer networks is becoming available to an increasing number of people, empowering them to perform attacks on computer networks (and thus on the social structures that they represent). Internet based systems are leading to information security concerns on a larger scale than ever before. According to Internet World Stats, in June 2012, more than one third of the world population is using the Internet. The Internet has been described as the "lifeblood of modern economy" (Quigley & Roy, 2012). New Internet-related technologies will continue to emerge and trigger new technology-based security problems and solutions. In Castells' vision, the Internet is a tool of management of new forms of life.

The role and influence of the mass media is changing as well, influencing political opinions and behaviour. Castells mentions that social groups could turn to Internet-based mobilisation or to aggression such as hacktivism, crime and fraud. On a macro level, this potentially affects corporations and multinationals, governments and regions. Social groups can use Internet-based social media even to enable a revolution. One example is the eighteen day long revolution in Egypt in January 2011. Castells (2012) analyses that the social media not only provided a communication infrastructure, but also had given the public a feeling of being together, enabling them to overcome their fears. On top of that, Internet companies and private television channels and global satellite channels disconnected themselves from the media networks owned by the state. Therefore, the party lost access to media and lost their power to influence people through the media.

2.4.3 Surveillance

The year 2001 led to many discussions that explicitly demonstrated the integration of micro level security issues and macro level thinking about society. After the terrorist attack on U.S. targets on 11 September 2001, the discussions about the relation between surveillance, security and privacy increased. Surveillance studies and information security are closely related. Surveillance can be interpreted as physical watching, but much policing and intelligence surveillance is digitised. Lyon (2007) states that surveillance is the "focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction" (p. 14). Furthermore, he writes that surveillance is accepted by most people when its purposes are clear and linked with safety and security or when allowed by the person's own choice (such as in social networks). It becomes less comfortable when personal data that was collected for a specific purpose (e.g. to register for a specific service or product), is used for a different purpose (to sell or to deny other products services).

Lyon and Wood (2012) relate security and surveillance in a way where surveillance is a means, a method or practice and security is the goal or intended outcome. This may be true when the focus is on national security, but the relationship between information security and surveillance is more complex than that. Sometimes surveillance is the method, but from an information security perspective, it can also be the goal.

Furthermore, the two overlap, sometimes as similarities, sometimes as contradictory forces.

A direct relationship of surveillance studies with the field of information security is found in the concept of identity management. Identity management entails the settings and strategies for access to data, systems, Internet sites or certain services, and these strategies overlap with physical border controls, with biometric passports and other means of identification and verification.

Biometrics refers to technologies for measuring and analysing human body characteristics such as fingerprints, voice patterns, facial patterns or eye retinas and irises, used to create a certainty about a person's identity. Jain et al. (2006) state that this technology can lead to cultural, societal or religious resistance. Furthermore, as argued by Holvast (2009), it can mean an attack on one's privacy when the collection takes place without consent and without transparency about the purpose for which the data is used.

Identity management in the information security field focuses on solutions to provide access to systems and data to only those individuals who are authorized to do so. Digital and biometric identity details can be tracked and used for selective disclosure of information and services. There are some concerns about possible use of identities for (price) discrimination of consumers and for social sorting. When many corporations simultaneously rely on such methods it reinforces social and economic inequalities (Lyon, 2007). Information security research into solutions for privacy-enhancing technologies focuses on hiding personal data during transactions, but these solutions are not always sufficient (Acquisiti, 2008). Another concern is that the theft of one's digital identity can lead to fraud and abuse of the identity to buy products or services or even to commit crimes. The inconvenience and economic loss suffered by victims often happens without the victim's knowledge and can take several years to straighten out.

From the perspective of an employer there is a need to monitor and control the security of important business data. Traditional information security threats of malicious software such as spyware, keystroke loggers, backdoors and viruses are surveillance tools as they can be used to monitor a user's activities and to access data stored on a computer. On the other hand, these surveillance tools can also be used as an implementation of information security to monitor employees. Measures such as firewalls, network traffic monitoring, audit trails, logging of user activity, logging of email and Internet activities are surveillance options that are embedded in most computer networks to prevent security incidents, to control user behaviour, and to benefit forensic investigations in case an incident occurs. Within organisations these are increasingly accepted forms of surveillance, although usually no consent is sought from the employees under surveillance (Lyon, 2007). This privacy-invasive software is a potential threat to the individual's right to be left alone, and does not always stand in court as evidence in the case of employee-employer disputes.

Another issue can be found in the physical security of the workplace. Information security measures in the physical environment are often implemented to perform surveillance of people accessing the premises (through CCTV or key logs on doors), but in turn these surveillance measures can lead to information security issues. An example is when a camera is pointed at a keypad or computer screen and as such able to oversee passwords and access codes. As a result, surveillance and information security can be opposing forces.

The Internet provides for numerous forms of surveillance. The individual consumer does not always have the means to oversee the implications of their online actions. This is illustrated by the personal data that is shared willingly in social networking sites. Marketing companies create maps of social networks based on the data from these sites. Trottier (2012) states that these maps are then analysed to extract useful information such as personal interests, friendships and affiliations, wants, beliefs, thoughts, and activities. With these maps, social media become both a resource for and a target of police surveillance, intelligence services, and corporations.

Some argue that the responsibility for the security of the personal data involved should lie with the providers of mobile, Internet and email services. From an information security perspective, these providers have to ensure that they protect this kind of personal data against unauthorized disclosure, damage and loss. On the other hand, they have to disclose it when the state or police requests it, and it is not always clear to the individuals involved which of their data is being requested or shared.

The on-going development in the storage of enormous amounts of personal data and the possibilities of data analysis, feed discussions on how to create appropriate protection within the technology as well as discussions on a higher level in the organisation's boardroom on how to protect privacy and avoid discrimination (Custers, Calders, Schermer, & Zarsky, 2013). Big Data is a problem as well as an opportunity for those conducting surveillance. According to Lyon (2012), it is making surveillance less “about direct human relationships or even about human-organisation relationships but as one of a number of ways in which social relationships are increasingly mediated by software codes” (p 321).

In this area, surveillance studies and information security share a problem. Privacy and data protection laws are inputs for information security to set boundaries for data access and sharing, and they are a counterweight to excessive surveillance. But these laws are often difficult to interpret in concrete measures, they differ in regions and compliance is difficult to audit. Data protection principles need to be applicable to a wide range of contexts and data sets, however the finer details are not defined. This leads to different interpretations and difficulties implementing the policy and principles into practice (Hoffman & Podgurski, 2007; Myers, Frieden, Bherwani, & Henning, 2008). As Lyon (2007) puts it:

> Globally, there should be agreements on the appropriate handling of personal data, not just to ensure higher levels of security or to increase the speed of commercial transactions, but because the issues are intrinsically important. These are not mere ‘business risks’ […], but matters of democratic practice, social justice and moral obligation. Personal data pertain to human beings whose life-chances and choices are affected for good or ill (p. 176).

2.5 Conceptual synthesis of the perspectives on information security

The previous sections showed that traditional information security risk perceptions are limited in explaining risks that affect more than one organisation and its business, ICTs and staff. It was argued that the global entanglement of people, ICTs, organisations with cultural norms and ethics calls for risk approaches that are wider than technology or business risks. An information security risk is not ‘a thing’ that can be singled out and contained. It is partly related to perception of dangers and annoyances and norms and values.

The concepts discussed in this chapter are brought together in the conceptual framework of the views of information security in Figure 2-1. The box in the centre of the figure illustrates the traditional technical line of security thinking, as discussed in sections 2.2 and 2.3.1 of this thesis. The box shows that technical information security is the domain of computer science, mathematics and electronic engineering. In this view, information security risks are technology risks that threaten systems. These risks can be contained through the installation of artefacts and mechanisms and through the use of standards and checklists.

Around the centre, the growing insight from business, sociological, political and human theories complement the technical scope. These different streams strengthen and inspire the field. Information security thinking has expanded from the concept of containment to socio-technical complexity. This does not mean that one could replace another: the different perceptions are complementary to each other and all of them are needed to understand contemporary information security. Information security risks include the whole of technology risks, business risks and society risks. A technology risk (such as the risks that a critical infrastructure stops working because of a technical issue) could cause a business risk (when organisations relying on the infrastructure cannot complete their production). In turn these risks could cause risks to people and groups in society. To illustrate the disappearing boundaries around environments and systems, the box around the technical area has dashed lines and the text on the outside is not framed at all, as a symbol of the pervasiveness of information security issues.

The outside area of Figure 2-1 is related to risks in society. As discussed in Section 2.4, these can be identified and better understood by studying information society discourse. From studying the works of information society thinkers such as Beck, Castells, van Dijk, and Lyon, it was identified that the scope of information security risks is global and infinite, through the connections in socio-technical networks. Furthermore, the risks can be economic (influencing stock markets), personal (identity theft, social inequalities, damaged social relations), political (bringing down governments, or damaging international relations), and have the potential to influence basic human rights (the right to be left alone, freedom of speech). Following information society theory, the conclusion is that the perception of societal information security risks is likely to be socially constructed by international power -and power struggles-, (lack of) public information policy, mass media and culture.

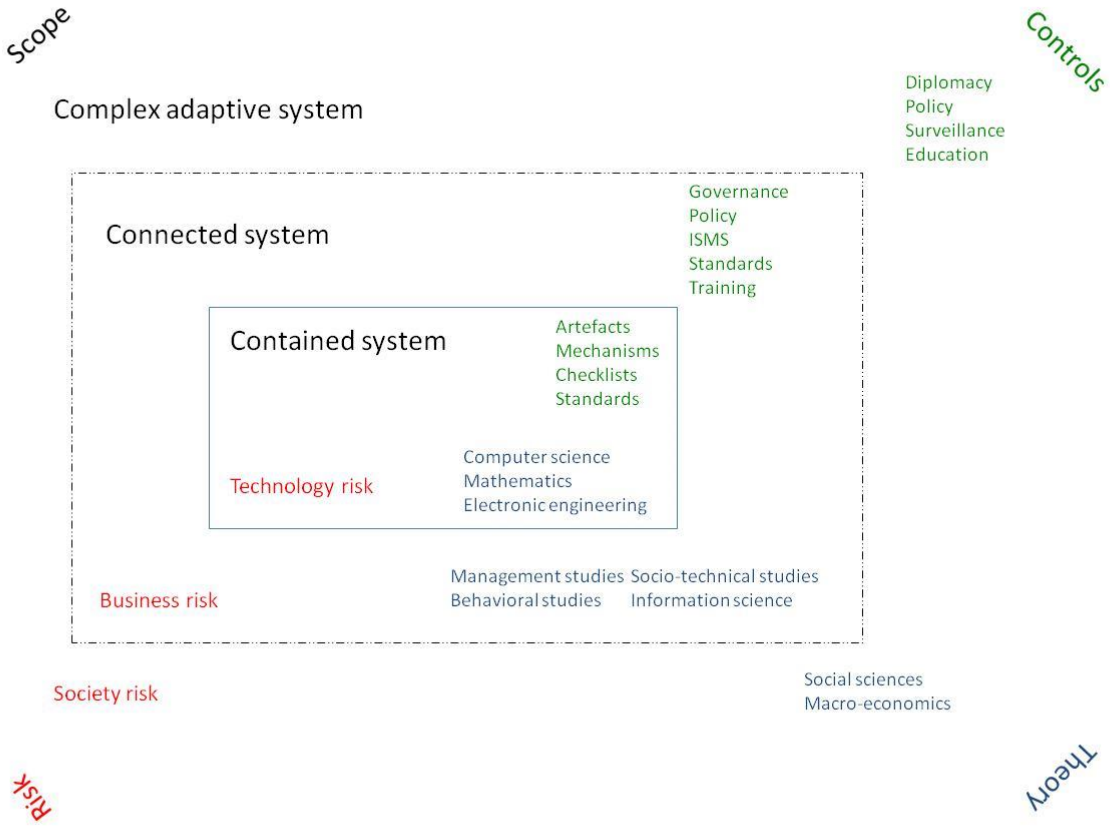


Figure 2-1 Conceptual framework of the perspectives on information security

The multi-disciplinary origin of information security controls is illustrated in the green text in Figure 2-1. Controlling information risks affects ICT systems, networks, people, and social groups. Controls can take any form, such as technical artefacts, building security, peer pressure, ethical norms, policies, cyber diplomacy and so on. These can be inflicted upon elements (an ICT system, an organisation or a human) in a system by governments or by managers, or they can emerge as security events occur. For instance, the research of Coles-Kemp (2008) showed that controls constantly emerge from ad hoc decision-making, parallel to formal change processes and thus that security management can be seen as an adaptive system. Security controls aim to create robust systems, and they alter themselves in response to threats. If one security incident affects a certain element (an ICT system, an organisation or a human), other units can respond due to their interdependence with the disrupted unit.

2.6 Conclusion

This chapter elaborated on the socio-technical view on information security risks that underpins this thesis. Several schools of thought were considered and brought together in a conceptual framework of socio-technical information security. The framework guides the exploration of the risk scenarios in this thesis and indicates the different areas to consider when assessing information security risks. These areas include human factors (e.g. behaviour, motivation, ICT skills and so on) and factors from the environment (such as public policy, social norms and ethics, crime rates, building or neighbourhood security and so on). In the literature and in practice, these areas are often approached in isolation and information security literature that combines these areas is scarce. The aim of chapter 2 was to provide background information of the socio-technical aspects of information security and to make a contribution to the knowledge of how it relates to information society.

The remainder of the thesis focuses on information security in healthcare organisations specifically. Therefore, chapter 3 reviews the literature on practical issues with information security in healthcare. The literature review seeks to answer why controls from society and management, such as governance and policy, and technology or process focused risk assessments do not always deliver satisfactory results.

3 Information security risks in healthcare

3.1 Introduction

This chapter reviews the literature on information security risks and controls in healthcare. It is shown that the foundations for risk controls, governance and policy, are suffering from inconsistency and from a low acceptance level. Furthermore, it is shown that risk assessments are based on the traditional philosophy of contained systems, which are not fit for the modern complexity of healthcare. This causes a gap in knowledge about the actual information security risks and these are further explored by examining issues with confidentiality, integrity and availability of information. It is concluded that there is a gap in knowledge about unwanted information security events. Furthermore, the proposed controls for these security events are suffering from issues as well. Examples are given of how this situation can lead to public loss of trust in healthcare, financial loss, discrimination, constraints on patient empowerment, unclear and unfair information ownership, and issues with quality of care, billing and patient safety.

3.2 Overview of the literature search

As was stated in chapter 2, information security should be studied from various angles. Therefore, literature databases from different knowledge areas were searched. These areas included health, social science and computing. A more detailed description of the research method and the literature databases can be found in chapter 4 (research methods) and Table 4.4.

The literature review focused on more recent literature, however some older publications were traced through references in these works and added when deemed relevant or when they appeared to be influential. Many publications cover models and frameworks for technical security policies or the development of technological artefacts. However, in line with the scope of this thesis, only publications were selected that were relevant for the research question.

The literature review focused on the following topics:

1. Information security controls (governance and information security policy).
2. Information security risk assessment methods.
3. Issues and risks to the information security goals of confidentiality, integrity and availability.

The search terms were based on these topics and related terminology. The field of information security is very wide and interdisciplinary. During the literature survey, it appeared to be easy to get distracted by related topics, and as a consequence, to get lost in the enormity of related issues and topics. The framework illustrated in Figure 3-1 supported and structured the literature review. The numbers in Figure 3-1 relate to the section numbers in this thesis where the different topics are discussed.

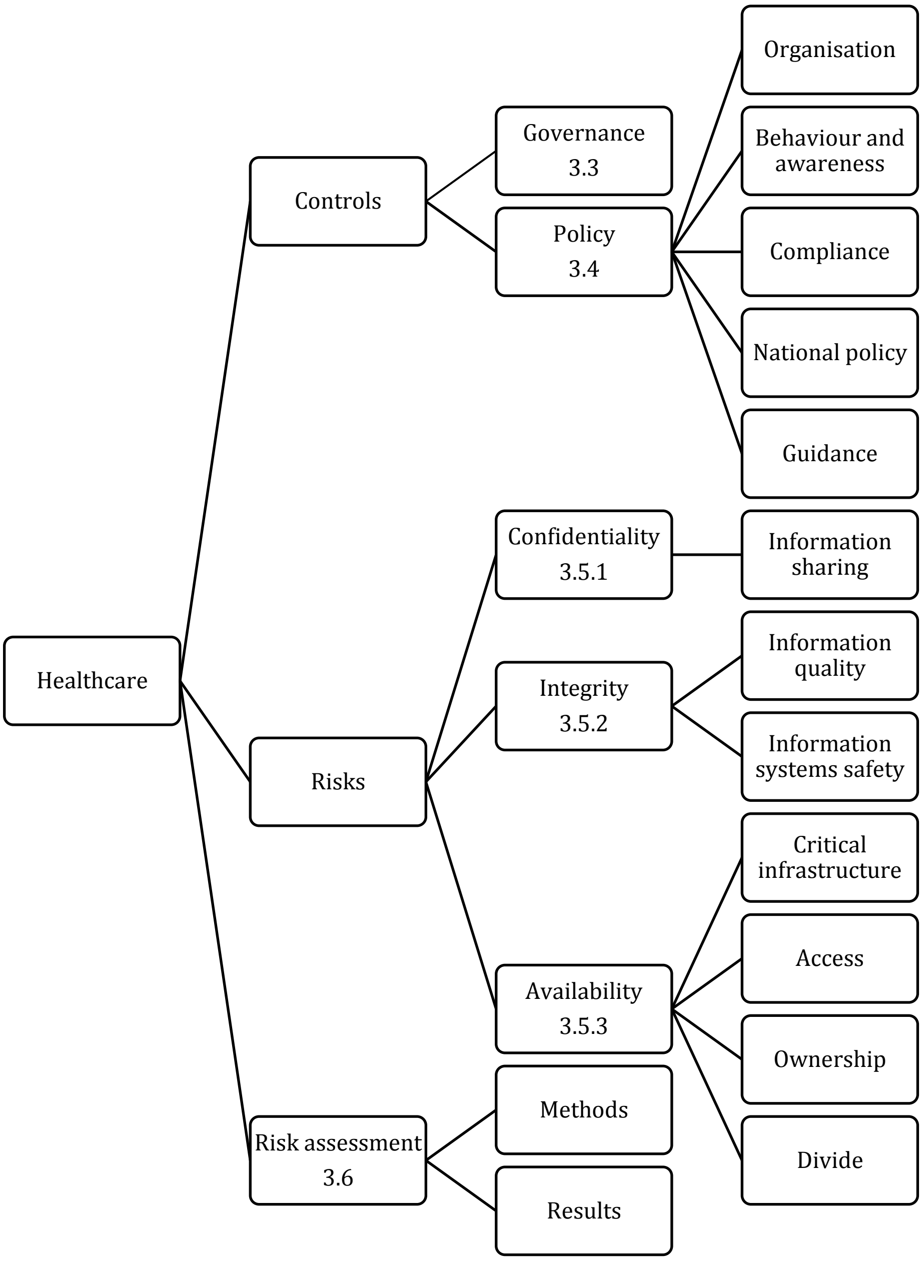


Figure 3-1 Literature search topics

3.3 Information security governance

Recent influences from the Sarbanes-Oxley Act (2002) and the Basel Framework for internal control in banking (1998) put corporate governance, with requirements for accountability, internal control and (operational) risk management, to the fore. Governance requirements made top management and boards of directors personally accountable for the ICT systems on which they base their planning and decisions.

These developments led to the development of the field of information security governance (Fitzgerald, 2012; Moulton & Coles, 2003; von Solms & von Solms, 2008). The difference between governance frameworks with the traditional ISMS frameworks is that information security governance has a strong focus on fraud prevention (von Solms, 2006), information security economics (Anderson, 2001; Anderson & Moore, 2006, 2009; Schneier, 2008) and accountability (IT Governance Institute, 2006).

Governance models treat information as a business asset with a monetary value, like other assets such as money, human resources and facilities. The international standard ISO 27002 states that *"*Information Security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities". The Department of Health in the UK (2012) follows this business-like approach by stating that information must be seen as "core to the business of health and care" (p. 15). The Department sees that information has the potential to improve quality of care, decision-making and efficiency. This potential can only be met if information is available to those who need it and when they need it; if the information is correct and complete; and if it is communicated in line with national and organisational policy.

The economic balance between investments in security controls and the potential risks they are likely to cover is now one of the most influential factors for management decisions. In modern management, information security incidents need to be prevented in order to prevent liability claims, but the investment in security mechanisms should be proportional to the potential risks. Anderson (2003) proposes a new definition of information security: "a well-informed sense of assurance that information risks and controls are in balance" (p. 310).

Information security in the NHS in the UK is integrated in the information governance framework. The governance model for the NHS, as stated by the Department of Health, includes the provision of information to patients, patient consent, records management (including paper records), information security and confidentiality, and information quality (Donaldson & Walker, 2004). As a part of their governance activities, NHS organisations are expected to establish and manage information governance programmes and to develop and maintain corporate or local policies. The local policy should address the information security components such as risk management methods and incident identification; recording; reporting; resolution; and management arrangements. The ultimate aim is "to demonstrate that an organisation can be trusted to maintain the confidentiality and security of personal information" (Health and Social Care information centre, 2013).

A key element of governance is accountability. Top management is seen as the ultimately responsible entity for the wellbeing of the organisation, and should thus accept the responsibility for information security as part of corporate governance (von Solms & von Solms, 2008). Governance requires senior directors' understanding of the risks and the opportunities and to gain assurance that these are properly and continuously managed. In contrast to that, lack of top management involvement has been suggested in the past to be one of the biggest drawbacks in obtaining effective information security in organisations (Kankanhalli, Teo, Tan, & Wei, 2003; Kotulic & Clark, 2004; Whittaker, 1999).

Furthermore, accountability is a hard requirement to fulfil after the erosion of organisational perimeters. In a situation of networked organisations, it is hard to prove for top management that they are in control of the business assets that are outsourced to business partners, vendors, or subcontractors. In the words of Colwill (2009):

> New security threats emerge from these third parties, which are neither completely outsiders nor completely insiders. A single outsourcing transaction can change the status of many hundreds of 'outsiders' to 'insiders' and may blur the distinction between a company's employees and third party personnel: they may be granted logical and physical access levels on par with an organisation's full time employees (p. 190).

Healthcare governance models tend to limit themselves to privacy of patient data (Department of Health and Human Services, 2013; Stahl, Doherty, & Shaw, 2012). However, information security in general is not limited to personal data. Corporate data such as copyright, trade secrets, news under embargo, intellectual property, strategic business information or price sensitive financial data are within the scope of information security. The ISO 27799:2008 for Healthcare Information Security Management focuses on personal health information, but identifies other data that needs protection, such as pseudonymized data; statistical and research data; clinical/medical data, including clinical decision support data (e.g. data on adverse drug reactions); data on health professionals, staff and volunteers; information related to public health surveillance; audit trail data; and system security data for health information (ISO/IEC, 2008 p. 7).

The concept of leadership and governance is relatively new in health, and there is little consensus on how to define, model or measure stewardship of the health system (Brinkerhoff & Bossert, 2008). Case studies, action research or other research on the effects, results or application of information security governance frameworks in individual healthcare organisations could not be retrieved by the researcher nor by the consulted topic librarian, suggesting a gap in knowledge in this area.

Outside of the healthcare literature, information security researchers have investigated various dimensions of information security governance. Steinbart et al. (2012) suggest that there are three streams in such research. One stream of research has examined ways to improve end user compliance with an organisation's information security policies. The second and third streams focus more on economic issues such as the value of investments in information security and stock market reactions to information security initiatives and incidents. They acknowledge a gap in research into operational issues.

Although there are still unanswered questions about the effects of governance, organisations are trying to control information security risks from an operational perspective. For this reason, the research literature on two specific operational issues of information security governance in healthcare was further investigated: information security policy and information security risk assessment methods.

3.4 Information security policy

An information security policy is a specific policy, which states management commitment to security, a definition of information security, and sets out the organisation's approach to managing information security. The international standard for information security management (ISO/IEC 27002:2005) specifies that it should contain a brief explanation of the security policies, principles, standards and compliance requirements of particular importance to the organisation, for example:

1. compliance with legislative and contractual requirements;
2. security education requirements;

3. prevention and detection of viruses and other malicious software;
4. business continuity management;
5. consequences of security policy violations;
6. a definition of general and specific responsibilities for information security management, including reporting security incidents;
7. references to documentation which may support the policy, e.g. more detailed security policies and procedures for specific information systems or security rules users should comply with.

For healthcare organisations additional requirements are identified in the ISO 27799:2008 standard. The healthcare information security policy should contain statements on:

1. the need for health information security;
2. the goals of health information security;
3. compliance scope;
4. legislative, regulatory, and contractual requirements, including those for the protection of personal health information and the legal and ethical responsibilities of health professionals to protect this information;
5. arrangements for notification of information security incidents, including a channel for raising concerns regarding confidentiality, without fear of blame or recrimination.

The information security policy is seen as one of the most important measures to prevent security incidents. However, many reports of incidents or security breaches still occur, suggesting the policies are suffering from some deficiencies (Doherty & Fulford, 2005; HIMSS Analytics, 2012; Information Commissioner's Office, 2010). The literature survey revealed that there are a number of common themes within policy issues. These themes are the style and wording of policies; support and feedback; training; norms and ethics; and national policy.

3.4.1 Style and wording

One suggested cause of problems with policy is the style and wording of the information security policies. Some policies can be as long over a hundred pages and in a technical writing style and they are likely to be ignored (Gold, 2010). A shorter policy gets across the message about the need for information security to a much wider audience than a larger guide would.

Stahl et al. (2012) performed a critical discourse analysis of 25 NHS information security policies. They used a methodology to identify truth, legitimacy, sincerity and clarity. In their analysis, they looked for evidence of ambiguity, confusion or lack of explanation, which might ultimately make it difficult for a policy's messages to be clearly and uniformly interpreted by members of staff. It became clear that the there was a significant amount of ambiguity, in particular regarding the policies' objectives and intended targets, as well as significant evidence of the use of jargon and unfamiliar language. Examples of such jargon are "self-regulatory practices" or "best practice" (p.86). The use of obscure and technical jargon could potentially stabilise existing dominant management hierarchies. Furthermore, they found that many of the NHS policy documents are written with an ideological undertone that management has the right to tell other members of the organisation how to behave, to implement surveillance (in order to check on that behaviour) and to sanction those who do not comply. For example, they found that it was common to state that failure to adhere to the policy "may result in disciplinary action or dismissal or lead to involvement of police service" (p.85).

However, as was found by Guo and Yuan (2012), sanctions do not positively influence the information security behaviour of staff. Their research into the effectiveness of sanctions on information security violations found that a policy enforcing strategy has limited effect. They found that enforcing becomes non-significant when an influencing strategy is used. Employees can be educated to hold themselves accountable for their actions. The authors suggest that there should be a focus on the link between employees' actions and business risks. Another tactic is to use role models who understand security issues and help to advocate policy compliant behaviour. Guo and Yuan furthermore discovered that the more senior the position of an employee, the more likely this person is to violate security rules. This conclusion may indicate an interesting topic for future research, as information security governance is expected to be driven by senior executives.

In terms of wording, it appears difficult to maintain a consistent and clear writing style. Organisations often use their own words to describe what information security means to them. For instance, the Information Governance Toolkit from the NHS defines information security as: "Protecting information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction" (Department of Health, 2010b). Yet, the same toolkit also publishes a code of practice for Information Security Management, in which the definition is: “The preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved” (Department of Health, 2007). This exhibits that even within organisations it can be difficult to maintain a consistent and understandable point of view.

Stahl et al. (2012) conclude their analysis of NHS policies with a number of recommendations to the design of information security policies. They state that the most important lesson that authors of policies must learn is that their policies must be locally derived and created, with participation of the largest group of readers and users. It is recommended that policies use accessible language and terminology and that employees are provided with a separate set of specific guidelines. Concrete examples of issues are helpful to demonstrate the relevance of the policies. Finally, technical content for specialist audiences should be kept in separate documents.

3.4.2 Support, feedback and training

Renaud and Goucher (2012) investigated how employees in a health board perceived and experienced information governance policies. They interviewed well-intentioned employees who may behave insecurely due to reasons other than deliberate malice. The research found a number of key issues. Staff often felt subjugated by policies. The policies were created without any opportunities for staff to influence the content or to provide feedback. Staff felt powerless in the face of sometimes operationally difficult policy directives. Furthermore, they felt a lack of support in implementing policy, regardless of how operationally incompatible the policy might be. Motivations to comply with the policy and to complete tasks effectively and efficiently sometimes conflicted. The researchers proposed a mediation through recognition and rewards for secure behaviour, the implementation of an incident response process, communication between policy makers and operational staff during the creation of policy, and to ensure that policy is fair and equal to all members of staff.

Clinical staff tends to prioritise the quality and continuity of patient care over the following of time-consuming security protocols. The Australian researchers Fernando and Dawson (2009) investigated how a variety of healthcare workers, nurses and doctors practice privacy and security activities in their routines. They found that privacy and security practices are negatively influenced by lack of training, amount of time consumed to perform the security procedure, poor configurations in information systems, lack of integration between information systems, scepticism about the information systems and the people who deliver support, and the natural healthcare environment (such as outdated building structure and fittings, complex regulatory and budget issues). Governance, rules to follow and ICT security settings are perceived as an increase of the workload of clinicians and cause scepticism and workarounds.

Hedström et al. (2011) compared information security policy with staff behaviour in a Swedish hospital and found examples of how staff modify or ignore the prescribed rules in their daily work if they thought that the procedures were not efficient or did not provide enough accessibility to information for their colleagues. Furthermore, they concluded that physicians or counsellors do not always write all confidential details in the patient record, as they prioritised the patient’s privacy over availability and integrity of information.

A review of 54 papers about the implementation of data protection policy in healthcare by De Lusignan et al. (2007) revealed that policies may be misinterpreted or necessary actions not taken if they are not specific, clear or directly relevant or if it does not address the specific tasks of the institution. The researchers state that when the finer details of the data protection principles are not defined, this leads to different interpretations and difficulties implementing the principles and policy into practice. Furthermore, they found that organisational policies also tend to get in trouble when organisational structures change. It can take months before a policy is updated to reflect the new structure, roles and responsibilities and thus leaves the organisation at risk. Security procedures need to be embedded into every practice, as they found that staff will not support inconvenient security controls. Although staff understands and accepts data protection principles, many do not accept personal responsibility for data security. The researchers indicate that staff training, as a means to increase awareness and acceptance of responsibility, shows variable successes. Increasing knowledge alone is not enough and some researchers suggest that establishing social norms and involving staff in the development of policy is more effective to encourage implementation.

Training and awareness are often seen as key to influence staff behaviour and policy compliance. In her Ph.D. thesis on information security management systems, Coles-Kemp (2008) argues that organisational learning is an on-going process and all the information security management processes contribute to this learning activity. Traditional information security training is a form of single-loop learning or maintenance training: concerned with how best to achieve goals and objectives. It plays an important role in ensuring that an organisation knows how to perform procedures and follows policies. However, she found that more control over security is possible when staff has more information about updates within the organisation and its processes. Coles-Kemp suggests that reflexivity or double-loop learning, enables the application of a learning situation back to the individual’s context and thereby challenge the user’s perceptions that have been formed and is therefore fundamental for information security.

Healthcare staff as computer users and their information processing tasks and skills is widely researched in the areas of medical informatics, health informatics and health information management. Healthcare staff needs to “be information able as information is at the heart of the clinical process” (Abbott et al., 2004, p. 77). Computing skills are a significant factor in the acceptance and efficiency of use of information technology in healthcare (Ward et al., 2008). Staff have to remember security procedures and mechanisms, such as locking their screens, password changes, password complexity and not discussing patient cases in front of others. Security skills have become important with the introduction of computing technology, as well as under the influence of the empowerment of patients demanding secure treatment of their personal data. The attitudes, norms, values and security knowledge have become an important aspect of the skill set of a healthcare employee. Education in the use of IT for health care professionals at undergraduate and postgraduate or continuing education levels is identified as an important aspect influencing a positive attitude in health care staff to information technology (Ward et al., 2008) and this effect may stretch into a positive attitude towards information security if this is included in educational programmes.

The technological developments in healthcare have not only led to a change in the requirements for the skill set of healthcare practitioners, they have also led to the development of the new profession of health informatics. According to the NHS Careers website, it is estimated that health informatics is one of the fastest growing professional areas within healthcare since its emergence in the last 25 years. Health informatics is concerned with the development and improvement of the organisation and management of information. The aim is to improve the well-being and quality of care for patients, their families and carers, and the general public, through the use of information and ICTs (Bath, 2008). Job-titles in this area vary and include: chief information officer; clinical informaticist; information management staff; health records and patient administrators; knowledge management staff; clinical informatics; or project manager.

All these professionals are potential advocates of good security behaviour and could function as the role models such as those suggested above by Guo & Yuan or De Lusignan et al.

3.4.3 Norms and ethics

The literature review of De Lusignan et al. (2007) revealed a strong emphasis in research on the development of technological measures to implement legislation. However, they suggest that a multi-faceted approach – looking at organisation, personnel and professional issues – may be more effective. The authors advocate the development of an enforceable code of practice for health informatics professionals to enhance trust and take-up of data protection policies, although they recognise that different social contexts and ethical viewpoints between countries may make it complicated to establish this.

Others also found that it is potentially more likely that employees follow the information security rules if these match their own normative beliefs and if their peers are following the rules (Herath & Rao, 2009). The security policies and procedures of an organisation embed underlying assumptions and beliefs about how to manage information security (von Solms & von Solms, 2004). In other words, security policies and regulations are expressions of values, as well as sets of instructions (Hedström et al., 2011).

In this light, it has been suggested that staff should be allowed more involvement when selecting controls and discussing policies to balance the quality of care with the security of information. Stahl et al. (2012) suggest that such an approach may contribute to the emancipation of information security managers and users and the effectiveness of the policies.

3.4.4 National information policy

Issues with policies do not solely exist within the internal context of organisations. Corporate policies are vulnerable to legislative changes requiring compliance (Orna, 2008). Legislation and national policy relevant to information society issues, amongst which is information security, is referred to as information policy.

According to Orna (2008), governments of all kinds encounter problems in the field of national information policy, caused by power relations, the nature of information itself and economic decisions. Orna states that information policies tend to focus on isolated topics such as copyright, intellectual property, data protection, or digital inclusion. This fragmentation has left some questions unanswered and new technological developments have raised additional issues.

An analysis of information policymaking in the United Kingdom by Buckley Owen, Cooke, & Matthews (2012) found that the government has no appetite for further bureaucracy and for a single information policy. The researchers interviewed policymakers at the highest level of responsibility. If was found from the interviews that there is no requirement for a national information policy, but instead there is the desire for a greater degree of coordination between policies to ensure that they do not conflict. Meanwhile, the opponents of information policy state that information policy may have an unintended negative effect on IT innovation and research (Kaiser, 2006; McGowan et al., 2012; Ness, 2007). For instance, existing long-running research into trends and developments of diseases in a certain population is now obstructed by new data protection legislation that does not allow the researchers to continue to analyse the data they have been using for many years. Ness (2007) found in his survey amongst clinical scientists that privacy rules were adding uncertainty, costs and delay to health research and that this makes research more difficult.

It has been suggested that the essence of political and social democracy is at stake without normative information policy (Duff, 2008, 2012). An example is the digital divide between the information rich and information poor, caused not only by the geographical spread of available communication technologies, but also by the socio-economic status of social groups and individuals. Duff argues that policy must address these social structures as well.

Information policy cuts through sectors such as health, environment, or education. In this respect, the current state of information policies within organisations and businesses is directly influenced by the state of the public or national information policy. In contrast to the inter-sectorial character of information policy, the Department of Health published a sector specific information policy for health and social care in 2012. The policy applies to England and sets out the ambitions to realise the potential benefits of information to improve health and care. The policy states that by 2015, it should be normal for patients to have online access to their health and care services records and personalised information to improve their health. Individuals will be able to take part in decisions about their care in a partnership with professionals. Care records will become the source for all services and to inform research. Confidentiality and security of personal data are promised throughout the policy:

> NHS and other care services will share the information about me with all those who need to look after me (with my appropriate consent), will protect my data and respect my confidentiality (p. 14, point 1.9).
>
> Background data about us which can be used to improve our own care – and which, when held securely and with appropriate confidentiality safeguards in place, […] will, wherever possible, be recorded once within our care records and shared across our care (p. 77, point 5.11).
>
> We have a right to use your data, and a corresponding responsibility to […] take all reasonable steps to protect your confidentiality (p. 84, point 5.39).

The report does not explain how the confidentiality and security will be approached or what the exact rules are. Confidentiality is related only to sharing data amongst and between health and care providers. The report promotes less bureaucracy in that respect:

> Concerns over security and privacy issues […] can lead to a culture that is overly risk averse and reluctant to share information at all, even where it would improve our care. The NHS Future Forum work has heard the clear message that not sharing information has the potential to do more harm than sharing it (p. 32, point 3.9).

The trend for more open records appears to be international, since Brussels is also consulting on its new Data Protection Regulations, which are built on the utilitarian principle of the greatest benefit for the greatest number (Wyatt, 2012). The UK government is furthermore promoting the idea of Open Data; to have data accessible, without limitations based on user identity or intent and free of restrictions on use or redistribution (Cabinet Office, 2012).

The current state of this information policy does not give grounds for organisations to implement an information security policy and to reach a state of compliance. The tendency to less bureaucracy and the focus on confidentiality only (and ignoring other information goals such as availability and integrity), does not help to improve the difficulties with organisational information security policy. The national policy does not articulate any clear answers or responsibilities for security issues. In fact, it is stated that when data protection and related issues get complicated, "there will be consultation with the Information Commissioner" (p.102), shifting the responsibility and final decision making entirely towards the hands of the Information Commissioner.

Furthermore, the policy implies that in the end, the quality of care and the success of the policy is the responsibility of the patient and service users themselves:

> Success will also rely on us as citizens and services users demanding better quality information, greater transparency, conveniences and experiences that meet our expectations of a 21st century health and care system (p. 15, point 1.18).

The policy does not further explore how citizens are supported to express their demands and what these expectations are.

The Department of Health expects that local health and social care organisations ensure they have appropriate systems in place to use and manage information. Details on how to protect the security of health and care data are not provided and for further support the document refers to the NHS Information Governance toolkit website, which contains examples of how local NHS organisations implemented policies and procedures.

Other types of important information which should fall in the scope of information security and thus in the scope of information policy are not mentioned in the policy. These types of information include: employee records; intellectual property; software licences; financial data; press releases under embargo; information regarding criminal investigations; and so on. Furthermore, Scotland, Northern Ireland and Wales are not in scope of the Department's information policy, and they have not published a specific integrated strategy for health information.

3.5 Specific healthcare information security issues

The ISO/IEC 27000:2009 defines information security as the preservation of confidentiality, integrity and availability. These three elements are often referred to as the CIA-triad. If one of these requirements is not met, there is an unwanted or unexpected event going on, which could compromise the quality and continuity of care.

Appari and Johnson (2010) asserted in their literature survey of healthcare information security research, that despite a growing stream of research on information security in general, only very limited amount of research has focused on studying information security risks in the healthcare sector. At first sight, this statement seems true when the term *information security* or *risk* is used as a search term. However, within healthcare, the CIA-triad is heavily discussed and researched under different terminology and within related topics. For instance, *confidentiality* has a relationship with research topics such as information sharing, data mining and authorised disclosure. *Integrity* is related to information quality and safety of health information technology, and *availability* is related to access to knowledge and patient records, information ownership, infrastructure resilience and storage of data. When literature searches are expanded with these terms, a large body of research from different academic fields becomes available.

Some authors suggest that the CIA-triad is limiting the perspective, is out-dated, and that it should be expanded with other elements. For instance, Parker (1998) argues that the CIA-triad is “dangerously incomplete” (p. 213) and that it should be expanded with possession or control, authenticity and utility, “or else criminals might find out about vulnerabilities that weren’t thought of” (p. 213). Others suggest expansion with characteristics such as responsibility, personal integrity, trust and ethicality (Dhillon & Backhouse, 2000); authenticity, accountability, non-repudiation and reliability (ISO/IEC, 2009); or privacy, identification, authentication, authorisation and accountability (Whitman & Mattord, 2012).

Conversely, these extensions are confusing. The additional elements tend to become a mixture of security goals, characteristics and solutions. For example authentication is a technical mechanism, and privacy is a human and constitutional right or freedom, which refers to people and not to information. Furthermore, authorisation is not an aspect of information, but related to a process that limits access to data, which in turn leads to confidentiality and availability of information. This diversity in attempts to create a new set of information requirements is perhaps related to the different conceptions of information security that were discussed in chapter 2. Depending on the perspective of the security researcher or practitioner, different information goals are pursued.

The next sections describe issues with confidentiality, integrity and availability of information in healthcare.

3.5.1 Issues with confidentiality

Confidentiality in health care is a legal obligation that is derived from statutory and case law as well as forming part of the duty of care to patient. It is a requirement within professional codes of conduct and it must be included in NHS employment contracts as a specific issue linked to disciplinary procedures (Beech, 2007). Patients have the right to be able to trust healthcare practitioners and should not be deterred from seeking treatment for fear that their personal information may be disclosed without authorisation or consent.

A large amount of healthcare information security research focuses on confidentiality in the context of Data Protection. Smith & Eloff identified in 1999 that the various data protection acts that had been issued internationally still left some unsolved legal issues. They expressed their worries about the lack of uniform policies and legislation, security issues with data sharing across the web and access control to patient data. They suggested that legal issues would become a primary research category in the future. However, almost a decade later, it was found that research focused mainly on technical measures to implement data protection legislation in healthcare organisations (de Lusignan et al., 2007). This section further explores more recent literature on the issues with confidentiality and information sharing.

The principle of data protection originated within the European Convention on Human Rights (1950), which gives individuals and their families the right of privacy, as well as suggesting the circumstances in which it may be appropriate for information to be shared. Data protection principles need to be applicable to a wide range of situations and data sets, however, the finer details are not defined. This leads to different interpretations and difficulties implementing the policy and the principles into practice (Hoffman & Podgurski, 2007; Myers et al., 2008). In contrast, discussions have arisen about whether or not the right to communicate and the right for citizens to access information should be added as a basic human right (International Telecommunication Union, 2003).

In many countries it is a requirement of the data protection legislation that the processing of personal data is both lawful and fair. It can mean an attack on one's privacy when the collection takes place without consent and without transparency about the purpose for which the data is used (Holvast, 2009). Sometimes an ethical dilemma occurs between maintaining a patient's confidentiality, and disclosing information in certain circumstances (Beech, 2007; van der Linden et al., 2009). These circumstances can be necessary when there is a vital interest at stake of the person involved. Other situations may arise when information is available in connection with crimes, children, or vulnerable adults, and when failing to disclose information may expose an individual to risk of death or serious harm. In a situation like this, the healthcare practitioner needs to choose between law and ethics. Some of the medical professions issue ethical codes with guidelines, but not all staff working in or for healthcare organisations are subject to those codes (e.g. IT staff with access to databases for the purposes of maintenance and support have potential access to all data, without being subject to any ethical codes).

Another dilemma arises when data from a patient's medical record is shared for the advancement of knowledge. Whilst this has the potential for increasing medical knowledge and improving the provision of healthcare, the use of data is not without its complications. Although the data held in databases may be anonymised, if a large number of detailed variables are collected, or when there are rarely occurring conditions included (e.g. heart transplant), it may be possible to link the data back to individual patients. Consequently, anonymised data is still subject to data protection principles (de Lusignan et al., 2007). Some scholars argue that it is not possible to completely delink patients' identities from their health information for several reasons such as the discovery of errors or irregularity in care provision, which require identification of the patient for corrective follow-up care (Appari & Johnson, 2010).

Patient consent is defined and interpreted differently in different countries. In general, it means that patients must give permission for the processing of their personal data. Different consent models exists, such as informed consent, implied consent, express consent, general consent with specific denials or general denial with specific consent (Mohammad, 2010). Truly informed consent requires that individuals know and understand the contents of the record. However, not all patients are competent to do so, and this requires an ethical security structure or appropriate substitute consent (Kluge, 2004, 2008). Furthermore, patients often have no real jurisdiction over who sees their medical history and may not understand the true implications of the disclosed information.

When perceived risks of privacy or security breaches increase, patients might avoid care (Myers et al., 2008). Brann and Matson (2004) discovered from the literature about this topic that: "Disclosure of personal information shared with a health care provider in confidence can cause serious hardships for the patient. Many patients experience discrimination, economic devastation, or social stigma as a result of confidentiality breaches" (p. 230).

Health care organisations face challenging projects when they are bringing data protection and electronic health records systems together. Confidentiality is often compromised when transmitting data via networks or over the Internet. The benefits of technology versus confidentiality are another conflicting area. Medical record transmission via computers increases the potential for unauthorised exposure of classified medical information to third persons. ICT experts would say that it is easier to control access to computerised records as there are more possibilities for audit trails and access control, but the translation of legal requirements into access control models has proven difficult.

Another aspect is that data storage is getting more and more outsourced to third parties who can provide service against lower cost. This leads to information security uncertainty. The third party can be located in other countries, and patient data may only be stored in countries that provide adequate privacy protection. Furthermore, the physical distance of third parties make it difficult to audit and control the quality of their security measures to protect the data and systems, and to adequately delete the data when it is no longer needed. New types of services provided by these third parties, such as cloud computing, make it even harder to keep track of where data is stored and how the security is controlled.

Confidentiality could lead to complications when patients use health portals or social networking sites for specific health issues. A person’s cyber identity can become essential for bonding with other patients or physicians. But the Internet is not a private club and posting personal data online is not automatically protected. This can lead to issues when personal details are abused. Health care providers are becoming a primary target for data fraud and identity theft (Kroll Fraud Solutions, 2010). The reasons for this are that both personal identifying information and health information are collected and stored in these facilities. There is often more data in one record than in other sources such as banks and schools. The value of a full identity profile, such as can be found in a medical record, could sell in the underground for $20 (RSA, 2010). In the U.S., these medical identities can be used to sell to people who use it to get medical care or prescription drugs (Johnson, 2009). The inconvenience and economic loss suffered by victims often happens without the victim’s knowledge and can take several years to correct.

3.5.2 Issues with integrity

Integrity as an aspect of information security implies the safeguarding against unauthorised modification of information. Security practitioners tend to focus on the part that says *unauthorised*, by developing and implementing access and authorisation models. However, these solutions aim to protect confidentiality and not the faulty modification of information (by user or system errors) and lack of data accuracy that all can lead to quality, billing and safety issues. For example, a national survey in 2003 of U.S. medical records managers found that 4-7% of the records had errors that resulted in over and under-reimbursement of billing claims (Lorence, 2003). Another example is that in the U.S., between 2008 to 2010, 11% of critical incidents involving healthcare information technology were associated with patient harm (Magrabi, Ong, Runciman, & Coiera, 2011).

Information integrity means maintaining and assuring the accuracy and consistency of data over its entire life-cycle and is defined as the “representational faithfulness of the information to the condition or subject matter being represented by the information” (Boritz, 2005). It is a requirement of the Data Protection Act to keep personal data accurate and up to date.

Traditional paper based medical records can become inaccurate in a number of ways, including backdating, fraudulent entries, erasures, or other modifications. Anyone who has access to the paper record can remove pages, add entries, erase or otherwise tamper with authentic entries. Health information processing systems and technology have the possibility to improve the integrity of medical records. On the other side, these systems and technology introduce a new type of technology-induced and human related errors. The ability to make changes to an electronic record depends upon the rights assigned to a user. Users with data modification privileges can generally add, delete, or modify data or entire records.

Information access control models and solutions are strongly related to the aspects of confidentiality and availability. Abuse of authorisations with the intent to modify information in a patient record is imaginable, for instance, when staff want to cover up their mistakes. However, most inaccuracies and inconsistencies occur due to incorrect use of systems, data entry errors, or system errors.

Information integrity and system usability are strongly related. A study of the implementation of a computerised physician order entry (CPOE) system, found that users create workarounds when encountering usability problems with the system (Niazkhani et al., 2011). These workarounds influence the integrity of the data. For instance, it was found that when the system is unavailable at the time a decision needs to be made, or when an order entry needs to be placed, the user starts to rely on memory about the patient or check paper notes they made during rounds. Other issues were printer problems, miscommunication of orders and ideas between nurses and doctors, or lack of mobile computer devices or usability issues of the system. The staff often fell back to manual and paper based means. These workarounds potentially lead to mistakes, for example with drug prescriptions or information interpretation errors. Although most of the workarounds were made with the intention of maintaining a smooth workflow or to ensure patient safety, in certain instances these workarounds burden providers with extra time and effort or endanger patient safety. The researchers recommend system implementers and evaluators to pay closer attention to recognizing and addressing workflows and workarounds and to design strategies to lessen the number of disruptions and their possible negative consequences.

Information integrity has also strong relations with data quality and information systems safety. Appari and Johnson (2010) suggest that national policy and standardisation initiatives to improve healthcare information technology (HIT) design, development, maintenance and use processes could be beneficial to data quality and safety.

Magrabi et al. (2013) compared the national HIT safety initiatives in seven countries. They demonstrated that there are gaps in the safety initiatives for HIT systems. National initiatives tend to focus on software for health professionals. Only a small subset of software is legally required to be safe in certain circumstances. EHRs and CPOE are seen to be outside this context. For these systems, standardisation is increasing, but this standardisation does not include safety aspects. The researchers found that England had the most comprehensive safety management programme for unregulated software, incorporating safety assurance based on standards for risk management and user interface design, with national incident monitoring. However, they state, the effectiveness is not known. They conclude that the safety of the majority of all types of HIT is not being explicitly addressed in most nations. The design phase of information systems is seen as crucial to deliver integrity. Their advice is that system developers should gain a better understanding of the workflows and users' requirements to prevent workarounds.

Kushniruk et al. (2013) reviewed national efforts to improve health information system safety in Canada, the U.S. and England. They state that data errors may arise from different phases of design; development; and implementation as well as the use of HIT, and are often only detected once systems are deployed within the real environment. They express the concern that the level of quality and safety associated with system use is highly variable, with calls being made for improved design and development processes, risk management, the need for reporting systems and new regulations related to ensuring system safety to maximize the benefits of HIT. The researchers compare the national policy initiatives between the three countries. They conclude that although the national healthcare systems differ, the underlying problems appear similar. Issues with relationships to vendors, error reporting, education, classification of errors and crosscountry exchange of information will benefit from the sharing and communication of ideas, methods, findings and recommendations across nations.

3.5.3 Issues with availability

Availability of information relates to the information being accessible when needed. Healthcare staff needs to access a patient's record to provide their care. Furthermore, patients require access to their records to check on their details. This availability of personal information is regulated through security mechanisms in the technology, procedures, policy, responsibilities and ownership of the information.

A much-discussed topic to ensure information availability in healthcare is electronic patient records (EPR). EPRs allow for easy accessibility and use. Healthcare staff no longer has to search for their or their colleague's file or clipboard with notes. The patient record is available real-time, independent of the physical location of the nurse, physician or patient. The Internet makes it possible to connect databases to each other, so that a doctor in one organisation can view a patient's record from another hospital.

In theory, the organisation and security of electronic records should be easier and better to control than paper records. In reality, security breaches of personal data are in the daily news, feeding the anxiety and questioning the advantages of electronic records to paper based records. The way that records are now accessed, processed, copied, stored and sent to other organisations, is not always understandable for users and patients. Monitoring devices, online services and electronic communication between facilities all possibly have locally stored patient data and leave data vulnerable for unauthorised access or interception during transmission. With so many stakeholders involved in the care, it is important that health records are complete and readily accessible, while at the same time access needs to be limited and controlled.

In the late 1990s, it was estimated that on average 17 people had legitimate access to a patient's record in managed care, including each member on a patient's treatment team, insurance administrators, utilization reviewers and clerks (Munson, 1996 in Rock & Congress, 1999). Nowadays, the number of staff with the possibility to access medical records has grown exponentially. Illustrative is the case of Richard Hammond, a well-known television personality in the UK. He was admitted to the hospital in 2006 after suffering a serious head injury during filming for his television show. It was calculated that around 300 medical staff accessed his medical records via the internal computer system in the 24 hours following his crash rather than the 20 or so, which would be expected for a patient in intensive care (King, 2008). Another estimation is that 100,000 non-medical staff in NHS trusts could have access to confidential patient records (Asley, 2010). This accessibility has serious consequences for the patient's trust in healthcare.

There appears to be a close relationship between availability and confidentiality. Many researchers in different countries found that patients are optimistic about the benefits that electronic records can provide to the healthcare system, but there is fear of the potential for confidentiality violations (Smit, McAllister, & Slonim, 2005). Some examples are:

- A survey by the Kaiser Foundation found that while 72% of respondents believed the electronic records were more efficient, nearly half also felt that paper records were more secure (Conn, 2007).
- In New Zealand researchers found that 73.3% of the participants in a survey were highly concerned about the security and privacy of their health records (Chhanabhai & Holt, 2007), but they see the advantages that electronic records can bring.
- A nationwide project in the U.S. on electronic health information exchange reports that many of the states raised the issue of trust as critical, specifically in the way it affects the potential adoption and viability of electronic health information exchange. Consumer concerns tended to focus on privacy risks from the implementation of new technologies and the potential for unauthorized disclosures of sensitive information to payers and employers (Dimitropoulos, 2007).
- Participants in a research study in Canada were asked about their attitudes toward privacy and health research and trust in different institutions to keep information confidential. Trust was highest for data institutes, university researchers, hospitals, and disease foundations (78% to 80%). Personal controls such as consent and the ability to audit who has accessed one's information – were among the most commonly cited approaches that improved people's confidence in the responsible use of their information for research. Third-party controls – e.g. research ethics boards, privacy officers, privacy commissioners, and panels of affected individuals – were nominated less often. The researchers noted as well, regardless of consent regime, the high level of concern that was voiced over what happens to one's personal information once it is released to researchers (Willison et al., 2007).

Researchers found that patients are keen to have access to their records and to share accountability for the contents (Delbanco et al., 2012; Leveille et al., 2012; Ralston et al., 2007; Walker et al., 2011), but in many countries this is not facilitated. For instance in the UK, patients could be charged up to £50 to gain access to their record (NHS, 2013) and they need to apply through the courts if they want to have information erased. In current society, characterised by individualism, self-determination and patient empowerment, this situation is becoming frustrating. The Department of Health aims to build partnerships between health and care professionals and patients that share decision-making. The owners of the data are the service users and patients and they should be able to access the relevant information about their condition and health, and to access their personal records online (Department of Health, 2012).

Ownership of health and care data is related to information policy. The data is created by an interaction between a health or care provider and a patient or user. There is some legal ground to recognize a co-ownership of the data that is the result of this interaction. The data would not exist without the patient, and would not exist without the involvement of the professional. Should other parties, such as insurance companies, get involved, then they too have a reasonable claim to ownership of that portion of the information that is generated by their involvement (Haislmaier, 2006). Information policy should provide the framework to decide on (shared) ownership rights and norms. Without such a framework, the information technology sector will continue to spend money on technological artefacts to maintain security, without really knowing why and where to implement these.

While most healthcare facilities today use at least some computer technology to manage patient records, the reality is that healthcare is in transition and paper records are still prevalent at many locations. The U.S. Department of Health and Human Services Administration (HRSA) (2011) sums up some the availability and access issues with paper records. They are issues such as: gaining access to record storage areas; finding records left on counters, exam rooms or copy machines; receiving misdirected fax copies; and other similar events. Inappropriate access can be accidental or intentional. Since access to paper records implies physical access, securing against inappropriate access is accomplished by segregating records into separate locked storage areas; restricting physical access to storage areas; recording sign in and sign out procedures; and maintaining records handling training and other similar procedures.

A second aspect related to availability of information is the performance and availability of the underlying ICT infrastructure. If this infrastructure becomes unavailable or does not work properly, the information is not accessible. This infrastructure, including the information systems and databases, need to be controlled and maintained to stay available.

The resilience of the infrastructure to disasters and the continuity of care when information systems become unavailable is key to healthcare. Fires, floods or other environmental disasters that damage physical locations can result in the complete loss of both paper and electronic medical records. Electronic records can degrade catastrophically -- tapes break, a bearing breaks on a piece of hardware, optical media is scratched. Such failures can happen at any time without warning. Depending on the type of storage and the amount of damage, it may be impossible to recover the affected data.

Healthcare infrastructure needs to be available all the time. It is considered as a critical infrastructure: an essential asset that needs to be available for the functioning of society. Critical infrastructures are vulnerable because they are highly dependent on networked information systems. On top of that they are interdependent: should one infrastructure (such as the electricity network) fail because of an accident, a natural event, or an intentional act, it could bring down other infrastructures as well. Healthcare has a dual relationship with other critical infrastructures. If healthcare infrastructure fails, it could lead to the loss of medical knowledge, the inability to control outbreaks of diseases, and loss of life. The other way around, in the case of a national disaster, one of the challenges is to prevent the extension of the surrounding chaos into the medical facility. At the same time, the use of technology in an unstable and unpredictable environment, such as after a disaster, creates specific requirements for health networks and hardware. For instance, Levy et al. (2010) describe how after the earthquake in Haiti, a field hospital managed to operate an electronic hospital administration system as well as a complete electronic medical record. This was achieved by using a dual-network infrastructure, both wireless and wired; using laptop computers with battery power; interconnected generators and the use of application software that was specifically designed to enable continuity of work during communication loss with the main server.

Critical infrastructures seem to be under constant cyber attack all over the world (Baker et al., 2010). The attacks that are occurring include massive denial of service attacks, stealthy efforts to penetrate networks undetected, and malware infections. The aims of the attacks vary from shutting down services or operations to theft of services and data or extortion attempts. They are also vulnerable for non-intentional information security risks, as illustrated by the destruction of a water-driven electrical generator at Russia's

Sayano-Shushenskaya dam in 2009 that was caused by a computer operator remotely starting the generator while one of the dam's turbines was being serviced.

Information security literature explores the security of critical infrastructures such as communication, water and electricity supplies (Ericsson, 2010; Farrell et al., 2004; Sterbenz et al., 2010), but healthcare resilience appears to be less often researched and applied. The 2007 World Health Organisation global assessment found that less than 50% of national health sectors had a specified budget for emergency preparedness and response (World Health Organization, 2008).

The American Medical Informatics Association's health policy conference supports the vision that system failures and other undesirable outcomes are in the nature of healthcare systems and unavoidable. They state that the "threats could affect the stability of the overall healthcare system" (p.461) and "disruptions in care and security challenges […] could result in the loss of public trust, a loss that may extend beyond the government to healthcare institutions and even providers" (p. 462) (McGowan et al., 2012). The conference members suggest specific actions to maintain the healthcare infrastructure and to prepare for contingency. These actions include the identification of the risks in new technology; the sharing of information about system performance; policies to promote interoperability to support system resilience and emergency response and new approaches to predict system failures.

A final risk is the risk of technology becoming obsolete. Retrieval and use of paper records is not affected by technological changes. Even where paper records are stored on film or micro-fiche, the expected technology life cycle is sufficiently long to avoid obsolescence concerns. Electronic records depend upon computing technologies that have notoriously short lifecycles. This means that during the life of an average medical record, the computing technologies will have undergone multiple generational changes. With each technology generation, previous technologies lose market value and manufacturers cease production. This means that the technology upon which the EHR system depends will become unsustainable as replacement parts become unavailable and operating systems and database platforms lose vendor support.

A third requirement for modern healthcare is the availability of medical knowledge through patient information portals and social media. The accessibility of knowledge about conditions might help to improve self-care and patient empowerment.

Unavailability of information can have direct consequences for the quality of healthcare in a society.

The Internet has given patients more availability to medical knowledge, which is causing a change in the relationship between doctors and patients. Cullen already identified this trend in 1998 (Cullen, 1998). Patients are nowadays empowered by access to their medical records and access to medical knowledge in general and as a consequence, are able to discuss their treatment options without accepting that "the doctor knows best". Mair (2011) states that the traditional paternalistic approach of doctors does not fit in today's society anymore, but society is still struggling with issues such as ownership and censorship of patient records.

Medical information is becoming available for a wider public through social media. Patients use forums to discuss and share problems, and offer their own reviews and opinions. The use of social media in healthcare is generally seen as the tool to empower patients and to improve quality of care through better communication (Hawn, 2009). A systematic review of 98 original research studies on social media in healthcare found that although there are many benefits, some limitations exist as well. One of the limitations is the need to:

> address regulatory and security issues to broach a way forward for best-practice that allows the benefits of social media to be utilized yet still protects patients' privacy and to therefore improve use of these media in routine clinical care. This is a public policy issue and is already being contested in the United States (Moorhead et al., 2013 p. 10).

Batchelor et al. (2012) researched legal frameworks governing the use of social media by people with dementia. In our aging society, people are increasingly being involved in e-health technologies, enabling users to avoid or postpone moving to care homes. The decision-making ability of ageing people is often diminished or compromised as a result of dementia or age-related changes. These people have a lesser ability to give informed consent to contracts or user agreements, or to understand digital footprints, and evidence of online activity and connections. The researchers found that many issues that come from a loss of competence have been addressed in existing regulations, such as managing their finances and property or powers of attorney, but the applicability to online environments is not straightforward and the issues have not been considered together in this context. The ethical and legal responsibilities and duties of care of technology providers, healthcare professionals, regulatory bodies and policymakers "need sustained transdisciplinary research" (p. 101). The questions about the legal framework concern not only the vulnerable people, but they concern all users of social media.

Issues with information availability resonate in sociological discussions about inequalities between patients in terms of access to, use of, or knowledge of information technology and the Internet. Patients who do not have the skills or means to access information about their condition or about healthcare services, are perceived to be disadvantaged in demanding the best possible care and to actively participate in medical decisions. Most of the health information is available through the Internet, however, the Internet is not equally accessible, with less educated, economically disadvantaged and socially marginalized persons being least likely to access it (Kalichman et al., 2002; Neter & Brainin, 2012).

3.6 Risk assessment methods

Standards and regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the U.S., or the Information Governance Framework for the NHS in the UK, require the performance of regular risk assessments and the implementation of controls to secure data. In the UK, the Department of Health recommends that the boards of NHS organisations should ensure that the effort and resources that are spent on managing risk are proportionate to the risk itself (NHS, 2009). Therefore, it is essential that risks are valued according to the likelihood and damage they can cause and that the risk assessment leads to a quantified value for the risk.

Information security risk management has been widely researched in the areas of information systems, financial organisations and in military environments. However, within healthcare, Appari and Johnson (2010) demonstrated that only anecdotal evidence exists of the successful implementation of frameworks. Such frameworks are the U.S. best practice approach Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) (Collmann, 2005) or the CCTA Risk Analysis and Management Methodology (CRAMM), which is the standard for the NHS (Macdonald, 2005; NHS Commissioning Board, 2012). For the purposes of this thesis, it was essential to survey methods used in healthcare and to compare their characteristics. An adjusted version of this section of the thesis was presented as a (peer-reviewed) conference paper at IADIS 2011 (Hazelhoff Roelfzema, 2011).

In general terms, risk management is the process whereby organisations methodically address the risks attached to their activities. Risk management can be applied to a business area, a project, a task or whenever money or resources need to be spent. Risk management for healthcare organisations can be defined as an organized effort to identify, assess, and reduce, where appropriate, risks to patients, visitors, staff, and organisational assets (Kavaler & Spiegel, 2003). Risk management in healthcare includes the whole spectrum of things that could and do go wrong. It includes slips, trips and falls involving staff, patients and the public, administrative errors that impact on patient care and clinical incidents that have a direct effect on the outcome of patient care. It also includes the management of the business risks associated with running a healthcare organisation or hospital including financial, ethical and information technology risks.

One of the most commonly used risk management standards that focus on organisations is called Risk Management–Principles and guidelines (AS/NZS ISO 31000:2009) which sets out a generic risk management process in five main steps:

1. Context identification: a description of the subject for analysis, i.e. the analysed system and its environment.
2. Risk identification: identify what could possibly happen.
3. Analyse risks: identify and evaluate existing controls and consideration of the consequences and the likelihood.
4. Risk evaluation: relating the resulting risk level with risk acceptance criteria.
5. Risk treatment: identification and assessment of treatment options.

Several boards within the NHS have adapted this standard for their generic and clinical risk management processes (NHS 24, 2013; South Western Ambulance Service, 2013).

From an information security perspective, risk management is perceived as part of the information security lifecycle (Peltier, 2005). Most methods suggest that negative events can be prevented and information systems can be made secure if countermeasures are developed and implemented in a logical sequential manner. There are many information security risk management methods available from standardisation organisations, consultants, centres of expertise and the like, all with a different scope varying from small to large organisations, from ICT systems to a business process point of view. The analysis methods can be quantitative (estimating numeric values through methods such as ALE-based methods, the Courtney Method, Livermore risk analysis method, dependency models, and simulation approaches) or qualitative (estimating risks through qualitative ratings with methods such as scoring in CRAMM, OCTAVE, scenario analysis, and checklist methods).

A study in the U.S. amongst 250 healthcare organisations concluded that healthcare organisations are actively taking steps to ensure that patient data is secure. However, hospitals appear to be focusing on how to handle a breach after it has taken place, rather than focusing on prevention through risk assessments (Kroll Fraud Solutions, 2010).

Where security risks have been researched in healthcare, there is a strong emphasis on specific projects or systems (Bolle, Hasvold, & Henriksen, 2011; Lim, Oh, Choi, & Lakshman, 2010; Samy, Ahmad, & Ismail, 2009). In large healthcare organisations, the number of people moving through operational areas is significant. By their nature, healthcare organisations operate in an environment where visitors and the public at large can never be totally excluded. Therefore, as stated by De Lusignan et al. (2007), the human side of ensuring data security is equally important in everyday practice.

In theory, any state of the art risk assessment technique could be employed to facilitate the prevention and management of potential information risks. Examples of these techniques can be found on the website of ENISA (2010).

Smith and Eloff (1999) argue that healthcare information systems are quite unique when compared to other information systems, with the result that they require a specific approach to risk management. They state that the purpose of a healthcare organisation is to take care of the patient. The most important asset is, therefore, the patient, as opposed, for example, to a financial institution where finances are the most important asset. Smith and Eloff further state that the need to protect the privacy of the patient is equally important as the sharing of patient data in order to ensure the availability of accurate and timely information to all authorised communicating partners. Security controls implemented to minimise risks, must thus be evaluated in terms of their functional benefits for protecting the privacy of the patient, whilst at the same time providing timely accurate information to service providers and physicians. Furthermore, the distributed healthcare environment increases the number of possible risks that could occur, in view of the fact that there are many communicating partners, some of whom could be untrustworthy. Most of the consequences of the occurrence of threats in healthcare information systems are very difficult to quantify, because of their non-financial nature. Another concern with respect to the vulnerabilities in healthcare, is its subjection to unique exposures, such as medical professional liability, managed-care errors, and dealing with emergency situations which differ greatly from other sectors. If a patient is, for example, admitted to the casualty unit of a hospital, it is essential that the patient data should be available at once in order to treat the patient properly. Lack of the availability and integrity of patient data could lead to loss of life. Smith and Eloff believe that all the above-mentioned features need to be incorporated when performing risk analysis in healthcare. Existing risk analysis models can thus be adapted to further improve risk analysis in healthcare environments.

3.6.1 Comparative review of methods

Information security risk assessment methods used in healthcare were compared using a framework of characteristics. The framework of characteristics was partially based on other comparative frameworks for information security risk assessment methods. Vorster & Labuschagne (2005) created a framework to support organisations to choose the method that best meets their needs. In this framework the criteria are as follows:

- whether risk analysis is done on single assets or groups of assets;
- where in the methodology is risk analysis done;
- people involved in the risk analysis;
- the main formulae used;
- whether results are relative or absolute (p. 97).

The criterion whether risk analysis is done on single assets or groups of assets is relevant, because assets that suffer from information security risks are closely related, as was argued in chapter 2 of this thesis. In many cases, “a threat will affect either all the assets of an organisation, or a group of assets, but seldom only a single asset” (Vorster & Labuschagne, p.97). This criterion is added to the comparative review under the heading: **focus**.

Another criterion that was reused from this framework was the possiblity of comparing risks. Some methods rank risks in a qualitative way and others score risks with a value. This criterion is added to the review as: **measurement method**.

ENISA (2010) has generated an inventory of risk assessment methods. Each method has been described through a template with 21 attributes that describe characteristics of the method. Some of these attributes that provide general information about a method are included in the review framework. These attributes include: **origin** (country and organisation), publication/first release **year**, compliance to **standards** and **scope**/target organisation.

Additional attributes were added to discover and emphasise individual strengths of methods. These attributes were: **key feature, research activity** and **presentation**.

After combining the relevant aspect of existing frameworks, the review framework for this thesis was as follows:

1. Sector: The market sector that it was designed for or developed in. Was it developed specifically for healthcare?
2. Standard: Formal method or industry standard that it refers to.
3. Year: The date when the method was published. This gives some indication of the maturity of the method.
4. Aggregation: Is it possible to analyse results and aggregate data from individual assessments to organisational or regional level?
5. Scope: Information systems, human, process, society focus or combined?
6. Measurement method: Is risk measured with a quantitative or a qualitative approach?
7. Presentation and risk description: How are risks presented and described in words?
8. Key feature: What makes this method special?
9. Research activity: Are there published case studies in healthcare organisations or evaluations available?

A literature search in databases with journals related to computing, healthcare, nursing and medical informatics (as listed in Table 4.4) was performed to find case studies or reviews relating to the use of a specific method in a healthcare environment. Only methodologies that include risk assessment techniques as part of the risk management process were assessed. Several information security methods or standards describe a management framework; they deliver a set of processes to manage information security in an organisation. The scope of this review did not include the question of how responsibilities and procedures are to be embedded within the organisation. This review only compared the risk measurement techniques, as they are the most relevant aspect for this thesis.

Unfortunately, the results did not show many widely implemented formal methods to information risks assessment in healthcare. The literature search found only five information security risk assessment methods for healthcare. Three of these approaches were reviewed in the framework of characteristics. A summary of the characteristics is illustrated in Table 3.1.

Two of the five methods for information security risk assessment in healthcare that were found were not reviewed. The first, Odessa, is a methodology that provides healthcare data security in medical information systems, developed in the UK in 1997 (Warren, Furnell, & Sanders, 1997). The second, Risk Management in HealthCare – using Cognitive Fuzzy techniques (RiMaHCoF), is a prototype for assessing information technology risks in healthcare, created in South Africa (Smith & Eloff, 2002). This approach is a qualitative assessment with the focus on technical aspects. Human aspects are not in the scope of this model. The search in the literature database and wider Internet searches did not find any published case studies or reviews or other evidence of these two approaches being used or having evolved since.

Furthermore, many reports with *risk assessment* amongst the key words used the ISO17799 standard and performed a gap analysis between the requirements in the standard and the organisation in scope (Bava et al., 2009). However, such a gap analysis using a checklist approach is not a risk assessment, as it does not evaluate the potential harm or likelihood of occurrence of an adverse event.

Table 3.1 Risk assessment methods used in healthcare

Characteristic	OCTAVE	CORAS	CRAMM
Origin	Created by the U.S. Computer Emergency Response Team for manufacturing, but tailored for health care since 2002.	CORAS is a European R&D project, aims to develop an integrated framework for model-based risk analysis of security critical systems within telemedicine and e-commerce.	The Central Computing and Telecommunications Agency (CCTA) of the United Kingdom government created CRAMM (CCTA Risk Analysis and Management Method) in 1987.
Publication year	1999.	2003.	1985.
Standards used	SP800-30.	AS/NZS 4360:1999	ISO 27001.
Scope	Risk-based information security strategic assessment and planning.	Applicable to security of critical systems to aid the early discovery of security vulnerabilities, inconsistencies and redundancies and will provide methods to achieve the assurance of the security policy implementation	Providing a structured and consistent approach to computer security management for all systems.
Data aggregation	No.	No.	Some.
Focus	Single asset.	Single asset, process.	Physical, software, data and location assets.
Measurement method	Qualitative ratings of potential impacts of identified threats to critical assets.	Qualitative.	Qualitative scoring system.
Presentation	Scenario, threat trees. Limited use of graphical modelling.	Scenario, UML graphical presentation.	Common risk based tables.
Key feature	Maps threat trees to risk profiles and scores impacts (although qualitative).	Graphical threat and risk modelling.	Supporting tool generates countermeasures for the risks.
Research activity	Several conference presentations and a case study.	Several conference presentations and a case study.	Rare reports of partial use.

3.6.1.1 CRAMM

Several NHS organisations refer to CRAMM as their standard approach for risk assessment (Jackland, 2009; Macdonald, 2005; NHS Commissioning Board, 2012; Scott, 2013). CRAMM is a risk analysis and management method developed by the British government organisation CCTA (Central Communication and Telecommunication Agency), now renamed the Office of Government Commerce (OGC). The method is supported by the CRAMM tool. Its original purpose was to provide government departments with a method that would be specifically aimed at performing security reviews for information systems. Since that time the methodology has been developed, both from the perspective of content and of technical support. The method was commercialised as a tool by a UK firm (Insight Consulting) and subsequently by Siemens, who now publishes the tool under version 5.1, released in 2003.

In CRAMM the information is gathered through interviewing the owners of assets, the users of the system, the technical support staff, and the security manager. In this manner, CRAMM is a review of the security of a product, conducted during the system development or for an already running system. Physical assets are valued in terms of the replacement cost. Data and software assets are valued in terms of the impact that would result if the information were to be unavailable, destroyed, disclosed or modified. There is not much focus on risks in operational processes or human factors.

The risk assessment is qualitative (using the words high, medium, or low to indicate the level of threat and vulnerability), and the supporting software provides the advantage of generating the appropriate controls and countermeasures for each risk.

The documentation produced during a CRAMM review uses a standardized format, mostly in the form of tables. The documentation is compliant with the mandatory documentation needed to achieve ISO 27001 certification. CRAMM is considered to be more a ISO 27001 compliance tool than a risk evaluation method.

In his Ph.D. thesis on information security risk management approaches, Cho (2003) outlines the following advantages of CRAMM: its well-defined structure; applicable to almost all types of system; regularly updated; comprehensive set of safeguards; and is widely used. However, some disadvantages are: takes a large amount of time and effort; it could get mired in too much detail; subjective and requires skilled analysis; existing safeguards are not considered during analysis stage; and costs of safeguards are not considered during risk management stage (p. 58).

Publications about the use of CRAMM in healthcare in the UK could not be retrieved from the consulted databases. Repeated requests placed at the supplier (Siemens) did not receive a reply. The Information Commissioners Office (ICO) (2013) observes that the use of CRAMM, in the UK or elsewhere, has significantly diminished. The ICO bases this observation upon the scarcity of reference materials or media references, as well as upon responses to the surveys the ICO conducted.

3.6.1.2 OCTAVE

OCTAVE stands for Operationally Critical Threat, Asset and Vulnerability Evaluation. It is a framework for security evaluation that was first published by the Software Engineering Institute (SEI) at Carnegie Mellon University (CMU) in 1999. It was developed in the USA to help the U.S. Department of Defense (DoD) address the requirements set out by the Health Insurance Portability and Accountability Act (HIPAA) for personal health data protection. It is a well-documented methodology with a strong presence in conferences and journal publications. Although it was developed for manufacturing, it has been tailored for healthcare since 2002. Several publications describe case studies in healthcare environments (Coleman, 2004, Woody, 2006). The general risk analysis process in OCTAVE starts with identifying the critical assets in the organisation. Critical assets are those assets that will have a large adverse impact on the organisation if their security requirements are violated. Then, a team of analysts identifies the threats to each asset and constructs threat profiles, which describe threat properties such as target asset, actor, motive, access and outcome. The next step is to identify systems in the IT infrastructure that are closely linked to the critical assets. These systems of interest are then analysed for vulnerabilities and a protection strategy is developed.

The measure of risk in OCTAVE is determined solely through the qualitative ratings of potential impacts of identified threats to critical assets. The method rejects use of the probability of risk occurrence. They state it can be extremely difficult to obtain such estimates with a reasonable level of accuracy. Coleman published a report on the use of Octave in three healthcare organisations of different size and geographical location (Coleman, 2004) and reported that the method is usable in different healthcare environments. The method documents the risk findings in tables and creates threat trees using a simple graphical tree-structure. The approach is similar to the one used in CORAS.

3.6.1.3 CORAS

A well-documented and relatively new approach is CORAS (Lund, 2011), a methodology that bases itself on a combination of: hazard and operability (HazOp), fault tree analysis (FTA), failure mode and effect criticality analysis (FMECA), Markov analysis, and CRAMM.

CORAS was a European Research & Development project that ran from 2001 to 2003. The aim was to develop an integrated framework for model-based risk analysis of security critical systems within telemedicine and e-commerce. CORAS has further evolved since, which now provides a customized language, the UML-based CORAS diagrams for threat and risk modelling, and comes with detailed guidelines explaining how the language should be used to capture and model relevant information during the various stages of the security analysis (Hogganvik, 2007). The CORAS' presentation of risks in diagrams improves the understanding of how events are related and could lead to a data security breach.

During risk identification CORAS uses *threat diagrams* to identify and document how vulnerabilities make it possible for threats to initiate unwanted incidents and which assets they affect. The threat diagrams give a clear and easily understandable overview and make it easier to see who or what the threat is, how the threat works (threat scenarios) and which vulnerabilities and assets that are involved. The threat diagrams are used as input to the risk estimation phase, where unwanted incidents are assigned likelihood estimates and possible consequences. After the risk estimation the magnitude of each risk can be calculated on the basis of its likelihood and consequence, and modelled in *risk diagrams.* The risk diagrams specify which threats initiate the different risks and exactly which assets they may harm. This risk representation is then compared to predefined risk tolerance levels to decide which ones that need treatments. In the treatment identification, the threat diagrams that contain the non-tolerated risks are used as basis for *treatment diagrams*. In this phase the appropriate treatments are identified and modelled in treatment diagrams, where they point to the particular place where they should be implemented (e.g. pointing to a vulnerability). The resulting treatment diagrams can be seen as a plan for how to deal with the identified risks.

The CORAS developers conducted several empirical studies with test groups, and concluded that the diagrams facilitate active involvement of the participants in the risk identification sessions, and they are very helpful in visualizing the risk picture. According to the participants, the diagrams explicitly illustrate the threats and vulnerabilities in a way that makes it easy to see the relations and precisely define the risk consequences (Hogganvik & Stølen, 2006). CORAS has been tested, but not widely implemented as a standard approach in information security policies and governance standards. A successful case study has been published for a cardiology eHealth service in Crete (Stathiakis et al., 2003), but no further reports of implementations could be found in the searched literature databases.

3.6.2 Evaluation

CRAMM and OCTAVE have a technology focus and assess the risks of a system, a database, an application or a network at a given point in time. This delivers incomplete results as information security has a wider scope than information systems.

Rouse (2008) describes how traditional approaches to the management of healthcare systems cannot rely on traditional information system management approaches. In his opinion, a major problem with the healthcare system is that it is not really a fixed system, but a complex adaptive system (Rouse, 2008). Traditionally, the management of systems (and thus implicitly the management of the security of those systems) are approached by decomposing a system into component elements (e.g. input, processes, output, subsystems, communication channels, devices) in order to make decisions about their design and security controls. Subsequently, the solutions are then recomposed by integrating the designed solutions for each element into an overall security system. However, not all security problems can be addressed through hierarchical decomposition. For example, decomposition may result in the loss of important information about interactions between the elements. Rouse argues further that another fundamental problem for very complex systems like healthcare is that no one is "in charge", no one has the authority or resources to design the total system.

Most traditional risk assessment approaches start with the establishment of the context of the assessment, or the boundaries of the review (Cho, 2003), as can be seen in CRAMM and OCTAVE. However, the boundaries of modern networked organisations, assets and technology are hard to define, as was argued in chapter 2 of this thesis. The fuzzy context of complex and adaptive systems makes it extremely hard to execute this first process step. For example, when a security incident happens within organisation A that supplies assets to organisation B, it is likely that organisation B gets affected by this incident. This could be directly, when the incident is a virus that contaminates systems that are networked, or it could be indirectly, when the incident involves major fraud or identity theft and organisation B has to explain the situation to its customers. Situations like this occur frequently within the area of sustainable management. If one organisation in a supply chain uses child labour or environmental polluting methods, customers of the vendor of the end-product will ask questions about the ethics of the vendor.

Another issue with complex adaptive systems is that they require adaptive decision making processes and adaptive risk assessment approaches (Rasmussen, 1997). In the information age, a holistic view of assessing risks should be adopted, moving away from the partial view of a single component, to consider the entire spectrum related to the environment that is being assessed.

Crinson (2008) proposes not to seek separate human and technical information security risks. He recommends a focus on how the demands of working with information systems impact upon, and in turn are reconfigured by, material practice within a particular organisation. He states that any assessment of the threat to the security of an organisation's information system will require a methodology that includes the contextual conditions and the existing sociotechnical security mechanisms.

It is essential that risks can be rated in a common currency, allowing financial, operational and clinical risks to be compared against each other and prioritized (National Patient Safety Agency, 2008). This comparison should include information security as a risk category. This currency or measurement could be improved by implementing quantitative risk scoring mechanisms, which is not impossible, as can be learned from the risk models in the banking and insurance industry (Hubbard, 2010).

For regulators and public administration, the management of risk and trust is crucial and it is critical that they receive high quality information about issues and communicate more effectively about them (Lips, Taylor, & Bannister, 2005). Individual healthcare organisations and the sector in general could benefit from a knowledge base of common security risks. None of the above methods support a central database to analyse risks and trends and to benchmark similar environments. Individual risk assessments lead to individual investments in countermeasures to control the risks. If healthcare practices and their partners were provided with the knowledge from others, investments could be shared or specific solutions could be copied and there will be a better understanding of each other’s key risks and priorities. Trend analysis would make it possible for regulators and individual practices to target the main risk areas more quickly and more cost-effectively. Regulators and public administration could also use this knowledge to adjust and maintain their policies and compliance requirements.

An integrated and adaptive risk management approach could support healthcare organisations to meet their compliance requirements. Information risks should not be approached from a technology point of view, as information risks include human, organisational, and societal threats, and should be part of a wider risk framework. The risks should be presented in understandable language, and be quantified in order to better map those risks to countermeasures. The development of a cross-organisational integrated risk management system will allow organisations to respond to their partner(s)’ key risks as they do to their own. Risk assessment results should not be kept within individual organisations; knowledge should be shared in a central system that enables a benchmarking and trend analysis for the whole sector, which could further contribute to policy improvement and cost reductions.

Risk management approaches can be classified into first generation approaches, such as checklist-based approaches; second generation analyses which focus on detailed valuation of assets, threats and vulnerabilities; and third generation approaches that distinguish themselves by including the examination of various perspectives of systems and interrelationships between systems (Cho, 2003). The third generation takes various views into account. However, it still needs to model the system in the conventional way. According to Dhillon and Backhouse (2001), risk analysis approaches are mostly grounded in systems theory concepts and can be criticised for being just another way of evaluating systems, as they often resemble the checklist or evaluation methods. Siponen (2005) performed a similar study and came to the same conclusions. Their conclusions show that risk and evaluation methods have not kept up with the progress in connected technology and artefacts.

The information society of today appears to have “outgrown the approach that traditional risk analysis utilises” (Gerber & von Solms, 2005, p. 25). Risks to the security of information are related to a diversity of other risk areas and cannot be treated in isolation from each other. Examples of such areas include conflicting policies, human resources risks (e.g. hiring an employee who turns out to be fraudulent), physical security risks (e.g. storing data in an unsecure building or natural disasters destroying data storage devices), health and safety risks (e.g. loosing key information processing staff due to an unsafe working environment), risks from crime and aggression (e.g. cyberterrorism, hacktivism or information warfare) or process risks (e.g. an information processing process without correct approval steps leading to falsification of data).

It is a major contention of this thesis that a new generation of holistic, adaptive risk approaches is required. Predictive analytics has made significant advances in the integration of predictive modelling with social and behavioural factors, referred to as Technosocial Predictive Analytics (Sanfilippo, Gilbert, & Greaves, 2012). A new generation of approaches is emerging where modelling and simulation is coupled with social intelligence practices, such as role playing and gaming, to stimulate collaborative decision-making. For example, Greene, Thomsen and Michelucci (2012) researched an approach in which many people were asked to contribute to solve a problem. The idea is that if citizens in a village observe security related events, they can report it. All these independent and sometimes incomplete observations are then evaluated by a group of experts in national security through a collaborative process of revision, evaluation and selection. Remote solvers may discover relationships between seemingly disjointed pieces of information that reveal important patters of behaviour and contribute to high-level intelligence. Using distributed contributors increases redundancy, and improves the quality of information.

Another example of collective data gathering, or crowdsourcing, is found in the weather information gathering research of Elevant (2011). She performed a comparative study of participants in Sweden and farmers in Sudan. Both groups participated by delivering information about local weather observation and it was tested if that information could contribute as a bottom-up practice for climatic information and extreme weather alerts. She concluded that both groups were able to deliver reliable information for forecasting, and on top of that, their participation had a positive influence on their empowerment as they create important data for governments and for the community.

Another stream of research provides insights into different risk analysis approaches. Knowledge based decision support systems for risk analysis are frequently developed and used in medical areas or in aviation. Padma and Balusubramanie (2009) gathered knowledge about shoulder and neck pain risk factors from literature and concept mapping interviews with specialists. The combination of the expert knowledge and a quantification of risk factors were used to create a knowledge based decision support system for patient diagnosis. Gürbüz et al. (2009) analysed fatal aviation incident reports in the Federal Aviation Administration database and applied data mining methods. They categorised the incident data in decision trees and as a result found some rules about fatality rates of incidents.

These approaches show how collective data gathering, expert knowledge, and data from past incidents can contribute to risk analysis. To the best of the researcher's knowledge, information security risks in healthcare have not been extensively researched from these perspectives, nor have any methodologies that apply these techniques made name within the community of security practitioners.

3.7 Synthesis of healthcare information security literature

This chapter reviewed the literature on information security risks and controls in healthcare. It was shown that healthcare organisations, such as those in the NHS in the UK, steer their information security by means of the information governance framework. This framework makes the top management responsible for the confidentiality, integrity and availability of information. However, academic research on the effectiveness of information security governance in individual healthcare organisations is rare. The foundations for risk controls, governance and policy, suffer from inconsistency and from a low acceptance level.

In contrast, a large body of research in healthcare focuses on technical measures to enforce these policies. However, the local and national policy framework to base these technical controls on is often not consistent, nor clearly defined and sometimes even contradictory. Furthermore, organisational or local information security policies suffer from lack of staff involvement, including from the responsible top management.

It was argued that risks associated with information security in healthcare are not being systematically and consistently assessed beyond the scale of specific information technology contexts. Analysing risks within the context of a system or one asset is not meaningful in modern networked organisations. The context is infinite and includes technical, environmental and social (including people, organisation, society) factors. The cultural context in which staff operates defines their views on information security risks, but this cultural context has not been widely researched, nor is it included in the leading risk assessment methods. Risk information is currently not gathered collectively, and the knowledge of healthcare staff and patients, security experts, and data from past incidents is not a part of the risk analysis scope of best practice methods. This situation causes a gap in knowledge about the actual information security risks.

The review of literature about issues with confidentiality, availability and integrity of information provided some insight into negative information security events in healthcare. These can be summarised as:

1. Confidentiality events: patients avoiding care, financial loss, embarrassment/stigma or discrimination;
2. Integrity events: issues with quality of care, billing and patient safety;
3. Availability events: constraints on self-determination and patient empowerment, aging technology, information ownership and responsibility.

Table 3.2 lists these issues in detail.

Table 3.2 Issues with the CIA-triad in healthcare

	Confidentiality	**Integrity**	**Availability**
Issues	The obligation to protect data versus the obligation to share information to prevent serious harm or death. The requirement for sharing private or embarrassing details for the advantages in knowledge to be able to create better care in the future. Digital identities are necessary to maintain control on authentication and access to data and systems, but these imply a new risk as they can be stolen and abused.	Modifying information during workarounds if a system does not work properly. Modifying information to cover up errors. Making unintentional user errors.	Technology makes it possible to access data that is stored anywhere by many stakeholders which improves care processes, but increases security issues. Patients want to access their records but in many countries this is not allowed or facilitated. Decision making ability of ageing people versus the possibilities of the use of technology and social media at home for self-care. Accessibility of medical knowledge to patients through the Internet contributes to better care but widens the gap between the knowledgeable people and those without access to Internet. Technology enables continuity of services but also ages quickly causing un-availability of data in older systems.

	Confidentiality	Integrity	Availability
			Availability of healthcare systems during a disaster versus the negative outcomes of the disaster itself, which make it impossible to use the systems.
Possible negative outcomes	Patients avoiding care. Financial loss. Embarrassment/stigma/discrimination	Quality issues. Billing issues. Safety issues.	Constraints to self-determination and patient empowerment. Unavailable data from older systems. Data and knowledge not available.
Possible solutions	Ethical codes Patient consent Technical artefacts	Standards and national for risk assessment, design, development, and maintenance methods. International collaboration. Education.	Framework for personal data ownership. Critical infrastructure strategy. Public policy for the use of social media in routine care.

It is suggested that countermeasures to these issues should be sought in public policy frameworks, such as: ethical codes, patient consent, strategies and formal methods for artefact development and risk assessment. However, as was shown in the sections 3.3 to 3.5, governance, policy and risk assessment approaches are suffering from problems and thus are not properly controlling possible information security risks.

3.8 Conclusion

Chapter 3 reviewed the literature on information security issues in healthcare. It was found that confidentiality, availability and integrity of information suffers from conflicting legislation, ethical considerations, and technological changes that cause unintentional unsecure side effects. The measures to control these issues are often sought in policy, but not grounded in thorough knowledge of risks that are specific for healthcare.

The remainder of the thesis addresses these issues by developing a method to identify information security risks in the healthcare sector. This method takes the following lessons from this chapter and from chapter 2 into account:

1. Knowledge about information security incidents must be included in the risk analysis because sharing lessons from the past contributes to the general knowledge of information security (Lips, Taylor & Bannister, 2005).
2. Many people and organisations must collaborate to gather security risk data, as sourcing risk information from multiple locations has shown an improvement in reliability of forecasting in other methods (Elevant, 2011).
3. Experts must be involved to identify trends and triangulate the data, as expert elicitation is a proven method for scenario building and forecasting (Padma et al., 2009; Rowe & Wright, 2001).
4. Chapter 2 concluded that information security should be approached from a socio-technical point of view. Technical, environmental and social (including people, organisation, society) factors should be part of the risk analysis. Risks are not limited to certain elements and occur in combination with each other (Crinson, 2008). Any description of risks should take these elements and any possible combination and co-occurrence of these elements into account.
5. Chapter 2 demonstrated that the scope of a risk analysis must not be limited to an asset or a contained environment. There is no such thing as an isolated system or an individual organisation. Assets and their social, physical, technical and human environment are entangled and therefore the scope is unlimited (Rouse, 2008). Risks are not exclusive to one organisation or system, but should be reviewed in relation to the global network.
6. The presentation of risks in scenarios has proved to contribute to the understanding of the risk by those involved in the risk assessment and therefor is preferred above the presentation in words only (Gürbüz et al., 2009; Lund, Solhaug & Stølen, 2011).

The next chapter describes de research methods that were used to create the novel HI-risk method. After that, chapter 5 describes the HI-risk method and how it integrates the requirements above. Chapters 6 and 7 report how the method was applied.

4 Research methods

4.1 Introduction

This chapter is concerned with the methodological choices in the creation and implementation of the HI-risk method: its design; its implementation; and the validation of the results. These different activities required different research methods, which are explained and justified.

4.2 Research methods in healthcare information security

In their survey of the research literature on information security, Appari and Johnson (2010) found that the majority of researchers use design research, qualitative research or quantitative research. Design research is sometimes called improvement research (Vaishnavi & Kuechler, 2008) and it involves the design of novel or innovative artefacts and the analysis of the use and performance of such artefacts. The main goal is to achieve knowledge and understanding of a problem domain by creation and application of a designed artefact. In healthcare information security research, examples of design research can be found in the development of technological solutions for access control (Ferreira et al., 2006), for (authorised) disclosure of patient data for secondary usage such as academic research (Malin, 2007), and for data sharing in a network of providers (Malin & Airoldi, 2007). Qualitative methods are widely employed in social sciences when researchers aim to develop understandings of human behaviour and motivations. Qualitative methods such as interviews, group discussions, and observations are frequently used in healthcare information security research within different research approaches. Some examples of the qualitative research into healthcare information security centre around the impact of legislation on healthcare practices (Terry & Francis, 2007), or on financial risk and fraud control (FBI, 2011). Lastly, researchers in healthcare information security have adopted several quantitative methods including surveys, econometric analysis and statistical modelling in the areas of patients' privacy concerns (Bansal, Zaheid & Gefen, 2007), public policy (Koppel et al., 2005), fraud control (Miller and Tucker, 2009), risk management (Rosenberg, 2001a) and impact of health IT on medical errors (Rosenberg, 2001b).

This thesis combines design research with quantitative and qualitative research methods. The result of the design is an improved method for risk analysis that contributes to the understanding of information security risks in healthcare.

4.3 Research strategy

The research strategy is based on design science research. Design research generally creates and evaluates a model, a method, a construct or an instantiation. Its mission, notes Van Aken (2004), "is to develop knowledge for the design and realisation of artefacts, i.e. to solve *construction problems*, or to be used in the improvement of performance of existing entities, i.e. to solve *improvement problems"* (p. 224). In practical terms, design can deliver artefacts such as a building, a training course, a medical system, an ICT system, a business process and so on. Designing a future artefact is different from describing and explaining the present (Van Aken, Georges & Romme, 2012). Therefore, the philosophical assumptions of design science for the purposes of ICT research are different from positivist or interpretivist approaches. Positivists assume that there is a knowable, single reality. They build knowledge through objective observations of this reality. These observations are done in a highly quantitative and statistical manner. The results are seen as truth, based on evidence, and form a foundation for predictions. Interpretivists believe that there are multiple realities that are constructed based on interactions. Knowledge is created through social interaction with reality in a subjective and interpretive manner. Interpretive researchers seek understanding and descriptions. Design researchers differ in that they assume that there are multiple realities, which are socio-technically enabled. New knowledge is developed to support the design of solutions to field problems. Van Aken et al. (2012) summarise the difference as: "Explanatory research studies the world as it is, design science research is interested in what the world can be" (p. 177).

Winter (2008) found that while design science research is the dominant information systems research paradigm in the German-speaking countries, in many other European countries this type of research is less visible. Nevertheless, there are some indications that design research is settling in as an accepted research approach. Three separate journals have celebrated design research with special issues, namely *MIS Quarterly* in December of 2008 (Vol. 32, No. 4), and the *European and Scandinavian Journals of Information Systems*, respectively: *EJIS* in October 2008 (Vol. 17, No. 5) and *SJIS* in late 2007 (Vol. 19 No. 2). In the management field, Organization Studies has also published a special issue on DS (Vol. 29, Issue 3). Besides these journals, the International Conference on Information Systems (ICIS) runs a separate track on design science research and there is now a separate conference called Design Science Research in Information Systems and Technology (DESRIST).

Kuechler and Vaishnavi (2012) point out that design science research is often used in the fields of education, healthcare, computer science and engineering. Van Aken et al. (2012) add to these the fields of architecture, medicine, accounting, organisation, and management studies. They argue that design science research can be regarded as a family of approaches: “driven by field problems, using a participant-observer perspective, and pursuing a solution orientation” (p.148).

Offermann et al. (2009) compared five existing design science research processes. These processes have three common phases: problem identification, solution design, and evaluation. Table 4.1 presents a comparison of five design science research processes as presented by Offermann et al.

Table 4.1 Comparison of design science research processes (Offermann et al. 2009)

	Peffers et al. (2008)	Takeda et al. (1990)	Nunamaker et al. (1991)	March & Smith (1995)	Vaishnavi & Keuchler (2004)
Problem identification	Problem identification and motivation. Define the objective for a solution.	Enumeration of problems.	Construct a conceptual framework.		Awareness of problem.
Solution design	Design and development.	Suggestion. Development.	Develop a system architecture. Analyse and design the system.	Build.	Suggestion. Development.
Evaluation	Demonstration. Evaluation. Communication.	Evaluation to confirm the solution. Decision on a solution to be adopted.		Evaluate.	Evaluation. Conclusion.

The applied methods are not fundamentally different from explanatory research and can be a mixture of quantitative and qualitative methods. To identify the problem, design science researchers commonly use interviews or literature research. The artefact design is a creative engineering process. Depending on the research field, specific design methods are used or the development process can be pragmatic. Once the artefact has been developed, it is necessary to evaluate it, using empirical methods. Methods in this stage could be observational, analytical, experimental, testing or descriptive. These are listed in Table 4.2, taken from Hevner et al. (2004).

Table 4.2 Design evaluation methods (Hevner et al., 2004)

1. Observational	Case study: study artefact in depth in business environment. Field study: monitor use of artefact in multiple projects.
2. Analytical	Static analysis: examine structure of artefact for static qualities (e.g. complexity). Architecture analysis: study fit of artefact into technical information system architecture Optimisation: demonstrate inherent optimal properties of artefact or provide optimality bounds on artefact behaviour. Dynamic analysis: study artefact in use for dynamic qualities (e.g. performance).
3. Experimental	Controlled experiment: study artefact in controlled environment for qualities (e.g. usability). Simulation: execute artefact with artificial data.
4. Testing	Functional (black box) testing: execute artefact interfaces to discover failures and identify defects. Structure (white box) testing: perform coverage testing of some metric (e.g. execution paths) in the artefact implementation.
5. Descriptive	Informed argument: use information from the knowledge base (e.g. relevant research) to build a convincing argument for the artefact's utility. Scenarios: construct detailed scenarios around the artefact to demonstrate its utility.

Design science research was selected for this thesis as the most appropriate research method because it aims to produce an artefact: a novel method to identify and monitor information security risks. To create this method, it is possible to use the strengths of existing methods and to combine these. The research followed the design science research process as proposed by Peffers et al. (2008). These authors describe a generic design process, based on their review of seven papers that evaluated design science research. In their proposed design process, suggestions for problem solving are drawn from existing knowledge or the theory base for the problem. The design starts with the identification and definition of a problem and its scope. Then, research is necessary to propose suggestions to address the problem. These suggestions provide a foundation for the creation of an artefact. During the actual development of the artefact, the existing knowledge is reused and synthesised. The authors suggest a sixth activity: the communication of the problem and its importance, the artefact, its utility and so on. This activity is not copied into the research design, as it is fundamental to writing a thesis.

Table 4.3 lists the process steps in the left column. The second column describes the activities performed in each of the six steps. The third column links the activities with the knowledge base; the raw materials from and through which the design was accomplished. The last column shows the research methods that were used in the present study to perform the activities.

Table 4.3 Research design

Design step	**Activity description**	**Knowledge base**	**Research methods**
Problem identification and motivation	What is the problem? Definition of the research problem and justification of the solution.	Understanding the relevance of risk analysis, the current methods and their weaknesses. Understanding information security issues in healthcare.	Literature review.
Define the objectives of a solution	How should the problem be solved? What are the specific criteria that a solution for the problem should meet?	Knowledge of that is possible, the strengths of existing methods of risk analysis, risk classifications and research method.	Literature review.
Design and development	Create an artefact that solves the problem.	Combine the strengths of existing methods of risk analysis, risk classifications and research methods to create a method that is a better fit to the problem.	Iterative creation of the classification. Design of the Delphi study.
Demonstration	Demonstrate the use of the artefact. Prove that it works by solving one or more instances of the problem.	Knowledge of how to use the method.	Implementation with survey, data analysis, and Delphi study.
Evaluation	How well does the artefact work? Observe and measure how well the artefact supports a solution to the problem.	Knowledge of relevant metrics and evaluation techniques.	Case study with observations, data analysis, interviews, and survey.

The empirical methods used to evaluate the method are quantitative and qualitative and include a simulation (through a survey and a Delphi study) and a test in a case organisation. These methods are discussed and justified in section 4.4.

4.4 Research methods

4.4.1 Literature review

The literature review focused on finding published material about information security risks and controls. The scope of information security is wide, which led to a wide search, incorporating many disciplines. It included material from social sciences, engineering and computing, and healthcare. The literature review approach followed Edinburgh Napier University's guidelines for literature review and critical reading (Hall, 2009). To find the relevant literature, the available databases in NUINlink at Edinburgh Napier University were used. NUINlink is the main search engine where all the electronic databases and e-journals that the university subscribes to can be accessed. The used databases within these sections were already mentioned in chapter 3, and are now detailed in Table 4.4.

Additional commercial reports, survey data and websites were found by Internet searches using 'out of the box' search engines and through blogs of security experts. Different search terms were used for different sections of the literature review. For any of the searches, the results were approached through similar steps: first to discard all the articles and books that were duplicates from the search results, then to discard the resources if the summary showed that the article was not relevant and finally after reading through the articles deciding whether or not to use them based on quality, relevance and usability.

The literature revealed that information security is a concept that can be approached from different perspectives. These differences have led to relevant studies within different disciplines, but leading to individual solutions for specific problems. It was shown that there is a gap of knowledge about socio-technical information security risks in healthcare. The findings of the literature were usable as a platform, or set of requirements, for the design of the HI-risk method.

The literature review was an on-going process throughout the four years of research. It was remarkable that in the last year of the research, some of the most relevant publications, placing information security in a wider societal context, appeared (Crossler et al., 2013; Mueller et al., 2013; Schneier, 2012; von Solms & van Niekerk, 2013), as well as on-going information security discussions in relationship to society (such as the discussions about the consequences of the U.S. PRISM system to the privacy of citizens worldwide, or the openness of governments' actions). This demonstrates a growing interest in the holistic view of information security and a growing understanding of the relevance of the relations between society discussions and information security.

Table 4.4 List of databases used in both literature reviews

Social science databases	Engineering/computing databases	Health databases
ASSIA (CSA)	Science Direct (Elsevier)	Edinburgh Napier Library Catalogue
British Humanities Index (CSA)	SpringerLink	AMED (EBSCO)
Edinburgh Napier Library Catalogue	Web of Knowledge	ASSIA (CSA)
ERIC (CSA)	Wiley online library	British Nursing Index (EBSCO)
Expanded Academic ASAP (Gale)	Edinburgh Napier Library Catalogue	CINAHL Plus with Full Text (EBSCO)
PsycINFO (EBSCO)	IEEE Xplore	MEDLINE (EBSCO)
Social Abstracts		Science Direct (Elsevier)

A second literature review was performed during the design stage, as a specific design method. This literature review had a different aim from the standard literature review that is expected in a Ph.D. thesis. Vaishnavi and Kuechler (2008, p. 142) propose five steps in this type of design method: (1) Identify existing solutions that satisfy some of the requirements for the solution of the problem; (2) select those solutions that are best suited to the problem; (3) extract concepts and ideas from the chosen solutions that seem to be promising; (4) based on the mined concepts and ideas, form a tentative solution; (5) modify and refine the solution to best suit the problem.

By following these steps, a socio-technical classification of information security risk factors was created. The second literature review compared existing security classifications to find possible combinations and improvements. It led to a novel classification of risk factors.

4.4.2 Data collection

4.4.2.1 Secondary databases

The HI-risk method is designed as a method that is used by a group of healthcare organisations simultaneously. To execute the method, data about past information security incidents in healthcare was needed.

The implementation of the method was not performed with a real group of voluntary participating organisations. Instead, it was attempted to gather data from a variety of healthcare organisations in order to create a diverse dataset. This data was sought in secondary data from past information security incidents. Methodical collected information about data security breaches is available through different sources. Several private organisations, research institutes and governmental bodies publish reports, statistics, papers and surveys about data breaches and information security incidents. ENISA evaluated more than 60 existing initiatives that collected security incident data (Casper, 2007). The list in their study was used for this research as a starting point to find data on security breaches. Additional sources were added, which were found through references in journal articles or on the web. Table 4.5 shows the overview of the data security breach reports and websites in this review. Some surveys are repeated every year and in those cases only the most recent ones were included.

Table 4.5 Data security breach reports and websites

Year	Organisation	Title	Healthcare respondents
2010	PricewaterhouseCoopers, CIO Magazine and CSO magazine	Global State of Security Survey, Trial by Fire	-
2010	Kroll Fraud solutions	Security of patient data	100%
2009	E&Y Global Information Security Survey	Global Information Security Survey 2009, Outpacing Change	6%
2009	Ponemon Institute	2009 Annual Study: Cost of a data breach.	0%
2009	McAfee	2010 Threat Predictions	
2009	Deloitte	2009 TMT Global Security Survey.	
2009	Govcert.nl	Trend report 2008. Insight into cyber crime: trends & figures	
2009	PricewaterhouseCoopers	BERR Information security Breaches Survey 2008	<9%
2009	Information Commissioner's Office	Table of data security breaches from 2007 until April 2009	20%
2009	Identity Theft Resource Centre	www.idtheftcentre.org	13.7%
2008	Computer Security Institute	CSI Computer crime & security survey	8%
2008	Verizon	2008 Data breach investigations report	<3%
2008	Perimeter eSecurity	A Comprehensive study of healthcare data security breaches in the U.S. from 2000-2007	100%
2008	CompTIA research	7th Annual Trends in Information Security: an Analysis of IT Security and the Workforce	-
2007	CSO magazine, U.S. Secret	2007 E- Crime Watch Survey –	7%

Year	Organisation	Title	Healthcare respondents
	Service, CERT® Program, Microsoft Corp	Survey Results	-
2007	Office of the Privacy Commissioner of Canada/Bell Information and Communications Technology inc.	Evaluation of personal health information remnants in second hand personal computer disk drives	-
2007	European commission	Statistical data on network security	-
2007	IT policy compliance group	Taking action to protect sensitive data. Benchmark Research Report.	12%
	DatalossDB	www.dataloss.db.org	
	Privacy Rights Clearinghouse	www.privacyrights.org	
	Attrition	www.attrition.org	
	Openrightsgroup	www.openrightsgroup.org	
	CERT	http://www.us-cert.gov/reading_room/#news	
	CSO Online E-Crime Watch	www.csoonline.com/info	
	Bugtraq	www.securityfocus.com	

Unfortunately, it appeared that the data from these surveys was not presented with enough detail to use in the database. Furthermore, each survey used different methodologies to collect data, with different taxonomies, over different time spans, dealing with different geographical areas and legislation. The result is that different organisations came to different and, sometimes, even contradictory, conclusions. Discovering information about data security breaches with a specific focus on healthcare was even more challenging. In most of the surveys, healthcare organisations form a minority within the group of respondents. The majority of the reports give a general overview spanning a diversity of industries and are limited in exposing information about healthcare organisations. A final shortcoming was that the collected data was often based on the memory of experts filling in a questionnaire and not based on consistent evidence gathering through incident registers. For all of these reasons, the data from these reports could not be used as a data source.

4.4.2.2 Survey

A new strategy to gather incident data was designed and involved approaching healthcare organisations directly. Some NHS organisations in the UK publish information about data breaches in the Information Governance section of the annual report. This information is publicly available. However, since this information is highly aggregated and not all NHS organisations do publish this information, it was decided to approach healthcare organisations directly with a request for insight into security incident information. After consultation with the dissertation supervisors, it appeared that another research project within the faculty was searching for options to gather very similar information from NHS boards in Scotland. It was advised that it would appear unprofessional for the university to have two different researchers from within the same faculty approaching NHS organisations with very similar questions, and it was recommended to approach this survey as a team.

The researchers met a number of times to discuss the best way to retrieve the information and the best format to gain quality data that would suit both projects. The format that would give the best possibilities for both projects to succeed was a survey by email.

Surveys can be a helpful means to collect large volumes of data. The questions can be completed at the convenience of the respondents without interviewer bias or error. The main difficulty in using a questionnaire is securing a high response rate. Kotulic and Clark (2004) tried to survey 1540 organisations about the effectiveness of security risk management. After intensive attempts to receive response to the survey, the response rate did not get higher than 0.61%. The researchers decided to change the focus of their study to investigate why organisations did not want to participate. They learned that the top reasons for not responding to the original survey were related to surveys in general, company policy regarding security information sharing, and excessive use of management time. The conclusion was that it is nearly impossible to extract information about security by mail from business organisations without having a major supporter. Firms are unwilling to divulge such information without strong assurances that the information provided will in no way harm them.

With this information in mind, and as the aim was to collect a large number of data from each respondent, it was considered that interviews (face-to-face or by telephone) would be too time-consuming. Organisations usually have an up to date list of incidents that they use in reports to the management. Therefore, the easiest way for the respondents to provide the information was to send that list by email. An email request was send to NHS boards and trusts in England and Scotland, for an overview of their information security incidents. As the research did not have a major supporter or sponsor, another strategy was used in the hope to receive the best response rate possible. Bearing in mind the advice of Kotulic and Clark that a major supporter was needed, and no supporter was available, the request was emailed to the Freedom of Information officers, referring to the Freedom of Information Act. This Act entitles members of the public to request recorded information from public authorities. A requester may ask for any information that is held (ICO, 2013), but in some cases, the organisation is not obliged to provide the information. However, this strategy resulted in a 81% response rate, which was satisfactory.

The survey contained a questionnaire and a request for a list of information security incidents in the past four years. The questionnaire and the list of incidents was required for the other project and for this research, only the list of incidents was required. The NHS Checklist for Reporting, Managing and Investigating Information Governance Serious Untoward Incidents, prescribes that NHS organisations must register information security incidents, and what must be registered (Department of Health, 2007). The survey used a spreadsheet in which the columns required similar information to this checklist. A limitation of this approach was that not the whole HI-risk classification could be tested. The classification contains more categories than the NHS policy. However, the researchers wanted to keep the vocabulary of the incident list close to what the health boards are used to. It was expected that this would be the most simple and effective way to gain a good response. Also, this weakness would be compensated during the later steps in the research, as the classification was going to be evaluated several times during the next stages of the research.

Initially, the emails were sent only to Scottish Health Boards, as the scope of the other project was limited to Scotland. After collecting the responses, the researchers went their own ways. The data was used in a joint paper about the results (Smith et. al. 2010), and in a thesis on IT risk assessments in healthcare by the other researcher (Smith, 2010).

The Scottish Health Boards reported a total of 504 incidents. After adding the Scottish incidents to a database, it was decided to broaden the research bed. The research bed was enlarged by sending the request for the list of incidents to the FOI officers of Care Trusts in England. England was added to create a bigger dataset in the collective register and thus a higher reliability of the representation of risk scenarios and consequently, would provide a better ground for generalisation. It would also enhance the diversity of organisations adding data. A list of the English trusts was available from the NHS website. All trusts have online presence and their websites were searched for the email address of the FOI officers. The FOI officers were sent an email with the request to provide information about information security incidents (Figure 4-1). Using the exact same request made it possible to combine the data from both surveys.

The responses were collected between September and December 2010. A total of 163 requests were sent and 132 replies were received. This means that a 81% response rate was received and this was considered satisfactory for the purposes of this study, and the remaining organisations were not chased for their reply.

Dear Sir or Madam;

Pursuant to the Freedom of Information Act, I wonder if you could supply me, within the statutory time period, with details of Information Security incidents and further details relating to the incident for your Health Board from 1st January 2005 until September 2010. This includes classification of incident, nature of incident, system or number of records affected, whether the incident resulted in disciplinary action being taken. Normally this information is recorded as part of Information Governance.

I have enclosed a table (Excel format) as this provides further clarification on the information sought and may aid you in satisfying this request. I have used classifications and types of incidents listed in the NHS Security Policy, which may further aid you.

Please note no identifiable personal details are sought. This request has been issued to all Health Boards and the responses will be used for research purposes as part of an academic study.

Should you require further clarification please do not hesitate to contact me by email.

May I take this opportunity of thanking you for your support,

Yours sincerely,

Attachment: Incident register

Date of Incident:	
Role of Individual to whom incident was reported:	Such as: IT Security Officer, Information Governance Lead, IT Manager, Manager responsible for Security, Practice Manager.
Nature of Incident:	Type of incident such as: loss of USB stick containing data, theft of PC or other equipment, misuse of email, unauthorised access to secure area, loss of smart key, unauthorised access to records, failure to appropriately dispose of waste materials containing data, malicious code damaging systems.
Location of incident:	
Cause of incident:	Vulnerability in procedure or internal control, vulnerability in physical security, vulnerability in computer security or combination.
Classification of Incident:	From NHS Information Security Policy Incident Classification Table: Insignificant, Minor, Significant, Major, Acute.
Number of records effected:	
Number of staff disciplined as a result of security incident:	
Was incident reported to IT Security Consultant at NHS NISG?	
Was incident reported to relevant Caldicott Guardian?	
Was incident reported to Chief Executive of Board?	
Actual or Estimated cost of incident to Board (to nearest £500)	

Figure 4-1 E-mail request for security incident data

4.4.3 Delphi study

The survey data was analysed to retrieve the most frequent incident scenarios from the past. To make a risk forecast for the future based on the knowledge of past experience, the scenarios needed to be judged. This was done through consultation of a group of information security experts. Several structured methods for involving experts in research are known. These methods provide for a structured process that combines the opinions of people who have significant experience or expertise in a defined field in order to assess unknown quantities, parameters or probabilities. The combination of experts' input summarizes the current state of expert opinion. Expert judgement analysis procedures can be approaches such as Delphi (Dalkey, 1969; Linstone & Turoff, 1975), Nominal Group Technique (Delbecq, van de Ven & Gustafson, 1975), Scenario Planning (Kahn & Wiener, 1967), or the Classical Model of Cooke (Cooke, 1991).

The Delphi method is a systematic, iterative survey method that enables anonymous, systematic refinement of expert opinion. The experts answer questionnaires in two or more rounds. After each round, a facilitator provides an anonymous summary of the experts' forecasts from the previous round as well as the reasons they provided for their judgements. Each expert may then revise their earlier answers in light of the replies of other members of their panel. It is believed that during this process the range of the answers will decrease and the group will converge towards the 'correct' answer. Finally, the process is stopped after a pre-defined stop criterion (e.g. number of rounds, achievement of consensus, and stability of results) and the mean or median scores of the final rounds determine the results (Rowe and Wright, 1999). It is a flexible research technique that can be modified to meet the needs of the given study.

Another possible way of expert judgement elicitation is through the Classical Model of Cooke (Cooke, 1991). In this model, experts provide a distribution for unknown quantities by specifying 5th, 50th, and 95th percentile values for the quantities of interest. The combination of the expert judgement is obtained as a convex combination of the expert distributions where the experts' weights are derived from the experts' responses to a set of seed variables whose values are known by the analyst and which are used to calibrate the accuracy of the experts' opinions. In this model the experts are not equally important to calculate the final answers.

The nominal group technique is an alternative for brainstorming sessions and was originally designed to generate ideas (Delbecq et al., 1975). Small groups of five or six participants are invited to discuss open-ended questions. Keeping the groups small avoids the problems of dominant personalities and the structure of the session prevents the group from discussing one direction for a long period of time. The disadvantage is that these persons would have to travel to a certain locations to meet, which is time-consuming for them.

Another instrument is scenario planning, also called scenario thinking or scenario analysis. Scenarios are hypothetical sequences of events constructed for the purpose of focusing attention on causal processes and decision-points (Kahn & Wiener, 1967). The analyst first identifies what he takes to be the set of basic long-term trends. These trends are then extrapolated into the future, taking account any theoretical or empirical knowledge that might impinge on such extrapolations. The result is a surprise-free-scenario. This scenario serves as a foil for defining alternative futures. These are generated by varying key parameters in the surprise-free-scenario. Probabilities are not calculated, as Kahn says, no particular scenario is much more likely than all the others. Scenario planning recognises that many factors may combine in complex ways to create sometimes surprising futures. The method also allows the inclusion of factors that are difficult to formalize, such as novel insights about the future, deep shifts in values, unprecedented regulations or inventions. Scenario planning does not aim to long term forecast, but to describe alternative routes for the future. To evaluate the risk scenarios in this research, the method is lacking the option to estimate frequency of occurrence.

Scenario planning concerns planning based on the systematic examination of the future by picturing plausible and consistent images thereof. Delphi, in turn, attempts to develop systematically expert opinion consensus concerning future developments and events. Researchers have stressed that both approaches are best suited to be combined. Authors refer to this type as Delphi-scenario (writing), expert-based scenarios, or Delphi panel derived scenarios. There are various types of information output of Delphi that can be used as input for scenario planning. Researchers can, for example, identify relevant events or developments and, based on expert opinion, assign probabilities to them. Moreover, expert comments and arguments provide deeper insights into relationships of factors that can, in turn, be integrated into scenarios afterwards. Also, Delphi helps to identify extreme opinions and dissent among the experts. Kinkel, Armbruster and Schirrmeister (2006) reported on their experiences with both Delphi-scenarios and scenario-Delphis. The authors found that, due to their process similarity, the two methodologies can be easily combined. Generally speaking, the output of the different phases of the Delphi method can be used as input for the scenario method and vice versa. A combination makes a realization of the benefits of both tools possible. In practice, usually one of the two tools is considered the dominant methodology and the other one is integrated at some stage. In fact, the authors found that in either case the combination of the methodologies adds significant value to futures projects.

Expert judgement has been successfully applied in many fields (Cooke, 1991), however, it has not often been used in the field of information security. Ryan et al. (2010) recently state that they were the first ones to apply expert judgement in a probability model associated with information security related incidents. They used the classical model of Cooke and a stochastic mathematical process to combine the probability distributions for cyber attacks. Unfortunately, their article does not evaluate the quality of their probability predictions and they seem to have overlooked the fact that expert panels exist in information security forums such as the many CERT teams across the world which not only help organisations to respond to cyber threats, but also predict new trends in threats and risks. Examples of these within Europe are listed at the ENISA website (ENISA, 2013).

For this research, Delphi was chosen over Cooke's model as the main method to collect data from experts. The advantage of the multiple iterations in Delphi, where results can be compared and adjusted, gives the effect of interaction between experts and thus is likely to increase the quality of the judgements. As information is shared, it is anticipated that better arguments and information will be more important in influencing the group and that redundant information will be discounted (Clemen & Winkler, 1997). The second reason is the impracticality of the expert weighting in Cooke's model. Rowe & Wright (2001) argue that all expert's opinions should be weighted equally as there is generally not enough appropriate data to adequately rate all experts, because their experiences are incommensurable, or because no objective measurement of past performance exits.

Other advantages are that Delphi has been proven to be a useful instrument in scenario development. As discussed above, the combination of Delphi and scenario thinking seems to work well and it is highly applicable to this research where we are looking to improve security risk scenarios. The aim of this stage in the research is to improve the risk scenarios and experts will be asked for their input not only on probabilities, but also on the quality of the scenarios.

A Delphi type of study is highly recommended for obtaining opinions from experts who live and work in different geographic regions and settings (Pulcini et al., 2006; Rowe & Wright, 2001). This is an important benefit, as the panel of experts is based in different regions, and they are not be able to get together to exchange their points of view personally (this also dismissed the option of the nominal group technique). The anonymity of the Delphi process also encourages open and honest feedback among experts (Gagnon et al., 2009; Williams & Webb, 1994). The latter is particularly important because participants are asked potential embarrassing questions about information security breaches. Although Delphi was developed in the 1950's, the extent of use in research has not fallen over the last 30 years, and between 2000 and 2005 there has even been a greater proliferation of articles using this technique as an instrument, particularly in social science and health science fields (Keeney, Hasson, & McKenna, 2006). Delphi is a usual instrument in the areas of technological and social forecasting, futures studies, social diagnosis, consensus interpretations of social or health realities, communication and participation (Landeta, 2006).

The Delphi method is an attractive method for graduate research and it has been used in at least 280 dissertations and theses (Skulmoski, Hartman, & Krahn, 2007) in a wide variety of contexts. A search in the UK Index of Theses found 45 theses that used Delphi as a research method and 20 of those were in the context of healthcare. Furthermore, Delphi is a common method in healthcare research. Thangaratinam and Redman (2005) calculated that since 1969, there have been over 1400 publications demonstrating use of this technique in a healthcare setting. Its applications have included forecasting disease patterns and health funding requirements, addressing clinical problems and education.

Traditionally in a Delphi study, the number of rounds depends on the level of consensus achieved. However, as the number of rounds increases and the effort required by the participants, one often sees a fall in the response rate (Skulmoski et al., 2007). Furthermore, there is the debate about the definition of 'consensus' and the importance of consensus. Woudenberg (1991) argues that consensus can never be the primary goal as it is not necessary for high accuracy of the judgement. Many researchers do not attempt to set a level for consensus prior to the enquiry. Instead, they make a decision after the data have been analysed or just set a limit to two or three rounds. For the HI-risk method, it was decided to perform three rounds during the simulation.

The method for selecting the Delphi panel is one of the most critical phases of a Delphi study (Kuusi, 1991). This is when the Delphi facilitator considers the most important stakeholders, the most important competence of the experts as well as the terms of delivering information in a Delphi process. To find the panel of experts for the simulation, a purposive sampling type was used after defining the criteria and characteristics of the panel members. Experts needed to have long-standing expertise (minimum of five years) in a senior role in either information security or risk management, in either healthcare organisations or research.

The literature does not advocate one particular optimal sample size for Delphi studies (Keeney, Hasson, & McKenna, 2011). Many studies have used different sample sizes. A panel size of 12 has been suggested to be an ideal number, as Hogarth (1978) showed that groups containing between eight and 12 members have predictive ability close to the '*optimum*' (Hogarth, 1978). Furthermore, Rowe and Wright, in their list with principles for a Delphi study recommend between five and 20 experts (Rowe & Wright, 2001). With larger panels come greater administration and no empirical evidence was found that larger panels provide better estimations. Skulmoski et al. (2007) investigated the use of the Delphi method in 41 PhD studies and concluded that the panel size in these studies varies greatly from eight to 345, depending on the diversity of expertise in the panel and the type of research question.

Thirty-five experts from the personal network of the researcher, conference speakers, and academics working on information security, were invited to join the expert panel by a personal email with a link to the online survey. They included information security managers, consultants, Caldicott guardians (NHS staff with a responsibility to ensure patient data is kept secure), a security journal editor, researchers, and healthcare professionals. Ten of them worked on the survey but only eight completed all questions (two respondents did not complete the whole survey and were excluded from the results analysis). In an attempt to increase the response rate, a reminder was sent to the remaining 27 and, on top of that, 13 more experts were approached through connections in healthcare consultancy and a healthcare software sales consultant who approached his clients with the request for participation. Furthermore, the secretariat of the NHS forum of Caldicott guardians was asked for help and discussions were started in online forums (expertise groups in LinkedIn). The extra effort gained four more experts, lifting the number of respondents up to 12. Compared to the 133 organisations that provided data for the incident database, the panel with the size of 10% of the number of participating organisations was considered satisfactory.

The size of the panel dropped in Round 2 to 11 and in Round 3 to ten. The input of the remaining ten panel members is satisfactory, as ten is still a valid panel size for a Delphi study and an 83% response rate as compared to Round 1 is still above the suggested 70% retention rate to maintain rigour (Sumsion, 1998). The level of professional expertise was also maintained in the third round as illustrated in Table 4.6. In the first survey round the panellists were asked to rate their expertise in different areas on a scale from 0 (no experience) to 5 (more than 10 years' experience). The panel members who completed Round 3 had an average strong expertise in information security (4), information governance (3.8) and risk management (3.8).

Table 4.6 Expertise per round

	Information security	Healthcare/medical	Caldicott guardian/data protection	Risk management	IT Security	Information governance	Other
Mean Round 1 (N=12)	4.0	3.5	2.9	3.4	3.3	3.5	2.6
Mean Round 2 (N=11)	3.8	3.5	2.9	3.2	3.1	3.6	2.6
Mean Round 3 (N=10)	4.3	3.3	3.1	3.8	3.8	3.8	4.0

Usually all participants in a Delphi study remain anonymous. Their identity is not revealed, even after the completion of the final report. This prevents the authority, personality, or reputation of some participants from dominating others in the process. Arguably, it also frees participants (to some extent) from their personal biases, minimizes the 'bandwagon effect' or 'halo effect', allows free expression of opinions, encourages open critique, and facilitates admission of errors when revising earlier judgements.

The questionnaire in the first round contained an introduction to the study, guidelines for completing the questionnaire and the questionnaire itself. The questionnaire was designed as an online survey. Before launching the questionnaire, it was piloted amongst researchers within the Edinburgh Napier University Centre for Social Informatics, a businessman and an information security expert to improve comprehension and to work out any procedural problems. The pilot delivered some excellent feedback about the presentation of the questions. The result was a change to a different survey software package (the free student version of SurveyGizmo) and an improvement in the answer categories. The final version of the questionnaires of all three rounds are added to this thesis in appendix A.

Some Delphi studies use Round 1 to gather information to design a questionnaire that will be used in subsequent rounds. This is also referred to as the blank sheet approach. Another approach is to present the expert panel with pre-defined lists. In HI-risk, a combination is used. The experts are presented with an online questionnaire that contains the scenarios from the previous research step. They are asked to express their personal opinion about the frequency of occurrence in the near future and to motivate their choice. The use of motivations or feedback in the Delphi procedure is an important feature of the technique (Rowe & Wright, 2001). Feedback that includes arguments in addition to summary statistics is an important source to enrich the understanding of the scenario. In addition, a blank sheet with the previously developed taxonomy or risk scenarios is provided to draw up one scenario they think is most likely to occur in the near future and one scenario that they expect to affect the largest number of patient records.

After the first round, the means and medians for each scenario along with the arguments from panellists whose estimates fall outside the quartile ranges were collected and represented in updated scenarios. Furthermore, the suggested new scenarios were added to the survey questions. The updated scenarios, the new scenarios and the comments were presented again in the second round.

In Round 2, the six predefined scenarios were updated with the mean estimates of the panel, plus the upper and lower quartiles, and the comments and opinions from all the panellists. Furthermore, a total of 14 new scenarios provided by the panellists in Round 1 were added. From these 14 new scenarios, nine were selected to be included in the mandatory section of Round 2. This selection was based on the following criteria:

- More than one expert created a very similar scenario (this happened three times).
- The six new scenarios with the highest expected frequency were added.

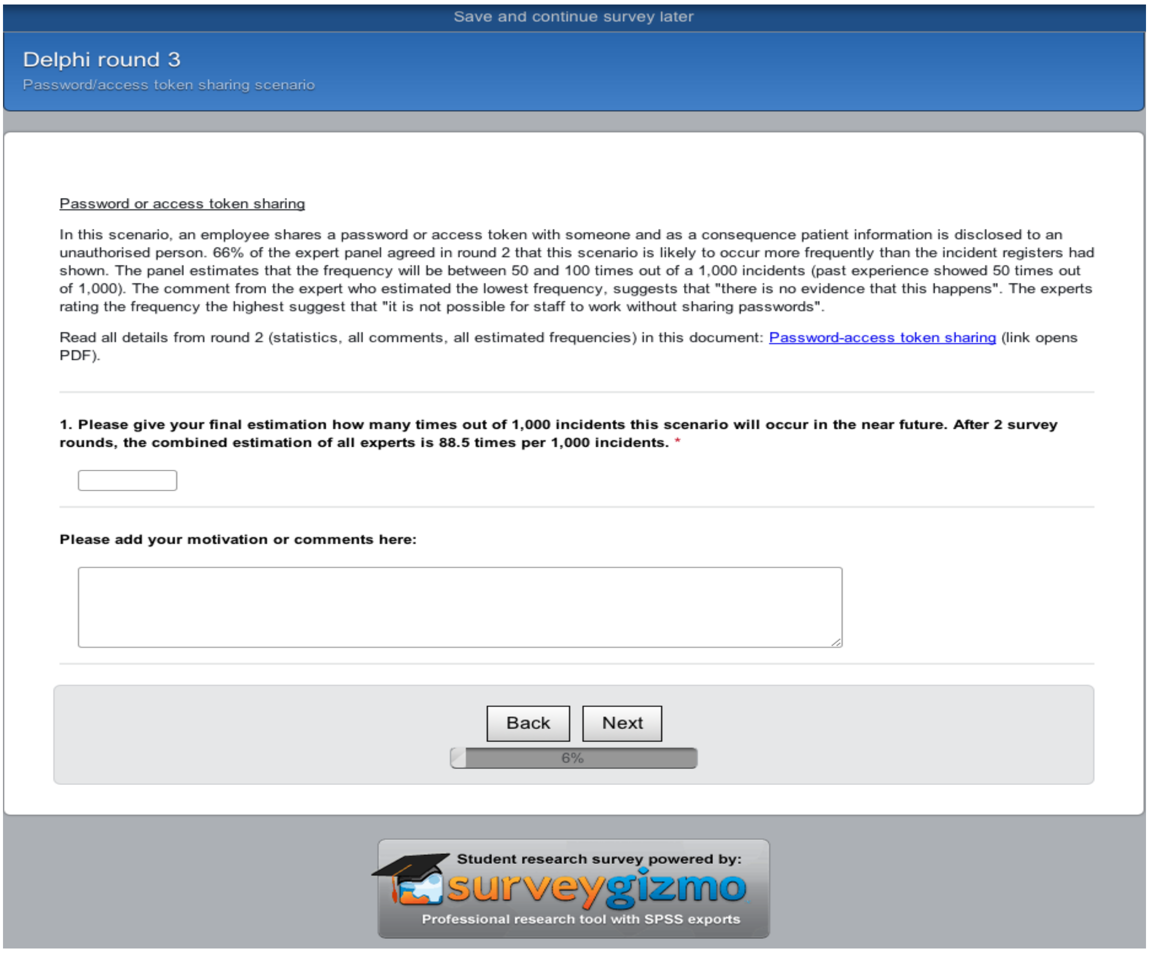
The remaining five new scenarios were added to the questionnaire as non-mandatory questions. The choice to make only 15 questions mandatory was based on fatigue level of the survey. SurveyGizmo runs a diagnostic test on the survey before publishing and the fatigue level score indicates whether or not the survey is more or less likely to cause survey fatigue. With all the added comments, the respondent had a lot of reading to do for each scenario and the completion time would be very long, increasing the risk of experts dropping out. The total number of questions per Delphi round is listed in Table 4.7.

Table 4.7 Number of questions per round

Round 1	**Round 2**	**Round 3**
6 scenarios from incident register 2 blank sheets	6 scenarios from incident register 14 new expert scenarios	6 scenarios from incident register 13 expert scenarios

The aim of Round 2 was to gather the opinion of the experts about the expected frequency of occurrence of a scenario and evaluate the level of consensus amongst the panel members. Round 2 delivered some more descriptive statistics that were used to present the data in Round 3. Added to the means, medians and comments for each scenario were range, largest estimation, smallest estimation, standard deviation and a visualisation of the distribution of estimated frequencies in box and whisker plots.

The questionnaire in Round 3 was a repetition of Round 2, enhanced with the data gained from Round 2. The survey was again divided into a mandatory section and a voluntary section. In the mandatory section, the panel were asked for their opinions about the ten main scenarios and in the voluntary section they could comment on nine less important scenarios. Figure 4-2 illustrates one of the screens from the Round 3 survey.


Save and continue survey later
Back
Next
6%
Student research survey powered by:
surveygizmo
Professional research tool with SPSS exports

Delphi round 3

Password/access token sharing scenario

Password or access token sharing

In this scenario, an employee shares a password or access token with someone and as a consequence patient information is disclosed to an unauthorised person. 66% of the expert panel agreed in round 2 that this scenario is likely to occur more frequently than the incident registers had shown. The panel estimates that the frequency will be between 50 and 100 times out of a 1,000 incidents (past experience showed 50 times out of 1,000). The comment from the expert who estimated the lowest frequency, suggests that "there is no evidence that this happens". The experts rating the frequency the highest suggest that "it is not possible for staff to work without sharing passwords".

Read all details from round 2 (statistics, all comments, all estimated frequencies) in this document: Password-access token sharing (link opens PDF).

1. Please give your final estimation how many times out of 1,000 incidents this scenario will occur in the near future. After 2 survey rounds, the combined estimation of all experts is 88.5 times per 1,000 incidents. *

Please add your motivation or comments here:

Figure 4-2 Screen shot of survey

4.4.4 Case study

The Delphi study delivered a risk map that needed to be tested in a real context. Hasson and Keeney (2011) discuss that the results of a Delphi study do not offer indisputable fact and that, instead, they offer a snapshot of expert opinions, for that group, at a particular time, which can be used to inform thinking, practice or theory. As such, Delphi findings should be compared with other relevant evidence in the field and verified with further research to enable findings to be tested against observed data to enhance confidence (Hasson & Keeney, 2011). In order to test the quality of the results, a real organisation would have to be involved in the testing.

Three possible methods to test the HI-risk output were considered. The first option was to hold a survey amongst healthcare organisations. Organisations could be presented with the scenarios and indicate how much they agree with the expected frequency. A survey would have the advantage that many organisations in different locations could be involved, but it is limited in investigating the organisational context. Furthermore, it would not provide an opportunity to test the quality of the map against a list of real incidents that had occurred.

The second option was an experiment with the model in a controlled environment. This option could deliver a concrete product: the prototype of an expert system for incident and risk monitoring, but it might be difficult to compare the results with real data in their context. Extending this prototyping to a real situation would require a longitudinal study within multiple healthcare organisations that would use the expert system for a longer period of time. This would have been the preferred option if the research had been sponsored. However, this study was self-funded, so unfortunately this was not feasible.

Considering the circumstances, a case study using multiple research techniques was chosen as the best possible strategy to validate the method. A case study suits the type of 'how' research questions (Yin, 2009), looking to find out how staff behaves and how information security risks are identified and controlled. On top of that it provides the opportunity to have in-depth conversations with employees in healthcare to gain a better understanding of the socio-technical context of information security. Furthermore, it is possible to actually observe people in their working environment to test some of the risk scenarios. Finally, it provides an opportunity to run a simulation with the risk map, using real information security incident data.

The case study was held at a large NHS hospital. A sponsor was found in the Speech and Language Therapy department. The case study proposal was given to Edinburgh Napier University's ethics committee within the School of Computing for consideration in September 2012. Although patients were not involved in this study and there was no need to access patient records, and thus formally this type of study would only need approval from the institution where the research will be conducted (NHS, 2012), it would have been possible that –as a visitor to a healthcare organisation- personal information was overheard or patients could be seen. Furthermore, during observations of staff and their security behaviour, members of NHS staff might feel uncomfortable during observations as they might see the researcher taking notes of non-compliant behaviour. Finally, the registers of incident data that were analysed could potentially contain sensitive information as well. For these reasons, ethical approval was requested from the university's ethics committee.

The School of Computing ethics committee decided to refer the request for approval of the case study to the ethics committee within the faculty of Life Sciences. This second committee did not approve of the research and decided that the researcher needed a NHS research passport. This passport is provided by the university having undertaken all the appropriate disclosures and checks on the student and confirms this to the NHS partner. Unfortunately, at that time, the university did not have a process in place to provide research passports and the case was taken to the University degrees committee and to the University Integrity committee in December 2012.

After completing several forms to allow a criminal records check of the researcher, and spending several weeks waiting for feedback or progress, the research coordinator within the case organisation advised in January 2013 that, after all, no disclosure approval nor research passport was needed (NHS, 2012). Furthermore, the university's ethics committee approved the research proposal on 14 February 2013. After that, the correct approval process ran through online forms, which needed completion in the Integrated Research Application System (IRAS). After the necessary authorizations within the case organisation were signed off on 25 March 2013, the case study took place in April 2013.

Semi-structured interviews were held with the IT Security Manager and with the two Information Governance Leads of the Speech and Language Therapy Department. These persons were selected because of their knowledge of information governance and risk management processes and their leading role in promoting secure behaviour amongst staff. The interviews were guided by a list of open-ended questions and more questions were created during the interviews. The set-up was face-to-face and the interviews were voice recorded and transcribed. The interviewees were asked general questions about information governance and information security, about their approach to risk assessment and their opinion about the most important risks. During the interviews, new potential risk factors were identified and these were added to the classification of risk factors. Furthermore, the researcher gained more knowledge about daily information security routines, policies, risk assessment methods and organisational culture.

Observations were held in two locations of the Speech and Languages Therapy department. The aim of the non-participative observations was to test if any risk scenarios could be spotted and if they would fit in the classification. The aim was specifically not to audit staff or to report any potential incidents, as was pointed out to the staff in a preliminary briefing. Staff were observed in their daily routines, without disturbing them. Any potential information security risks were noted and matched against the classification. This led to adjustments of the classification where risk factors were recognised that had not been listed yet. The aim was to test the classification, not to test the security of the case organisation. The observation form to take notes on was the classification itself (presented in Table 5.6 in this thesis), and observed categories were ticked and missing categories were noted and added.

On behalf of the researcher, the IT Security Manager forwarded a survey to his colleagues who regularly participate in risk assessments. The survey was created online in SurveyGizmo with the aim of surveying the business requirements for the HI-risk method. Unfortunately, only three responses were received and the IT Security Manager indicated that it was unlikely to receive a better response, as only a few members of staff perform risk assessments. Therefore, the results of this survey cannot be used for generalisation, but they still provide a useful indication of opinions about risk assessment methods within the IT department. The survey contained nine questions about risk assessment methods, frequently occurring risks and risk management.

The ultimate test of the quality of the forecasts was the analysis of the incident register. The incident register data was copied into the HI-risk database and benchmarked against the risk map, using the same scenario analysis technique as before with the primary data. This led to conclusions about the quality of the forecast shown in the risk map.

4.5 Evaluation of the research methods

As discussed above, the original research plan was to create a database of security incidents, and to perform a quantitative analysis with data visualisation techniques. Bayesian statistics would support the possibility of calculating potential future risk scenarios, even when one or two variables are unknown. Unfortunately there appeared some hurdles with the data collection, which caused the research plan to change twice.

The first hurdle was the lack of re-usable secondary data and databases about security incidents. Unfortunately, published data from past surveys appeared to be not detailed enough, was fragmented and was collected with different methodologies, different taxonomies, over different time spans, dealing with different geographical areas and legislation. The result is that different publications came to different and even contradictory conclusions. Finding information about data security breaches with a specific focus on healthcare was even more challenging. In most of the surveys, healthcare organisations form a minority within the group of respondents. This hurdle led to the decision to change the original plan and to gather primary data directly from healthcare organisations.

The second hurdle was the low level of quality of the primary data about security incidents that could be collected. After a survey, healthcare organisations provided a list of their past security incidents to the researcher. The description of these incidents was often very high level and abstract and gave only limited insight in what actually happened. There was not enough detailed data available to run quantitative statistical analyses. Therefore, the analysis of the incident database was done through qualitative techniques. On the positive side, this research hurdle confirmed the value of the role that experts play in security risk management. The design choice to include expert knowledge in the method, proved to be very important to fill in the omissions and to triangulate the quality of the scenarios.

The HI-risk method uses a combination of data gathering techniques from different sources with the aim of producing risk data that is less dependent on scope, time and stakeholders. The selected techniques have been validated and checked for reliability by doing the following:

- Reviewing other methods for risk assessment for the use of chosen research methods. All individual techniques have been used by other researchers and practitioners to study information security risks, however, to the best of the researcher’s knowledge, they have not often been used in combination with each other.
- The surveys were piloted on independent staff within the faculty and external information security consultants and IT sales managers, all of whom were unrelated to the research.
- The Delphi study is self-validating through its design in three rounds.
- The HI-risk method was validated by running a simulation to prove the usability of the process steps.
- The results of the method simulation were validated in a case study. Hevner et al. (2004) pointed out that the result of any design research could be considered a success as long as the practical addition to an area of knowledge can provide the basis for further exploration. The results of the case study are encouraging for further development of the automated part of the method.

4.6 Conclusion

This chapter explained the research methods. It was a requirement that the HI-risk method that was created included risk data collection techniques to ensure less dependency on subjectivity, time and stakeholders. The research used a diversity of qualitative and quantitative methods to collect and analyse data within a design science research strategy. Figure 1-1 in chapter 1 showed a summary of the steps that were performed during the research and refers to the chapters in this thesis that report the results of each step. This chapter explained the methods behind these steps. The steps follow the process of design science research. In this process, the first step describes the problem and motivation of the project. Then the requirements for a solution are created. The third step is to create the artefact: which in this research is the HI-risk method. The artefact is then demonstrated and evaluated to measure how well it performs.

This approach ensured that the best possible effort within the circumstances was made to create a reliable method and resulted in validated risk scenarios that included risk categories from different perspectives. The next chapter (chapter 5) describes the final artefact that was created: the HI-risk method.

5 The HI-risk method

5.1 Introduction

Chapter 5, 6 and 7 together represent the research results. The results are separated over different chapters because they represent the different stages in the research.

First, this chapter 5 presents the design of the HI-risk method. This is the artefact that was created during the research. The design of the HI-risk method is based on an evaluation and re-use of best practices. This chapter explains how the method came to be: the requirements that is was based on, the process steps within the method and how existing methods were reused and adjusted to fit the requirements for HI-risk.

Chapter 6 presents the results of a simulation with this method. To simulate HI-risk, primary data was collected, analysed and used as input for a three-round Delphi study. The conclusion of this simulation was a forecast of risk scenarios in healthcare.

Chapter 7 presents the validation of the forecast by means of a case study. The HI-risk method was tested to determine how reliable the results are for practical use in an individual organisation.

5.2 Method requirements

From the background and literature review chapters, the following requirements for an information security risk assessment approach were identified (as detailed in Section 3.8 of this thesis):

1. Knowledge about information security incidents must be included in the risk analysis.
2. Information security risk data must be sourced from multiple locations and organisations.
3. Experts must be involved to identify trends and triangulate the data.
4. Technical, environmental and social (including people, organisation, society) factors must be part of risk analysis.
5. The scope of a risk analysis must not be limited to an asset or a contained environment. Assets and their social, physical, technical and human environment are entangled and therefore the scope is unlimited.
6. Risk factors occur in combination with each other in scenarios.

These requirements were taken into consideration for the design of the method.

5.3 Method description

HI-risk [short for Health Information risk] is a method for the healthcare sector to identify and monitor its information security risks. The method is not limited to one individual organisation; it is based on the concept that all healthcare organisations experience similar risks and could benefit from the knowledge that exists in the collective, in order to take effective security measures. The aim is to reach a collective state of information security: a state where we (as patients, as voters, as tax payers, as healthcare consumers, as family and friends of patients) have trust in the level of respect, protection and quality of care that our information receives from the people and organisations that we share it with. HI-risk is aimed at healthcare organisations in general –the scope is not limited to primary or secondary care, private or national healthcare-, and includes technical, environmental, and social (human, organisational and societal) risk factors.

When there is an issue with our trust, caused by uncertainty about the level of respect, protection and quality of care that our information -in electronic or other form- receives, there is a security incident. According to the international standard BS ISO 31000:2009, the likelihood of occurrence of an incident, combined with the consequences of a certain event, is called a risk.

To describe a risk, it is therefore necessary to know the possible events. The HI-risk method provides the opportunity for participating organisations to register their incidents in a central database. From this database, an analysis of the incident scenarios can visualise the most frequent scenarios. These scenarios are presented to a group of experts in the field: security experts, information governance functions, risk managers, and so on. These experts can express their opinions about the expected frequency of occurrence for the future. Their expectation is based on their experience, their knowledge of countermeasures being taken, and their insight into new potential threats. The combination of incident knowledge from the past and expert expectations for the future forms a risk map. The map is the main deliverable of the HI-risk method, and healthcare organisations can use that to monitor their information security risks. The map changes constantly, as incidents occur every day and every entry in the register changes the frequencies in the database. This ‘living’ map provides a well-informed overview of the state of information security in healthcare.

The method differs from other method such as CRAMM and OCTAVE (Table 5.1). The biggest difference is that HI-risk does not start with context identification. The context includes all systems, people, processes, environments and wider contexts thinkable. The scope is indefinite; everything related to healthcare should be able to contribute knowledge to this method.

Table 5.1 HI-risk compared to other methods

BS ISO 31000:2009	OCTAVE	CRAMM	HI-risk
1. Context identification: a description of the subject for analysis, i.e. the analysed system and its environment.	Create threat profile	Asset identification	Not applicable: context is indefinite
2. Risk identification: identify what could possibly happen.	Threat and vulnerability identification	Asset valuation Threat and vulnerability assessment	Register incident data Expert elicitation Risk map
3. Analyse risks: identify and evaluate existing controls and consideration of the consequences and the likelihood.			The consequences and likelihood evaluation are part of the expert consultation. Furthermore countermeasures taken by the collective will lower the number of incidents and thus lowers the risk likelihood automatically.
4. Risk evaluation: relating the resulting risk level with risk acceptance criteria.			This step can be added to HI-risk. The decision to accept or not accept a risk could be made by the collective or by an individual organisation.
5. Risk treatment: identification and assessment of treatment options.	Develop protection strategy	Countermeasure selection and recommendation	This step can be added to HI-risk or be left to the participants. Risk solutions can be left to emerge from the collective or could be created collectively. The use of standards and checklist could be helpful, but they limit the creativity and innovativity of possible solutions.

Furthermore, as was argued in the background chapter and the literature review, controls against risks can either emerge by themselves or could be enforced. Selecting controls to treat risks is therefore not a necessary step of risk analysis, the treatment of risks should be left to the individuals within the collective. The use of best practices and standards might inspire some solutions, but these only deal with the threats which are known. “Risk is unknowable” (Parker, 1998 p. 500), and the unpredictability of new threats makes it impossible to have all the answers included in an existing checklist. It is therefore best to leave controls to emerge from the practice.

Three main processes form the method: a collective information security incident registration process, scenario analysis and expert consultations, as shown in Figure 5-1. The next sections of this chapter detail how these processes were developed.

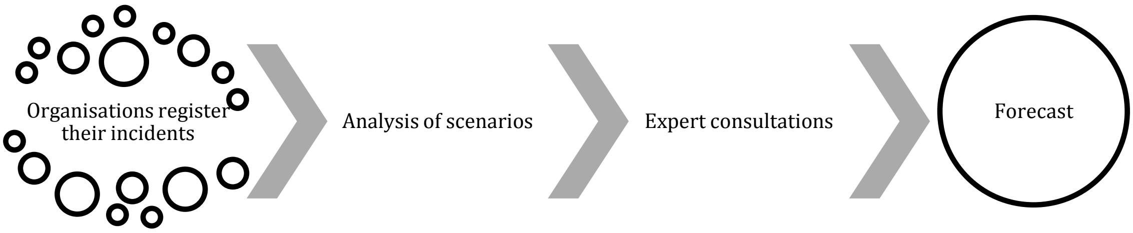


Figure 5-1 HI-risk process

5.4 Collective register of information security incidents

The first part of the HI-risk method is a collective information security incident register. Incident data from a group of participating organisations within a network (such as within one supply chain, a geographic region, a conglomeration of organisations reporting to one board, and so on) is logged according to a standardised terminology and structure. This structure is the classification of information security elements. The classification was developed specifically for the HI-risk method, as (to best of the researcher’s knowledge) no commonly accepted classification or taxonomy for healthcare information security risks was available.

A taxonomy is a system for naming and organising things into groups that share similar characteristics. When creating taxonomies, certain criteria need to be met. In the biological and library sciences, taxonomy development is a long-term, collaborative effort involving classification specialists. Taxonomies evolve slowly through a consensus process that involves representatives from multiple public and private sector organizations. A classification of information security incidents "must be comprehensible to both security experts and to those less familiar with security" (Lough, 2001, p. 39). Furthermore, the classification must be complete, so that every factor that contributes to the incident must fit somewhere in the structure. Amoroso (1994) states that classifications should have categories with the following characteristics:

- **Mutually exclusive** – classifying in one category excludes all others because categories do not overlap.
- **Exhaustive** – taken together, the categories include all possibilities.
- **Unambiguous** – clear and precise so that classification is not uncertain, regardless of who is classifying.
- **Repeatable** – repeated applications result in the same classification, regardless of who is classifying.
- **Accepted** – logical and intuitive so that categories could become generally approved.
- **Useful** – could be used to gain insight into the field of inquiry.

Throughout the course of the research, the classification of the HI-risk method was compared several times with these criteria, bearing in mind that any classification is an approximation of reality and should be expected to fall short in some characteristics. This may be particularly the case when the characteristics of the data being classified are imprecise and uncertain (Howard & Longstaff, 1998), as is the case for the typical information security information. The results of these comparisons are described in section 7.4.1 of this thesis.

To develop the taxonomy, it was first investigated which categories needed to be included. Taxonomies that were "presented in the past have a common set of categories" (Lough, 2001 p. 236) and these were reused in the HI-risk classification. The key categories often used in other information security classifications are **threat**, **vulnerability** and **risk**. These categories are different concepts and each of them can have its own taxonomy of sub-categories and variables.

The ISO/IEC 13335-1:2004 defines **threat** as a potential cause of an unwanted incident which may result in harm to a system or an organisation. A **vulnerability** is defined as a weakness of an asset or group of assets that can be exploited by one or more threats. In this vision, one or more threats could lead to an exploitation of one or more vulnerabilities. This suggest that a **risk** is caused by a scenario of one or more threats, exploiting one or more vulnerabilities, leads to one or more events that could harm one or more systems, assets or organisations.

The required categories depend on the definition of what is an information security risk. As stated before, a risk is the combination of some incidents that lead some damage. Together, the categories in the classification should represent a risk scenario. A risk scenario is the expected frequency of occurrence of a situation where one or more THREAT agent(s) perform(s) one or more METHOD(S) to exploit one or more WEAKNESS(ES) that cause(s) one or more undesirable EVENT(S), leading to DAMAGE.

Thus, the categories required for the classification are threat, method, weakness (or vulnerability or flaw), event and damage. Many existing information security taxonomies specify one or more of these categories.

Publications which attempt to classify computer security threats and vulnerabilities started to appear in the 1970s (Abbott et al., 1976; Anderson, 1972; Lackey, 1974; Neumann, 1978). These classifications served as system design requirements and it was believed that it was better to solve security issues during the design stage than afterwards. Authors like Howard & Longstaff (1998), Krsul (1998) and Lough (2001) reviewed some pioneering classifications and used them to create new ones. Many others have performed similar reviews. Table 5.2 shows several of these published taxonomies and classifications from different authors over time. These classifications tend to focus on a specific system, a specific type of event or a technology. Many of these taxonomies were designed for a specific operating system, for software, focus on only vulnerabilities or only on threats, or do not take human and procedural elements into account. This makes many of them incomplete to use in a socio-technical model. Furthermore, the limited focus on only vulnerabilities or threats does not match the definition of a risk in this thesis.

Table 5.2 Overview of security taxonomies

Year	Author	Type of taxonomy
1972	Anderson	Threats and vulnerabilities
1974	Lackey	Threats
	McPhee	Integrity flaws in operating system
1975	Saltzer & Schroeder	Vulnerabilities
	Parker	Functional vulnerabilities
1976	RISOS study	Vulnerabilities in operating systems
	Attanasio	IBM VM/370 OS flaws
	Nielsen (SRI)	Breaching incidents
1978	Bisbey & Hollingsworth	Protection analysis taxonomy
	Peter Neumann	Categories of flaws
1984	Perry & Wallich	Types of computer crimes
	Straub & Widom	Motivations of attackers
1988	Hogan	Operating systems
	Rissenbatt	Network communication vulnerabilities
1989	Neumann & Parker	Computer misuse techniques
1990	Beizer	Bug taxonomy
	Brian Marick	Defect classification
1991	Russell & Gangemi	Vulnerabilities and threats to computer security
1992	Spafford	Common system vulnerabilities
1994	Cheswick & Bellovin	Firewalls and Internet security
	Landwehr, Bull, McDermott, Choi	Computer program security flaws
	Syverson	Replay attacks in cryptoprotocols
1995	Icove et al.	Computer crimes and computer criminals
	Dunnigan & Nofi	Deception techniques
	Aslam	Security faults in the Unix operating system
	Bishop	UNIX system and network vulnerabilities
	Brinkley & Schell	Types of computer misuses
	Kumar	IDS attack signatures
	Gritzalis	Flaws in cryptographic protocols
	Stallings	Network security
1996	Cohen	Internet holes, attacks
1997	Lindqvist & Jonsson	System intrusions
	Du and Mathur	Software errors that led to security breaches
	Cohen	Attacks against information systems
	Jayaram & Morse	Security threats to networks
1998	Howard & Longstaff	Incident taxonomy with events & attacks
	Krsul	Software vulnerability analysis
1999	Asaro, Herting, Roth, and Barnes	Confidentiality breaches in EMR systems
	Bishop	Vulnerability classification
	Ristenbatt	Network vulnerabilities
2000	Mostow, Bott	Internet attacks
2001	Man, Wei	Attacks against mobile agents
	Lough	Taxonomy of attacks in wireless

Year	Author	Type of taxonomy
		networks
	Richardson	Vulnerabilities to support denial of service attacks
2002	Piessens	Taxonomy of Internet software vulnerabilities
	Jiwnani	Maintaining software with a security perspective
	Wood, Stankovic	DoS attacks in WSNs
2003	Cheswick	Attack classes
	Welch, Lathrop	Threat taxonomy
	Kamara et al	Vulnerabilities in firewalls
	Gray	Vulnerability taxonomy
	Hussain et al	DoS attacks taxonomy
	Alvarez, Petrovic	Web attacks taxonomy
2004	Hoglund	Software problems
	Delooze	Internet attacks
	Golle et al.	Attacks in VANETS
	Arce	Shellcode attacks
	Brann and Mattson	Typology of confidentiality breaches in healthcare
	Jiwnani, Zelkowitz	Taxonomy for auditing software
	Pothamsetty, Akyol	Protocol vulnerabilities
	Yongzheng, Xiochun	Privilege vulnerabilities
	Langweg	A classification of malicious software attacks
	Newsome et al	Sybil attacks in WSNs
	Killourhy et al	Categories of anomaly in IDS
	Mirkovic, Reiher	DDos Attack and defense mechanisms
2005	Christey	Vulnerabilities
	Weber	A software flaw taxonomy: aiming tools at security
	Tsipenyuk	A taxonomy of software security errors
	Hansman, Hunt	Taxonomy of attacks
2006	Kjaerland	Taxonomy of attacks
	Seifert, Welck, Komisarczuk	Taxonomy of honeypots
2007	Bazaz & Arthur	Vulnerabilities
2008	Myers	Confidentiality breaches
2010	Verizon incident sharing framework (Veris)	Incident classification
2010	Samy, Ahmad & Ismail	Threat categories in healthcare information systems
2011	ISO 27005	List of consequences, threats, vulnerabilities

One taxonomy that was reused was the incident taxonomy of Howard and Longstaff (1998). They reviewed many computer and network incident taxonomies and divided the different approaches into six categories: lists of terms, lists of categories, results categories, empirical lists, matrices and action-based taxonomies. They concluded that none of these approaches provide a common language to combine or compare security information. In their project, which was funded by the Sandia National Laboraties and the CERT Coordination Centre, they created a taxonomy for security incidents that combined of several matrices. In their taxonomy, an incident entails a combination of an attacker, an attack, an event and objectives. This taxonomy, copied in Table 5.3, formed the basis for the CERT incident database. Its strength to re-use it in HI-risk is the formula behind the formation of the columns: an incidents is triggered by and attacker to reach a certain objective. The attack is made up of tools, vulnerabilities, events and an unauthorised result. Its weakness is that its focus is on computer systems, and there are no categories for social or environmental events. This weakness was identified by Howard himself: in his Ph.D. thesis (Howard, 1997) which formed the foundation of this taxonomy, where he identifies the lack of human risk factors such as professionalism, behaviour, error, motives and commitment. Another weakness is the limited description of unauthorised results, or damage category.

Table 5.3 Computer and Network incident taxonomy (Howard & Longstaff, 1998)

Incident						
	Attack(s)					
			Event			
Attackers	Tool	Vulnerability	Action	Target	Unauthorized result	Objectives
Hackers	Physical attack	Design	Probe	Account	Increased access	Challenge, status, thrill
Spies	Information exchange	Implementation	Scan	Process	Disclosure of information	Political gain
Terrorists	User command	Configuration	Flood	Data	Corruption of information	Financial gain
Corporate raiders	Script or program		Authenticate	Component	Denial of service	Damage
Professional criminals	Autonomous agent		Bypass	Computer	Theft or resources	
Vandals	Toolkit		Spoof	Network		
Voyeurs	Distributed tool		Read	Internetwork		
	Data tap		Copy			
			Steal			
			Modify			
			Delete			

Parker’s (1998) proposed framework for information security expands on the ‘unauthorised result’ column of Howard and Longstaff. Parker calls this “potential information losses” (p. 242) and lists the following categories:

1. Availability and utility losses
    a. Destroy, damage, or contaminate
    b. Deny, prolong, accelerate, or delay use or acquisition
    c. Move or misplace
    d. Convert or obscure
2. Integrity and authenticity losses
    a. Insert, use, or produce false or unacceptable data
    b. Modify, replace, remove, append, aggregate, separate, or reorder
    c. Misrepresent
    d. Repudiate (reject as untrue)
    e. Misuse or final to use as required
3. Confidentiality and possession losses
    a. Locate
    b. Disclose
    c. Observe or monitor and acquire
    d. Copy
    e. Take or control
    f. Claim ownership or custodianship
    g. Infer
4. Other losses
    a. Endanger by exposing to any of the other losses
    b. Failure to engage in or allow any of the other losses to occur when instructed to do so.

Human risk factors are related to human errors and many publications exist in this area, such as Baysari, Mcintosh and Wilson (2008), Cosby (2003), Hollnagel (1998), Reason (1990), and Shorrock and Kirwan (2002).

Liginlal, Sim and Khansa (2009) analysed publicly reported privacy breach incidents and derived a human error taxonomy of privacy breach incidents and their causes. They divided the main types of incidents into two categories: human error and malicious acts. Within these categories were two possible sources of error: IT-enabled or manual processes. This led to a list of eight leading causes of breaches.

Table 5.4 Taxonomy of human error (Liginlal et al., 2009)

Breach type	Source of error	Leading cause of breach
Human error	IT-enabled process Manual process	1. Lost computer equipment 2. Inappropriate skill in using IT 3. Insufficient monitoring 4. Improper disposal of documents 5. User entry errors
Malicious acts	IT-enabled process Manual process	6. Internet threats, attack, or hack 7. Employee manipulation and malfeasance 8. Unauthorised access

A number of taxonomies that focus on information security within healthcare have also been reused. Asaro et al. (1999) organised a collection of indicators from scenarios of confidentiality breaches in the form of a taxonomic tree. The indicators help to determine the information needs for audit trail generation and analysis by giving an overview of the information that is likely to be targeted in the record and the motivation of the attacker. The tree represents two paths of indicators: the motivational indicators based on the relationship between the patient and the user (or the breacher of the confidentiality), and indicators within the system such as unexpected number of patients accessed. The user-patient relationship types that are identified are: familial, employment, friend/neighbour, adversarial legal, professional or other. These types of relationship explain motivations to access a patient’s record and are useful to identify potential risk factors related to people and social circumstances. Asaro et al. also identified information elements that could be targeted. These are listed in Figure 5-2.

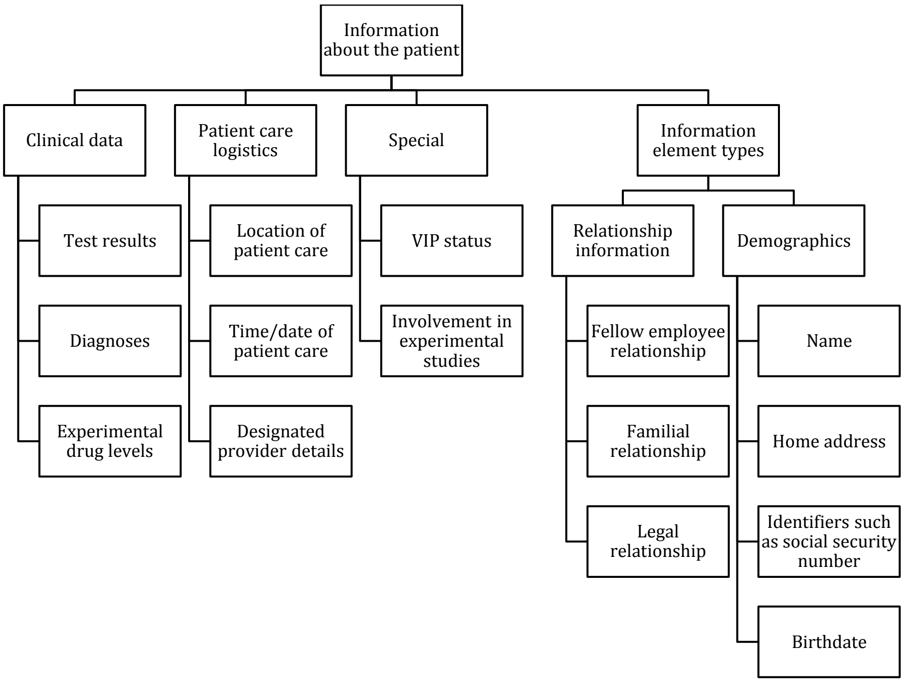


Figure 5-2 Information elements, based on Asaro et al. (1999)

Brann and Mattson (2004) created a typology of confidentiality breaches during conversations, based on interviews with 51 patients and observations of the behaviour and actions of healthcare providers. Patients gave their definitions and experiences concerning confidentiality within the hospital of study. Observations of the behaviour of staff resulted in additional experiences, which were all combined in a typology. This typology was later expanded with written communication (Brann, 2007). The typology that emerged is purely based on human behaviour and verbal communication, and did not include electronic communication which makes this typology an interesting addition to the above mentioned taxonomies that focus mostly on computer technology based threats and vulnerabilities. The types of confidentiality breaches in healthcare communication that were found are illustrated in Table 5.5.

Table 5.5 Typology of confidentiality breaches (Brann & Mattson, 2004, 2007)

Theme	Type
Internal confidentiality breach	Informal conversations among health care providers about patient’s or co-worker’s health status Telephone conversations involving health care providers or insurance company representatives Communication between health care providers and patients overheard by another patient or provider reveals information to a patient about another patient Communication about a patient between a health care provider and a non-patient
External confidentiality breach	Sharing confidential information with family Sharing confidential information with friends
Accessibility to written communication	Leaving records, notes, forms available for others to peruse Disposal of client’s records in non-protected area

Carthey and Clarke (2010) wrote a guide for individuals and teams working to improve patient safety. The guide aims to build awareness of the importance of human factors in making changes to improve patient safety. In the guide, the conclusions of research in safety culture and human factors are brought together. Five elements of safety culture are indicated to be related to reduction of human errors:

1. Open culture: staff feel comfortable discussing patient safety incidents and raising safety issues with both colleagues and senior managers.
2. Just culture: Staff, patients and carers are treated fairly, with empathy and consideration when they have been involved in a patient safety incident or have raised a safety issue.
3. Reporting culture: staff have confidence in the local incident reporting system and use it to notify healthcare managers of incidents that are occurring, including near misses.
4. Learning culture: the organisation is committed to learn safety lessons, communicates them to colleagues and remembers them over time.
5. Informed culture: the organisation has learnt form past experience and has the ability to identify and mitigate future incidents because it learns from events that have already happened (for example incident reports and investigations).

Researchers have also created classifications of security behaviour (Schultz, 2002; Stanton, Stam, Mastrangelo, & Jolton, 2005). Surprisingly, the classical view of the technical inside and outside still persists in many of these approaches (Franqueira, van Cleeff, van Eck, & Wieringa, 2010). Classifications related to human behaviour and organisational culture frequently make a distinction between *insider behaviour* and *external attackers*. Illustrative of this is that it is frequently claimed that insiders are the biggest problems for information security (Baker et al., 2011; Baker, Hylender, & Valentine, 2008; BERR, 2008; Crinson, 2008; CSI, 2011; Franqueira et al., 2010; Libenson, 2007; Liginlal et al., 2009; Schultz, 2002; Verizon, 2012; Williams, 2008).

The decision to re-use elements of the models above was based on the goal of being as complete as possible for the description of socio-technical information security incident and risk scenarios in healthcare. In terms of the requirements of Amaroso (1994), as listed in section 5.4 and highlighted cursive in the text here, the classification must be *exhaustive*. The categories needed to be extended beyond threats and vulnerabilities, as a complete description of a risk also includes the actual events and damages. Social and environmental variables contributing to information security risks were included. On the other side, it was decided not to expand in detail on all possible computer vulnerabilities, as these can be very technical or system-specific. For this study, these types of vulnerabilities were not *useful*, however, in future studies it will be possible to add these to the classification without much effort.

Eventually, the 5 categories included in the HI-risk classification (threat, method, weakness, event and damage) were *repeated* as much as possible from existing classifications. A threat describes the initiator: the who or what started the incident, the where, and the why information was ‘attacked’ or targeted. The method describes the methods and techniques that are used to ‘attack’ information, or to cause an undesirable event. The weakness is the flaw or vulnerability in the security controls, procedures, or human nature; it is the weak spot that is being taken advantage of. The event is what goes wrong: the asset and the information items that are exposed or damaged. The damage category lists the negative outcome: the number of records affected, the quantitative value and qualitative description of the damage. These 5 main categories aim to be logical and intuitive, so that they can become *accepted*. The sub-categories within the 5 main categories are *mutually exclusive* and *unambiguous*; they should not overlap or cause confusion. The classification is presented in Table 5.6. The sub-categories and elements are filled with what was learned from the classifications reviewed in this chapter, the literature review in chapter 2 and 3 (as summarised in Table 3.2) and the lessons learned after the surveys, interviews and observations (as described in chapters 6 and 7).

Table 5.6 Classification of security risk and incident factors

Category	Sub-category	Element
THREAT		
Initiator	Person	Medical staff
		Financial administration staff
		Trainee
		Personal assistant
		Secretary
		Admin support
		Management/executive/board
		Technicians
		Cleaners
		IT staff
		Restaurant/catering staff
		Volunteers
		Other staff:…
		Unknown staff
		Employee in partner organisation or related healthcare provider
		Employee in third party supplier or contractor
		Ex-employee
		Patient
		Family or carer/representative of patient
		External group or activists
		Government/police
		Researcher
		Unknown
		Other person:
	Environmental element	Earthquake
		Weather related
		Fire
		Water
		Animals
		Unknown
		Other:….
	Social	Change in legislation
		Change in organisation/merger/acquisition
		Change in organisational policies
		Implementation of new infrastructure
		Implementation of new marketing medium
		New products or services developed
		New trends in society
		Social atmosphere within organisation
		Redundancies
		Regional crime levels
		National/regional security alert evel
		Other:…
	Asset	Building
		Hardware
		Software
		Resources (water, electricity,…)

Category	**Sub-category**	**Element**
		Communication assets
		Other:…..
Motive	Unintentional	No motive, unintentional action
	Intentional	Justice
		Satisfaction
		Resignation
		Knowledge
		Financial gain
		Emotional gain
		Political gain
		Covering up errors
		Convenience
		Thrill
		Status
		Challenge
		Unknown
		Other:…..
Location	Within premises	Reception
		Parking
		Public space
		Consultation room
		Corridor
		Cafeteria
		Ward
		Other:…
		Unspecified internal location
	Other location	At the patient's home/environment
		At the staff member's home/environment
		Public transport
		On the premises of other healthcare provider or related organisation
		In a public place
		Private transport
		Other:….
	Unknown	
Unknown		
METHOD		
Personal		Making a mistake
		Stealing
		Copying
		Unauthorised accessing
		Damaging, breaking
		Manipulating
		Abusing ICT facilities
		Inserting a script/program
		Libel
		Overhearing/eavesdropping
		Overseeing
		Intimidating/verbal threats
		Harassment
		Pressuring
		Falsification

Category	Sub-category	Element
		Offensive jokes, offensive language
		Personal comments about a person’s physical appearance or character
		Other:…
		Unknown
Physical		Burglary
		Robbing
		Hijacking
		Physical attack
		Natural disruption
		Other:…
		Unknown
Automated		Data tapping
		Toolkit
		Distributed tool
		Other:…..
		Unknown
Unknown		
WEAKNESS		
Human vulnerability	Procedure/policy not followed	Unattended asset or record
		Security facility not used
		Sharing of password or access token
		Sharing personal details when asking for IT support
		Unsecure disposal of data carrying assets
		Other procedure not followed:….
	Situational	Telephone conversation in public area
		Informal conversation in public area
		Untidiness
		Other:…
	Mistakes	Fax to wrong recipient
		Email recipient entry errors
		Data entry errors
		Hasty working
		Lack of skills/training
		Other:…
	Mental state	Emotions
		Mental workload
		Failing to take due care and attention
		Distractions
		Other:…
	Unknown	
Organisational vulnerability	Procedural	Paper record in internal post
		Paper record in external post
		Organisational changes, new procedures, routines
		Lack of internal control in procedure
		Security flaw in storage of data
		Insufficient supervision
		Lack of security in email application

Category	Sub-category	Element
		Flaws in settings in authorisations/privileges
		Lack of control of outsourcing partner
		Failure to implement timely measures of control
		Process design
		Relocation of activities to new site
	Cultural	Lack of learning culture: the organisation is not committed to learn lessons, to communicate them to colleagues and to remember them over time
		Social atmosphere within organisation
		Closed culture: staff not feeling comfortable discussing incidents and raising issues with both colleagues and senior managers
		Unjust culture: staff, patients and carers are not treated fairly, with empathy and consideration when they have been involved in an incident or have raised an issue
		Lack of reporting culture: staff have no confidence in the local incident reporting system and do not use it to notify healthcare managers of incidents that are occurring, including near misses
		Lack of informed culture: the organisation has not learned from past experience and has not the ability to identify and mitigate future incidents.
		Staff's job satisfaction
	Other: …..	
	Unknown	
Physical security vulnerability	Storage facility	Lack of lockable space
		Lack of secure filing cabinets
		Other:…..
	Transport	Transportation of media
		Transportation of paper records
		Other:…..
	Secure areas	Fax in unsecured environment
		Printer in unsecured environment
		Unsecured remote working environment
		Lack of visual control on entrance point
		Other:…..
	Maintenance	Lack of maintenance to building and facilities
		Clearance of a building
		Other:…
	Vulnerability in security facilities	Alarm system
		Windows
		Doors
		CCTV
		Guards not alert

Category	**Sub-category**	**Element**
		Unsecured entry points
		Other:…..
	Unknown	
Computer vulnerability		Design
		Implementation
		Configuration
		Website
		Maintenance
		Changes
		Equipment
		Other:…..
		Unknown
Unknown		
EVENT		
Confidentiality breach		Read/observe/hear personal data
		Copy personal data
		Disclose personal data
		Acquire personal data
		Locate personal data
		Other:…..
		Unknown
Availability breach		Data lost or gone missing
		Destroy data
		Damage data or facilities
		Delay process
		Data, notes or reports not available when needed
		Other:…..
		Unknown
Integrity breach		Insert false data, notes or reports
		Modify notes, data or reports
		Remove parts of data, notes or reports
Breach of ethical norms or code		Spreading illegal material
		Publication of harmful material
		Other:…
Affected asset	Affected data item	Patient identifiable information
		Clinical data
		Patient care logistics
		Payment details
		Insurance details
		Financial information
		Employee’s personal information
		Confidential research data
		Confidential organisational data
		Copyrighted data
		Data under embargo
		Medical recordings: illustrations, video, voice,

Category	**Sub-category**	**Element**
		scans, x-rays, photos, ultrasound picture
		Unknown
		Other:…
	Technology related asset	Application
		Server
		System
		Networks & Devices
		Other:…
	End user devices	Desktop
		Laptop
		Ipad/tablet
		Smart phone
		PDA
		Self-service kiosk
		Entry device/card reader
		Printer
		Scanner
		Copier
		Fax
		User authentication device
		Patient monitoring system
		Implant
		RFID chip
		Unknown
		Other:…
	Offline data	Backup tapes
		Disks/cd/dvd/stick
		Documents
		Hard disk
		Smartcard
		Unknown
		Other:…
	Facility	UPS
		Camera
		Physical barrier
		Security system
		Power infrastructure
		Unknown
		Other:…
Unknown		
DAMAGE		
Direct costs		Repair cost
		Mailing expenses
		Replacement costs
		Fines or penalties
		Legal costs
		Consultancy costs
		Research or investigation costs
		Call centre costs
		Unknown
		Other:…

Category	Sub-category	Element
Indirect costs		Embarrassment, awkwardness, anxiety or distress to the organisation or medical staff
		Embarrassment, awkwardness, anxiety or distress to the patient
		Affecting reputation of organisation or medical staff
		Patients opting for for other healthcare provider
		Loss of health or life of patient
		Discrimination
		Quality of care affected
		Compliance to regulation affected
		Tensions in work environment for medical staff
		New products or services stalled
		Other:….
		Unknown
Affected number of patients		0-9
		10-99
		100-999
		1,000-9,999
		>10,000
		Unknown
Unknown		

The classification was the first step in the design of a database that can hold all the incident data from the participating organisations. This database was created with Microsoft Office Access. All elements from the classifications are represented in the columns in the database. When information security incidents are registered in the database, it is possible to count frequency of occurrence of elements and frequency of co-occurrence of multiple elements.

5.5 Scenario analysis

Each incident is described as a scenario. The threat category is always the start of a scenario, followed by the used method that exploits a vulnerability or weakness. This all leads to an event that causes damage.

The concept of analysing a risk as a scenario is based on fault and attack trees, also referred to as cause-consequence diagrams (Nielsen, Platz & Runge, 1975). The advantage of trees is that for more complex situations they can be divided into sub-trees, which can also be reused in different situations. Fault trees have been used before, for the analysis of failure conditions of complex technical systems. Schneier was the first to associate the term ‘attack tree’ with the use of fault trees for attack modelling which made this approach more widely known (Schneier, 1999). It has since been used by Reddy et al. (2008) to analyse consumer information privacy, by Grunske and Joyce (2008) to predict security for component-based systems, and by Edge et al. (2007) to analyse the security of online banking systems.

Attack trees can capture the steps of an attack and their interdependencies. The idea is to build a graph to represent the decision-making process of attackers. The roots of the tree represent potential goals of an attacker. The leaves represent ways of achieving the goal. The main building blocks of attack trees are called nodes. The nodes are used to model steps of an attack, events or attacker actions. Each tree has a single top node, which represents the achievement of the attack's ultimate goal. The nodes under the root node are high-level ways in which a goal may be achieved. Child nodes represent attack steps that have to be performed successfully before another step can occur.

To facilitate the scenario analysis, the database of past incidents is copied to Excel. The COUNTIFS formula in Excel applies criteria to cells and counts the number of times all criteria are met. The syntax of that formula is:

COUNTIFS(criteria_range1, criterial1, [criteria_range2, criteria 2]…)

This formula allows counting the number of co-occurences of a selection of variables. In other words, this formula counts the number of times certain scenarios occurred. This generated an overview of the most frequent incident scenarios from the past.

The presentation of a scenario description can be graphically supported, as is done in other methods such as CORAS. This graphical presentation in tree maps has shown some positive contributions to the understanding of risks.

5.6 Expert elicitation

The second step in the HI-risk method is the consultation of a group of information security and healthcare experts by means of the Delphi method. The process consists of a number of rounds of questionnaires and an analysis of the results. After each round, the researcher provides an anonymous summary of the experts’ forecasts, as well as the comments that they provided with their judgements. Each expert may then revise their earlier answers in light of the replies of other members of the panel. It is believed that during this process the range of the answers will decrease, and the group will converge towards the ‘correct’ answer, as explained in more detail in the Methodology chapter.

The Delphi method was chosen over other methods for expert elicitation because of the multiple iterations and the convenience of the online survey possibility. This way, the experts did not have travel in order to meet physically, creating the possibility to create a panel that is not bound to geographic location.

In the first round, the experts are shown the most frequent incident scenarios and asked to indicate the expected frequency of occurrence in the future. This question is repeated in Rounds 2 and 3, with the addition of showing them the answers and comments made by the other experts. After three rounds, the combined opinion of expected frequency is considered to be the forecast. Furthermore, experts are given the opportunity to point out trends they see for future incidents.

The output of the Delphi study is combined with the most frequent scenarios from the incident database and presented on a risk map. This map is a graph with two dimensions: frequency of occurrence and severity of the damage (in number of affected patient records). The scenarios are positioned on this graph as a visualisation to support decision-makers in their decision which scenarios require action.

5.7 Risk monitoring

Risk monitoring is used to review the state of risk scenarios, to identify new risks and to assess the effectiveness of risk treatment. The risk map and the risk scenarios provide an overview for information security risk managers that can be used to compare the risk situation in an individual organisation with the situation in the network of organisations. Furthermore, it can be used to act quickly on new risk scenarios that occur in other organisations, in order to prevent them from happening in the own organisation.

The knowledge that is derived from the HI-risk method can also be used to create collective policy and measures of control. It supports the knowledge management and knowledge sharing of the participants and could improve the security of the collective of participating healthcare organisations.

5.8 Conclusion

This chapter described the HI-risk method. The first step in the method is the registration of information security incidents by a group of collaborating organisations. The register follows a classification that was created after studying existing models to describe risk factors. From the collective incident register, an overview of the most frequent scenarios is generated. The second step is the elicitation of expert knowledge in a three-round Delphi study. The panel judges the most frequent scenarios and estimate the possible future scenarios. The output of both steps is combined in a risk map.

The HI-risk method was put into action and evaluated in a case study. The next chapter (chapter 6) reports how the method was carried out and chapter 7 describes the results of the case study.

6 HI-risk method demonstration

6.1 Introduction

This chapter describes how the HI-risk method was performed by gathering incident data from healthcare organisations, scenario analysis and by the expert elicitation. The aim of this research step was to test the usability of the method and to deliver the main output of the method: the risk forecast.

The data to create the database was collected through a survey. After that, a Delphi study was carried out with a panel of 12 selected experts. During the registration of the collected incident data from the survey and the Delphi study, the usability and completeness of the classification were tested. It also showed if the categories were mutually exclusive, repeatable and unambiguous. The execution of the method resulted in additions and alterations to the classification. The survey data and the Delphi study results were combined to create the map of information security risks in healthcare. This map presents the most frequently expected information security risk scenarios.

6.2 Data collection for the incident database

Data was requested directly from NHS Health Boards and Care Trusts in Scotland (14) and England (149) through a FOI request, as discussed in the Methodology chapter. The list of organisations that were approached are listed in Appendix A. The responses were collected between September and March 2010. A total of 163 requests were sent and 132 replies were received (Table 6.1). As noted earlier, this means that a 81% response rate was received and this was considered satisfactory for the purposes of this study, and the remaining organisations were not chased for their reply. Two organisations replied that collecting the data for the answer would cost more than £600 and therefore included no response. The information about the incidents was copied into the incident database.

Table 6.1 Overview FOI responses

Number of sent FOI requests	163
Number of replies	132
Number of no replies	28
Undeliverable emails	3

The returned incident registers contained some narrative information about incidents and a basic categorisation of cause and location. The presentation of the information differed widely. Almost all of them were unique in their format and descriptions of incidents. Some respondents completed the provided spreadsheet, others sent a list generated from an IT service desk application or referred to their annual reports.

There appears to be no common approach to report and administer incidents, even though guidelines exist (Department of Health, 2010a). One observation was that the organisations that provided the highest numbers of incidents also recorded them with more detail and included near misses. This does not mean that they suffer from more incidents than others, it possibly means that these organisations experience a greater awareness and professionalism towards information security and therefore report higher numbers of incidents as they could be better in identifying and reporting them.

All usable replies were selected from the 132 organisations and the data was restructured into the HI-risk database. Eventually 2108 incidents from 83 organisations were added. Hundreds more incident descriptions could not be used; they were often too generic to be able to make an interpretation for the model.

6.2.1 Data analysis

The data in the incident database was analysed to discover patterns in co-occurrences of variables. The variables are nominal and qualitative, so it was not possible to perform advanced quantitative statistical analysis. It was possible to count frequencies of occurrence of individual variables. Counting the frequency of occurrences of a specific threat or specific vulnerability in an organisation's incident register gives some information about past incidents and could be used to make decisions about the implementation of security controls. An organisation could, for instance, decide to focus on process improvements and employee training to bring down the number of incidents caused by vulnerabilities such as human errors when handling personal data. Or they could decide to invest in physical security measures to prevent theft and damage if the frequency of thefts is high. Although this type of data is very basic, according to Hubbard (2010), it still can help to make potentially good decisions, because the decisions would be based on structured data, which is better than no data at all. Some examples of such basic statistics are shown in Figures 6-1 to 6-4.

Figure 6-1 shows the number of incident and the number of patient records that were affected. The figure visualises the fact that most incidents impact a low number of patients. It also shows that the higher the number of affected records, the lower the frequency of occurrence. Only 3 large-scale incidents occurred.

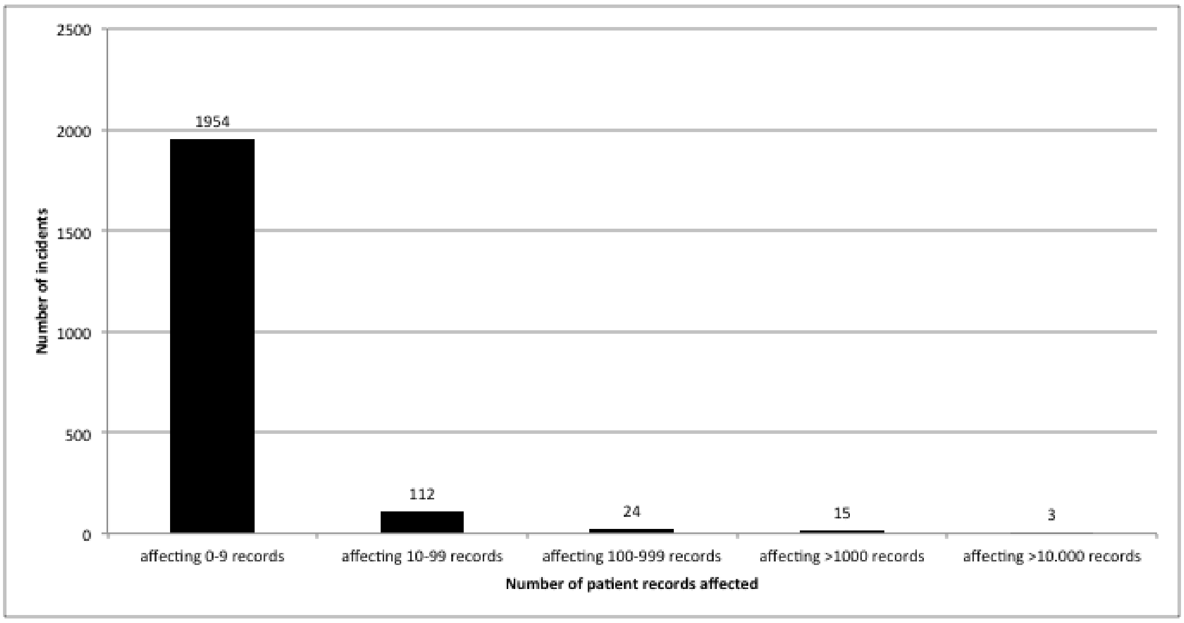


Figure 6-1 Number of incidents and damage

Another example in Figure 6-2 shows the types of threat initiators that were registered. It shows that staff were the main initiator of incidents, but that a large amount of incidents were triggered by unknown causes. Not knowing the cause of incidents is deemed problematic, as this information is needed to decide which countermeasures to implement.

The list of occurred vulnerabilities is shown in Figure 6-3. This graph shows again that there are many unknown factors. Furthermore, it shows that leaving assets unattended is by far the most frequently registered factor in information security incidents.

In Figure 6-4 the affected assets are shown. It shows that paper records are the third most frequently affected asset during information security incidents.

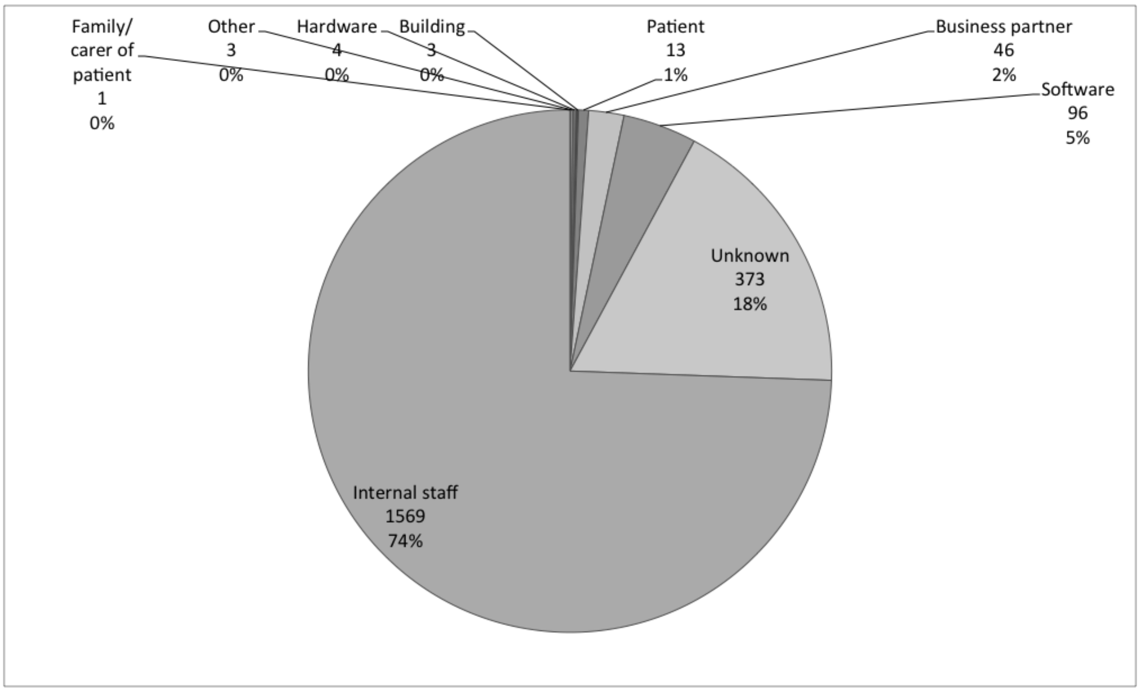


Figure 6-2 Number of incidents per threat initiator

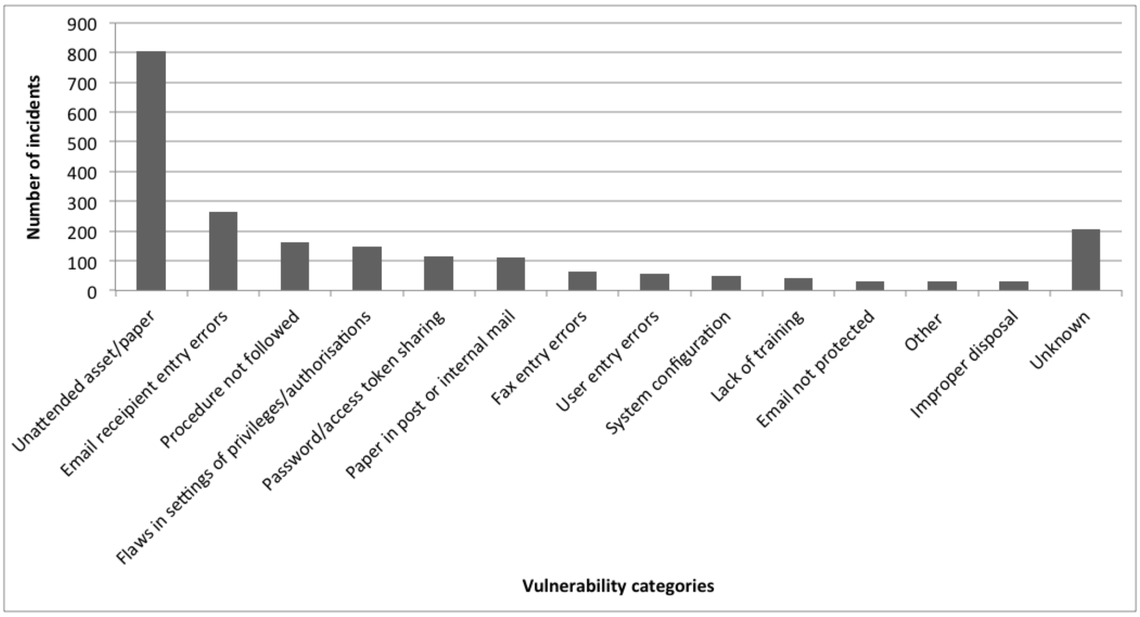


Figure 6-3 Vulnerabilities

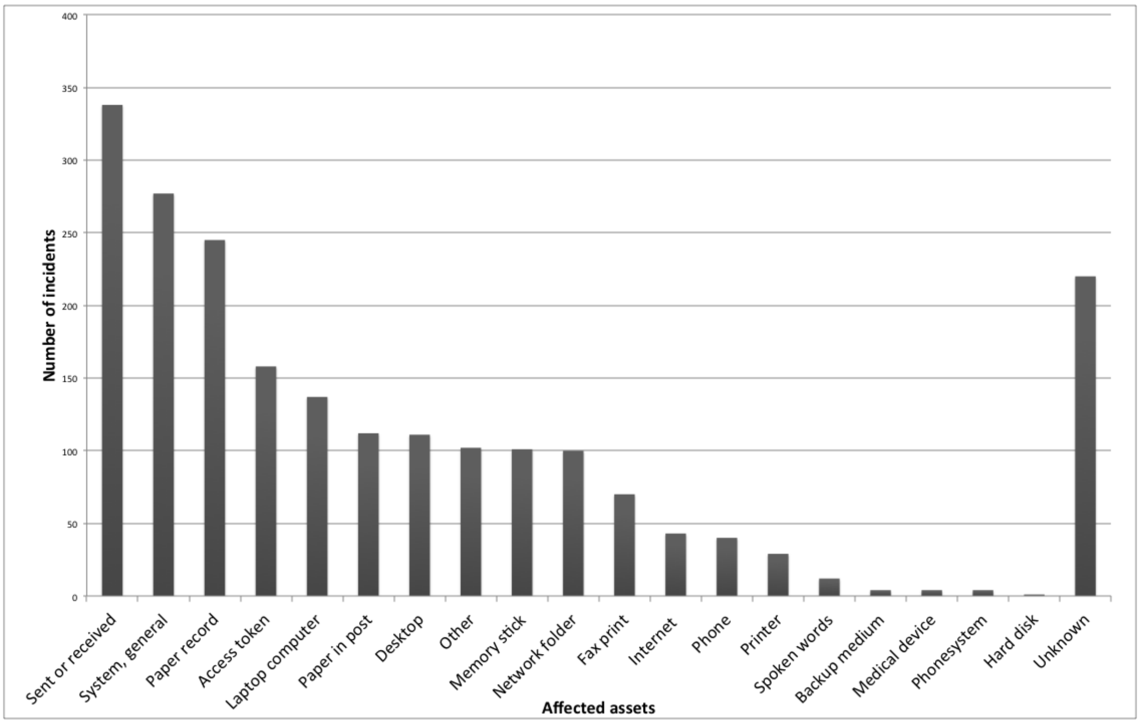


Figure 6-4 Affected assets

One research hurdle appeared with the data. The quality of the data in the database was limited, causing limitations to the analysis. During the data entry, it appeared that the classification itself and the responses to the FOI requests showed some weaknesses:

1. Only nine elements of the threat category *initiator* appeared in the incident register.
2. The respondents did not report the *motivations* of the initiator. It was not reported what initiators wanted to achieve, what their relationship was and what kind of attacker they were.
3. The list of *vulnerabilities* turned out to be too detailed for this exercise. The description of the incidents was too abstract to use all of the elements. Therefore, only the sub-categories could be used for the test.
4. The majority of the respondents did not report the *damage* that was suffered from incidents.

The survey data also added value to the classification and some adjustments were made:

1. The location of the incident was registered in most cases. During the analysis, it became clear that additional elements needed to be added to the list of possible locations. Incidents also occur at home with the patient or staff.
2. From the list of affected assets only a few seemed to occur. Two devices were added: medical devices and phone system/switchboard (including answering machines).
3. A new sub-category was added to the list of possible damage. Almost all organisations registered the number of patient records affected to the breach and adding this number to the register provides for an indication of the severity of the incidents. This suggests that healthcare organisations find this number important to register.

The HI-risk approach is looking for patterns beyond the basic statistics, in the form of scenarios. These scenarios show the combinations of variables that occur together during an incident. The data is analysed for the number of times certain variables occur together in a scenario, leading to an overview of most frequent scenarios (Appendix B). This way, 181 unique scenarios were distilled from the 2108 incidents. The top 5 most frequently occurring scenarios and the most damaging scenario (scenario 6) were used in the next research step, to ask experts for their opinion about how these most frequent scenarios from the past could serve as an indicator for future risks. These scenarios are illustrated in Figure 6-5 and 6-6. The scenarios can be described as follows:

Scenario 1: Email to unauthorised recipient.

Ten out of 100 incidents (10% of past incidents) involve an internal employee located on the premises who sends an email which includes patient-identifiable data, to a recipient who is not authorised to see that data and consequently discloses the personal details of a few patients (less than 10 patients).

Scenario 2. Unattended asset goes missing.

Nine out of 100 of the incidents (9% of past incidents) involve an internal employee located on the premises leaving an asset unattended and consequently the asset goes missing. The asset contained personal information of a few patients (less than 10).

Scenario 3. Wrong privileges set.

Six out of 100 incidents (6% of past incidents) involved an internal employee on the premises who unintentionally was given the wrong privileges or authorisations, causing disclosure of personal patient information to unauthorised persons.

Scenario 4. Password or access token sharing.

Five out of 100 incidents (5% of past incidents) involve an internal employee sharing his password or access token leading to disclosure of patient information to unauthorised persons.

Scenario 5. Procedure not followed.

Four out of 100 incidents (4% of past incidents) involve an internal employee located on the premises who does not follow the formal procedures leading to disclosure of patient information.

Scenario 6. More than 10,000 patient records affected.

A few (0.14%) of the past incidents involved the loss or destruction of data on a portable (backup) medium, affecting more than 10,000 patient records.

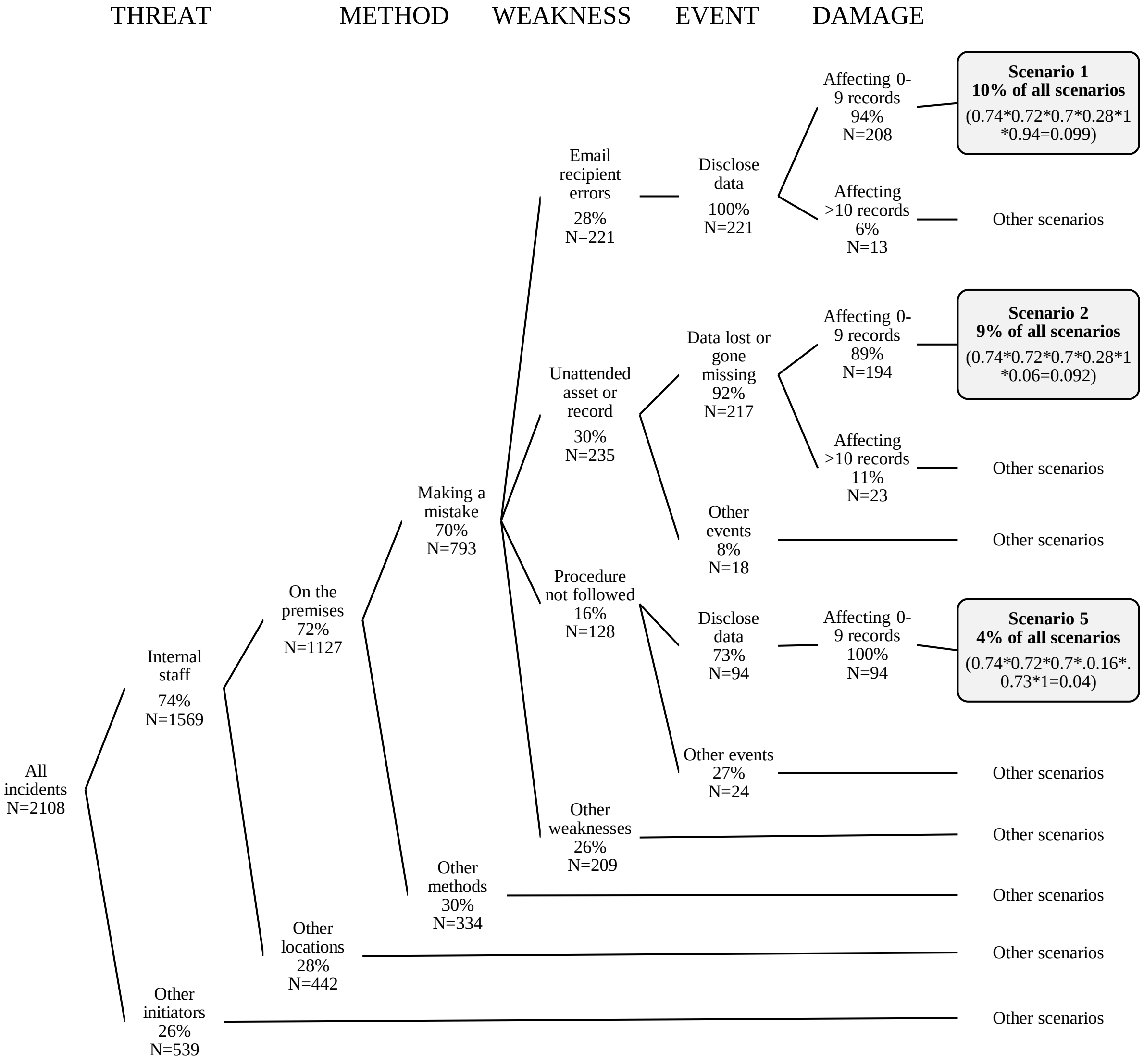


Figure 6-5 Mistake scenarios tree

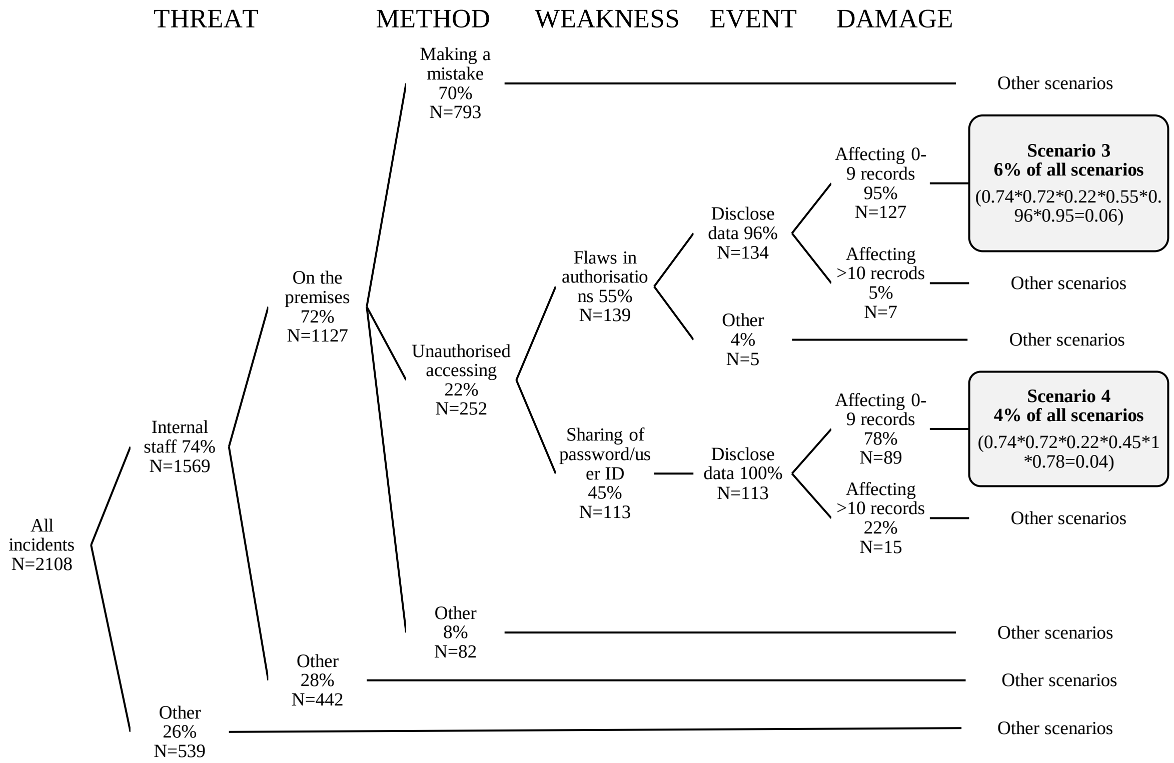


Figure 6-6 Unauthorised access scenarios tree

6.3 Expert elicitation

The scenarios presented in the previous section were useful to learn about past incidents, and they were then used as input for an expert panel to judge the expected frequency of occurrence in the near future. The experts' opinions were gathered with a three-round Delphi study. The approach and rationale behind the Delphi method was explained in chapter 4 of this thesis. In this section, the result of the Delphi study is presented. A shorter version of this section has been published in the peer-reviewed journal Computers & Security (Van Deursen, Buchanan and Duff, 2013).

The results are presented in four different ways: a narrative (section 6.3.2); in box-and-whisker plots (Figure 6-7 to 6-25); by means of descriptive statistics (Table 6.2); and in a table showing the consensus per round (Table 6.3). For each individual scenario, a narrative about the expert's opinions on the scenario is presented from section 6.3.2 onwards. The aim is to investigate the reason behind outlying estimations and to analyse alternative views on the scenarios. The comments give valuable information about the rationale behind outlying scores. Where the opinions were very diverse and there were not enough consensuses to define a group judgement, the comments were analysed for possible explanations of the diversity. Equally, outlying opinions were analysed. The spread of opinions is visualised graphically in a box and whisker plot by showing the interquartile range (the range that contains the answers of the middle 50 percent of the respondents). These diagrams have a box showing the range from the first to third quartiles, and the median divides this large box into two boxes for the second and third quartiles. The whiskers span the first quartile, from the second quartile box down to the minimum, and the fourth quartile, from the third quartile box up to the maximum. The median is indicated with a diamond. These figures are included in the next sections with the scenario discussions.

6.3.1 Descriptive statistics

The descriptive statistics of the expected frequency of occurrence for the most important scenarios are shown in Table 6-2. The table shows the 19 scenarios that were evaluated by the experts, as was described in section 4.4.3 of this thesis. These include the 6 scenarios presented to the experts in Round 1 and the 13 scenarios that were created by the experts in the blank sheet. The statistics include mean, median, range and standard deviation of their judgements. The final group judgement is based on the median rather than the mean, since single extreme answers can 'pull' the mean unrealistically (Gordon, 1994 p. 9). Furthermore, when the distribution of the frequencies for some scenarios differ highly, the median is a more stable figure than the mean (Armitage, Berry, & Matthews, 2002). These statistics show that the experts estimated that scenario 2, staff sharing passwords or access tokens, is the most likely event to occur in the near future. The median of that scenario is 8.9, which means that the experts predict that almost 9% of all future incidents will fit into this scenario.

Table 6.2 Expected frequency of occurrence per scenario per round

	Round 1	**Round 2**	**Round 3**
Scenario 1 Unattended asset or record goes missing			
Median	5.0	4.5	5.0
Range	20	9.5	5.5
Largest	20	10	8
Smallest	0	0.5	2.5
Mean	6.1	4.6	4.9
St Dev	5.5	3.6	1.36
Number of experts (N)	12	10	10
Scenario 2 Password or access token sharing			
Median	5.0	8.9	8.9
Range	29.9	29.5	5.0
Largest	30.0	30	10
Smallest	0.1	0.5	5
Mean	7.7	11.3	8.1
St Dev	9.3	8.5	2.12

	Round 1	**Round 2**	**Round 3**
Number of experts (N)	12	10	10
Scenario 3 Email to wrong recipient			
Median	2.3	3.0	3.0
Range	9.9	4.5	5.0
Largest	10.0	5	5
Smallest	0.1	0.5	0
Mean	4.2	3.1	2.8
St Dev	3.8	1.9	1.27
Number of experts (N)	12	10	10
Scenario 4 Theft from the premises (blank sheet scenario)			
Median	7.5	5.0	5.0
Range	0.0	9.9	8.0
Largest	7.5	10	10
Smallest	7.5	0.1	2
Mean	7.5	3.7	5.0
St Dev	-	3.2	2.18
Number of experts (N)	1	9	10
Scenario 5 Procedure not followed			
Median	4.0	3.5	4.5
Range	9.9	9.5	6.8
Largest	10.0	10.0	8.8
Smallest	0.1	0.5	2
Mean	4.4	4.3	4.3
St Dev	3.9	3.4	2.11
Number of experts (N)	12	10	10
Scenario 6 Wrong privileges set			
Median	1.7	2.3	2.5
Range	14.8	8.5	2.5
Largest	15.0	9.0	4.0
Smallest	0.2	0.5	1.5
Mean	3.7	3.0	2.8
St Dev	4.4	2.6	0.8
Number of experts (N)	12	10	10
Scenario 7 High impact mistakes (blank sheet scenario)			
Median	5.3	3.5	2.8
Range	4.5	20	4
Largest	8	20	5
Smallest	3	0	1
Mean	5.3	4.7	2.9
St Dev	3.18	6.10	1.15
Number of experts (N)	2	9	10
Scenario 8 Working in a public place (blank sheet scenario)			
Median	7.5	2.0	2.5
Range	0	9.9	1
Largest	8	10	3
Smallest	8	0	2
Mean	7.5	3.6	2.4
St Dev	-	3.77	0.42
Number of experts (N)	1	9	5
Scenario 9 Unsecure remote 3rd party (blank sheet scenario)			
Median	7.5	2.5	2.3

	Round 1	**Round 2**	**Round 3**
Range	0	6	2.5
Largest	8	6	3
Smallest	8	0	1
Mean	7.5	2.8	2.0
St Dev	-	2.42	0.83
Number of experts (N)	1	9	10
Scenario 10 Transportation of data (blank sheet scenario)			
Median	0.8	0.7	1.0
Range	0	1	5.8
Largest	1	1	7
Smallest	1	0	1
Mean	0.8	0.6	2.0
St Dev	-	0.38	2.51
Number of experts (N)	1	6	5
Scenario 11 Family of patient (blank sheet scenario)			
Median	0.8	0.6	1.0
Range	0	1	9.5
Largest	1	1	10
Smallest	1	0	1
Mean	0.8	0.5	2.6
St Dev	-	0.53	4.14
Number of experts (N)	1	6	5
Scenario 12 Backup medium goes missing			
Median	0.4	1.0	0.8
Range	9.9	5.9	0.9
Largest	10	6	1
Smallest	0	0	0
Mean	1.4	1.6	0.7
St Dev	2.78	1.91	0.38
Number of experts (N)	12	9	5
Scenario 13 Improper disposal (blank sheet scenario)			
Median	0.8	0.5	0.9
Range	0	1	1.5
Largest	1	1	2
Smallest	1	0	1
Mean	0.8	0.5	0.9
St Dev	-	0.55	0.46
Number of experts (N)	1	6	10
Scenario 14 Third party discloses data (blank sheet scenario)			
Median	0.3	0.5	0.5
Range	0.5	0.7	2.3
Largest	1	1	3
Smallest	0	0	0
Mean	0.5	0.6	0.8
St Dev	0.29	0.29	0.65
Number of experts (N)	3	9	10
Scenario 15 Unsecured remote working (blank sheet scenario)			
Median	0.8	0.5	0.5
Range	0	4.95	0.7
Largest	1	5	1
Smallest	1	0	0

	Round 1	**Round 2**	**Round 3**
Mean	0.8	1.5	0.6
St Dev	-	2.08	0.26
Number of experts (N)	1	9	5
Scenario 16 External groups (blank sheet scenario)			
Median	0.6	0.4	0.5
Range	0.5	1	0.8
Largest	1	1	1
Smallest	0	0	0
Mean	0.6	0.3	0.5
St Dev	0.35	0.33	0.32
Number of experts (N)	2	9	5
Scenario 17 Trainee breaching confidentiality (blank sheet scenario)			
Median	3.0	0.3	0.5
Range	0	2	1
Largest	3	2	1
Smallest	3	0	0
Mean	3.0	0.5	0.5
St Dev	-	0.77	0.35
Number of experts (N)	1	6	5
Scenario 18 Breach at the patient home (blank sheet scenario)			
Median	7.5	0.2	0.2
Range	0	5	0.8
Largest	8	5	1
Smallest	8	0	0
Mean	7.5	1.3	0.4
St Dev	-	2.12	0.35
Number of experts (N)	1	9	5
Scenario 19 Covering up errors (blank sheet scenario)			
Median	0.8	0.3	0.2
Range	0	1	2.4
Largest	1	1	3
Smallest	1	0	0
Mean	0.8	0.4	0.7
St Dev	-	0.49	1.03
Number of experts (N)	1	6	5

Table 6.3 shows the level of consensus after grouping the individual responses into ordinal categories. When forecasting risks, it is not ideal to focus too much on the absolute numbers as it is generally not easy to forecast the exact number of times a risk materialises with the relative small amount of data that was gathered for this study. For that reason, the quantitative data is grouped into qualitative categories. These categories are presented as: very rarely (<0.5% of all incidents), rarely (0.5-1% of all incidents), sometimes (>1-5% of all incidents), frequently (>5-10% of all incidents) and very frequently (>10%). The underlying frequencies are not grouped into equal intervals, as this leads to many categories without cases in them. Therefore, intervals of unequal size

were chosen in a way that showed the optimal appearance, as suggested by Healey (2011).

Table 6.3 Consensus levels for frequency of occurrence

	Round 1		**Round 2**		**Round 3**	
	Frequency	Consensus	Frequency	Consensus	Frequency	Consensus
Scenario 1 Unattended asset or record goes missing						
Very rarely	2	17%	2	20%	0	
Rarely	0		1	10%	0	
Sometimes	5	42%	4	40%	9	90%
Frequently	4	33%	3	30%	1	10%
Very frequently	1	8%	0		0	
Scenario 2 Password or access token sharing						
Very rarely	2	17%	1	10%	0	
Rarely	3	25%	0		0	
Sometimes	1	8%	0		2	20%
Frequently	4	33%	6	60%	8	80%
Very frequently	2	17%	3	30%	0	
Scenario 3 Email to wrong recipient						
Very rarely	2	17%	1	10%	1	10%
Rarely	1	8%	2	20%	0	
Sometimes	5	42%	7	70%	9	90%
Frequently	4	33%	0		0	
Very frequently	0		0		0	
Scenario 4 Theft from the premises (blank sheet scenario)						
Very rarely	0		2	22%	0	
Rarely	0		1	11%	0	
Sometimes	0		5	56%	7	70%
Frequently	1		1	11%	3	30%
Very frequently	0		0		0	
Scenario 5 Procedure not followed						
Very rarely	3	25%	1	10%	0	
Rarely	2	17%	1	10%	0	
Sometimes	2	17%	5	50%	8	80%
Frequently	5	42%	3	30%	2	20%
Very frequently	0		0		0	
Scenario 6 Wrong privileges set						
Very rarely	3	33%	1	10%	0	
Rarely	3	25%	1	10%	0	
Sometimes	3	25%	6	60%	10	100%
Frequently	2	17%	2	20%	0	
Very frequently	1	8%	0		0	
Scenario 7 High impact mistakes (blank sheet scenario)						
Very rarely	0		2	22%	0	
Rarely	0		0		1	10%
Sometimes	1		6	67%	9	90%
Frequently	1		0		0	
Very frequently	0		1	11%	0	
Scenario 8 Working in a public place (blank sheet scenario)						
Very rarely	0		4	44%	0	
Rarely	0		0		0	

	Round 1		**Round 2**		**Round 3**	
	Frequency	Consensus	Frequency	Consensus	Frequency	Consensus
Sometimes	0		2	22%	5	100%
Frequently	1		3	33%	0	
Very frequently	0		0		0	
Scenario 9 Unsecure remote 3rd party (blank sheet scenario)						
Very rarely			2	22.22%	1	10%
Rarely			2	22.22%	2	20%
Sometimes			4	44.44%	7	70%
Frequently	1		1	11.11%	0	
Very frequently			0		0	
Scenario 10 Transportation of data (blank sheet scenario)						
Very rarely			3	50%		
Rarely	1		3	50%	4	80%
Sometimes						
Frequently					1	20%
Very frequently						
Scenario 11 Family of patient (blank sheet scenario)						
Very rarely			3	50%		
Rarely	1		3	50%	2	40%
Sometimes					2	40%
Frequently					1	20%
Very frequently						
Scenario 12 Backup medium goes missing						
Very rarely	7	58%	4	44.44%	2	40%
Rarely	3	25%	2	2.222%	3	60%
Sometimes	1	8%	2	2.222%	0	
Frequently	1	8%	1	11.11%	0	
Very frequently			0		0	
Scenario 13 Improper disposal (blank sheet scenario)						
Very rarely			3	50%	4	40%
Rarely	1		3	50%	5	50%
Sometimes			0		1	10%
Frequently			0			
Very frequently			0			
Scenario 14 Third party discloses data (blank sheet scenario)						
Very rarely	2		6	67%	7	70%
Rarely	1		3	33%	2	20%
Sometimes			0		1	10%
Frequently			0		0	
Very frequently			0		0	
Scenario 15 Unsecured remote working (blank sheet scenario)						
Very rarely			6	67%	4	80%
Rarely	1		0		1	20%
Sometimes			3	33%	0	
Frequently			0		0	
Very frequently			0		0	
Scenario 16 External groups (blank sheet scenario)						
Very rarely	1		8	89%	3	60%
Rarely	1		1	11%	2	40%
Sometimes			0		0	
Frequently			0		0	

	Round 1		**Round 2**		**Round 3**	
	Frequency	Consensus	Frequency	Consensus	Frequency	Consensus
Very frequently			0		0	
Scenario 17 Trainee breaching confidentiality (blank sheet scenario)						
Very rarely			5	83%	4	80%
Rarely			0		1	20%
Sometimes	1		1	17%	0	
Frequently			0		0	
Very frequently			0		0	
Scenario 18 Breach at the patient home (blank sheet scenario)						
Very rarely			6	67%	4	80%
Rarely			1	11%	1	20%
Sometimes			2	22%	0	
Frequently	1		0		0	
Very frequently			0		0	
Scenario 19 Covering up errors (blank sheet scenario)						
Very rarely			4	67%	4	80%
Rarely	1		2	33%	0	
Sometimes			0		1	20%
Frequently			0		0	
Very frequently			0		0	

6.3.2 Results per scenario

6.3.2.1 Scenario 1: Unattended asset or record goes missing

In this scenario, an internal employee accidentally leaves an asset unattended and as a consequence this asset goes missing, directly leading to the loss of data of up to 10 patients and indirectly leading to costs and embarrassment for the staff or organisation and affecting the compliance to regulation. The type of asset is not specified in detail in this scenario. It could be anything such as an i-Pad, smart phone, laptop, USB stick, diary or a paper record and so on.

The experts commented that this scenario *"*is very likely with USB sticks or smartphones or even paper files" (ID15, Round 1), and it does happen, as "small unencrypted USB devices do go missing, are left in drives or are simply mislaid" (ID14, Round 1). Furthermore, it was mentioned that it "applies more to paper than to electronic assets" (ID20, Round 1).

It was also mentioned that very often it is not clear if an item was mislaid or stolen. The scenario in which items are stolen is described in Scenario 4: theft on the premises, where theft can be proven. In the comments it was mentioned that sometimes organisations combine these two scenarios in their incident registers. In the scenario meant here, items go missing by mistake, sloppiness or unknown causes, while Scenario 4 is based on burglary and robbery.

This scenario was reported frequently in the registers of past incidents (9% of all incidents), but the panel did not estimate the possible frequency of occurrence to be this high. This lower expectation may be influenced by

> Thin clients or private clouds hosting virtual machines. No data held locally. Moving towards this with private cloud data centres (ID19, Round 2).
>
> As personal data is less stored on devices and more in the cloud, the incidents will transition to the cloud storage space as well. Scenarios are different in that case (ID24, Round 3).

The frequency estimations in Round 1 varied along a range of 20. The range of answers declined in Round 2 and even further in Round 3 to 5.5. The median remained the same but the range of answers was drawn closer to the median. As the mean and median were closer together in Round 3 and the standard deviation decreased, the agreement amongst the experts seemed to have increased. Furthermore, the consensus rate went up from 40% to 90% for the category *sometimes*: the frequency of occurrence of this scenario is expected to be between 1% and 5% of all incidents, in contrast to the past experience, which was 9% (*frequently*). Round 3 showed no significant outliers anymore. Figure 6-7 illustrates that in Round 1 the highest expected frequency was 20, and that the interquartile range was large. In Round 3 this interquartile range was smaller, indicating that most answers were in a small range from each other.

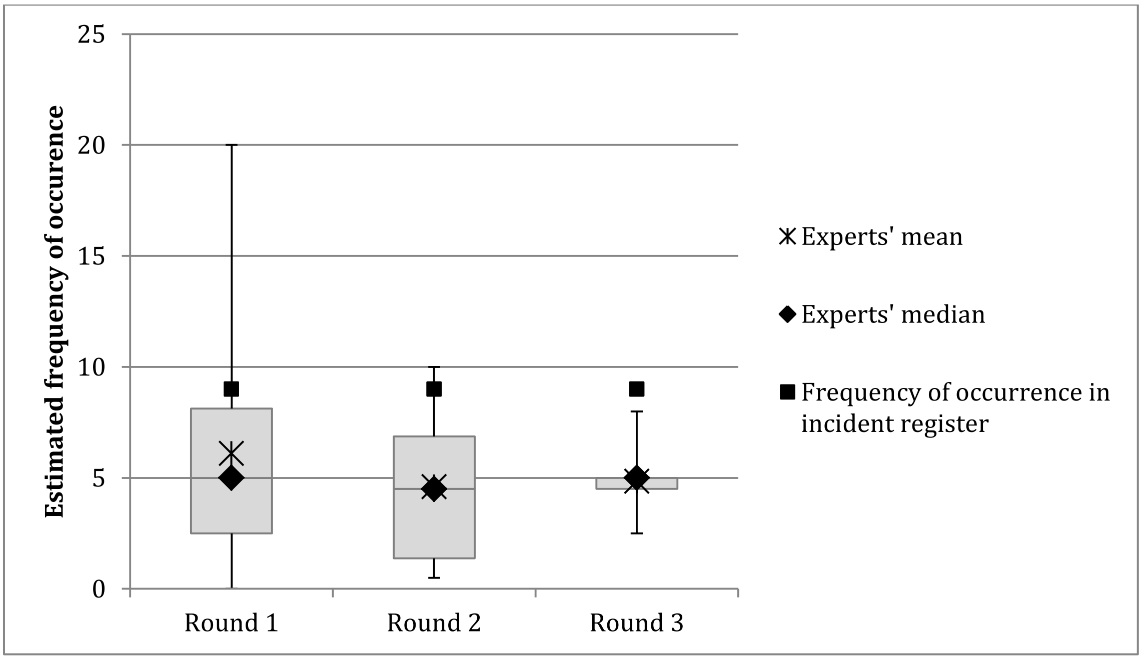


Figure 6-7 Distribution of estimated frequency of occurrence (scenario 1)

The majority of the panel (90%) estimate that this scenario occurs sometimes (between 1-5% of all incidents). Industry reports suggest that one of the biggest current trends is the growing use of mobile devices (replacing unfixed desktops and workstations) to access and store patient records, leading to an increasing level of risk (CompTIA, 2012; Ponemon, 2011), which supports the expert panel estimation as one of the most frequent scenarios. However, the experts also mentioned that the use of encryption, a ban on memory sticks and thin clients or private clouds hosting virtual machines are measures that organisations are taking to lower the frequency of occurrence of this scenario, and as a result the expectation is that it will happen less frequently in the near future.

6.3.2.2 Scenario 2: Password or access token sharing

In this scenario, an employee shares a password or access token with someone and, as a consequence, patient information is disclosed to an unauthorised person. The experts agree that this scenario is likely to occur more frequently than registered in the incident registers. The experts rating the frequency on the highest end suggest that it is otherwise not possible to gain access:

> From past experience, I know it is impossible to work without sharing passwords. A true situation. A student nurse is required to gain experience on a particular system before being allowed own credentials. The only option is to use someone else’s password to gain the experience to be issued with own credential. Crazy, but this is from first-hand experience. Whether this leads to disclosure is a totally different question as it all comes down to personal integrity (ID26, Round 2);
>
> Personnel that are working in a hospital only for a short period of time (co-assistant) use passwords from doctors frequently since they otherwise don’t have access to the computer systems (ID12, Round 1);

and that it is standard practice:

> Based on knowledge of how student nurses are trained, the sharing of passwords is standard practice. The passwords are being shared with novice staff and hence their appreciation of potential consequents tends to be poor; likewise they are more prone to making mistakes than experienced staff (ID25, Round 3).
>
> In all environments that I know, password sharing is common. The fact that most people are trustworthy keeps the incident rate down (ID18, Round 1).

It is often not perceived as a risk, as it is sometimes in the best interest of a patient and colleagues are allowed to see the data anyway:

> Given prominence of IG across NHS, staff are aware that they shouldn’t share passwords. However, understaffed wards with clinicians and nurses under

> pressure to treat patients.... yes, this will happen, and it will be seen as acceptable if it is perceived to be in best interest of patient (ID22, Round 3).

Not only can this lead to disclosure of personal patient data, but auditing becomes an issue too.

> Clinical teams will share passwords, as the perception is that it is quicker to jump on another to save time, and to alleviate patient distress, pain, etc. Management may issue access tokens in an attempt to reduce incidents of this type as people are seen to own their individual access token and may be less likely to give it away. However temporary staff may still share access for convenience. Audit becomes an issue. (ID19, Round 2).

The work pressure and the way systems are designed seem to enable this practice, and it is suggested this risk scenario should be controlled with awareness training, special arrangements for temporary staff or trainees and additional terminals to work from. This risk scenario has been pointed out by other researchers as well. A study of the state of information security in twenty Dutch hospitals found that in two-thirds of these hospitals it was common to share one logon-id and password within a department (IGZ/CBP, 2008). The work pressure and the way systems are designed seem to enable this practice, and it is suggested to control this risk scenario with awareness training, special arrangements for temporary staff or trainees and additional terminals to work from.

The panel estimated that the frequency of occurrence of this scenario is higher than suggested by past incidents (9% compared to 5%). After Round 3, the mean and median became closer together and the standard deviation lower, suggesting consensus amongst the respondents. Figure 6-8 illustrates a shrinking interquartile box over the rounds. The consensus rate for this scenario is 80%.

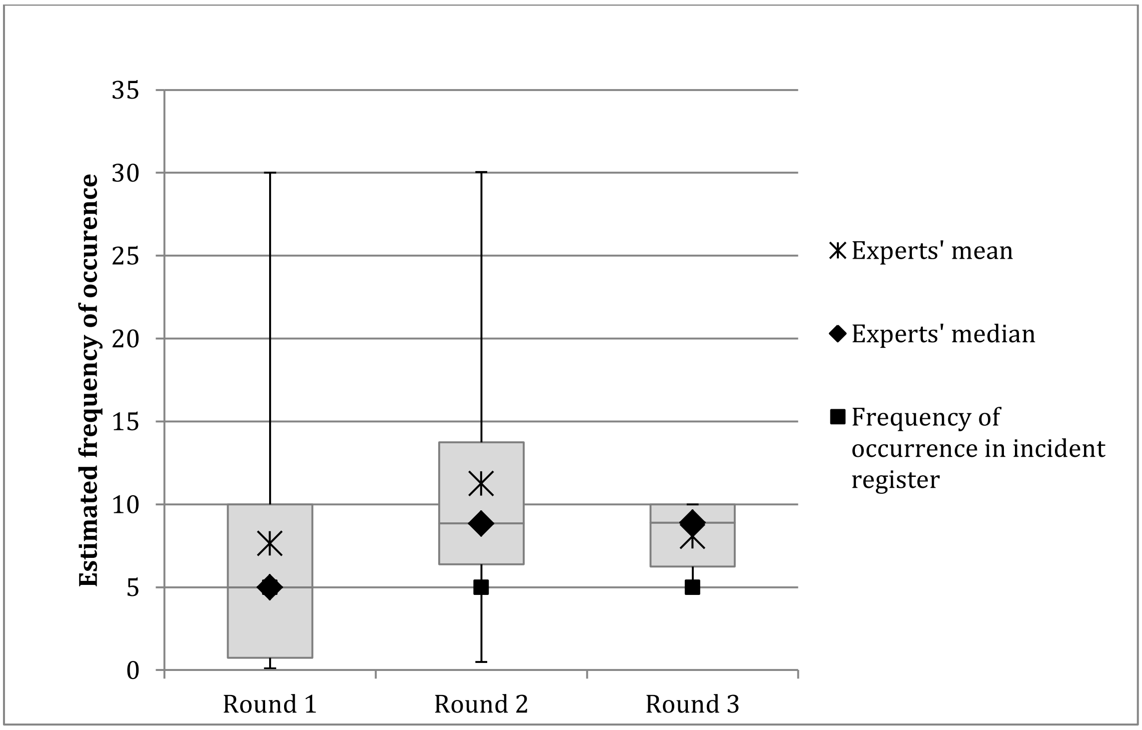


Figure 6-8 Distribution of estimated frequency of occurrence (scenario 2)

6.3.2.3 Scenario 3: Email to wrong recipient

This scenario was reported as the most frequent in the registers of past incidents. It involves emails containing personal data of patients being sent to either the wrong recipients and/or to persons not authorised to receive that information. It is a scenario caused by unintentional mistakes by employees. The incident could lead to heavy fines, as can be illustrated by the £80,000 penalty that the ICO in the UK imposed on a County Council after a member of staff emailed highly sensitive personal information about a large number of vulnerable people to unintended recipients by clicking on an additional contact list, which had only been intended for internal use (Information Commissioner, 2011).

The panel commented that some organisations do not use email to exchange patient data and thus have a lower frequency of occurrence.

> We have another solution in place to exchange patient data (ID24, Round 2).

In other organisations it appears to happen often and it can also mean that notes on patients are included in meeting minutes. When the minutes are sent to a distribution list, it can easily happen that the list contains people who should not receive these details.

The experts did not estimate the possible frequency of occurrence to be as high as it occurred in the registers.

> This occurred at about 5:1000 10 years ago. Policies on patient identifiable information have since been adopted which seem to have addressed the issue (ID23, Round 1).

Others commented that mistakes are easily and often made.

> It is very easy in a large healthcare organisation or hospital for employees to mistype email addresses or confuse recipient details. The larger the number of people with access to email, the more prone to error. Particularly where the staff IT expertise or workloads vary (ID14, Round 1).

90% of the experts expect the frequency of occurrence of this scenario to be between 1% and 5% (this scenario will happen sometimes), in contrast to past experience, which was 10% of all registered incidents. The mean and the median are close together.

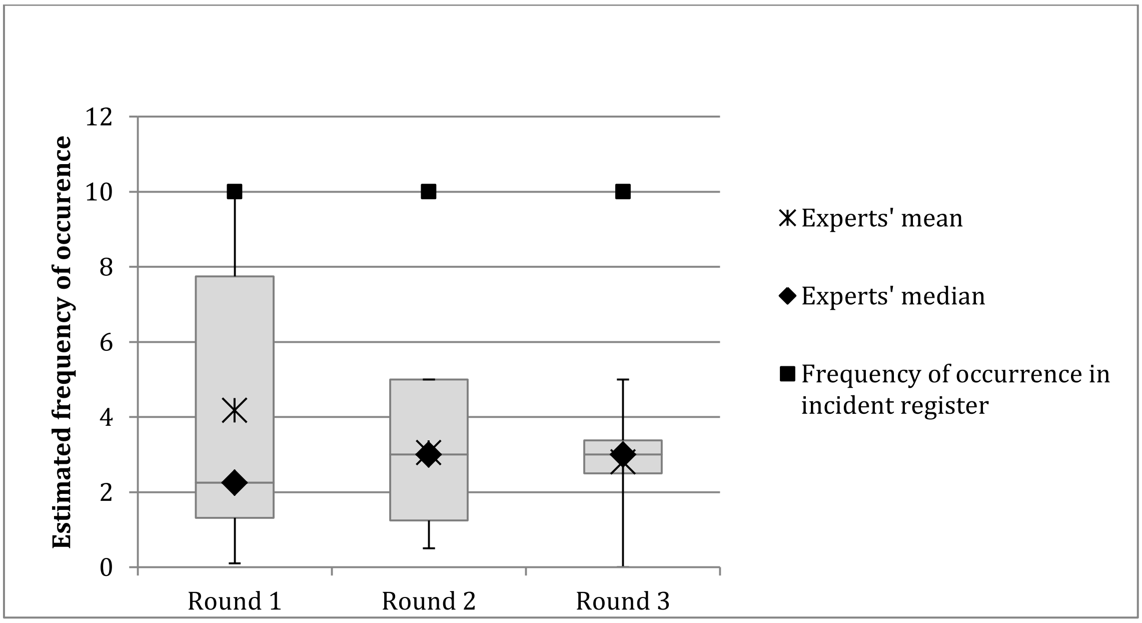


Figure 6-9 Distribution of expected frequency of occurrence (scenario 3)

6.3.2.4 Scenario 4: Theft on the premises

This scenario was suggested by the panel in Round 1. The scenario involves the theft of devices with personal data stored on it from the premises of the organisation. It can lead to a number of possible events such as loss of data and a breach of confidentiality. Theft of computers, laptops or other devices is the biggest cause of privacy breaches in healthcare reported to the Secretary of the U.S. Department of Health & Human

Services (2012). In their list of breaches, it shows that 50% of the breaches of health information security (that affected 500 or more individuals) are caused by theft.

The scenario was reported frequently in the incident registers although the experts together estimate the frequency to be a little lower. The combined experts estimation is 5%, and the past experience frequency was 6%. 70% of the experts agree that this scenario happens sometimes (1% to 5% of all incidents are like this scenario). One expert suggests that this scenario could be combined with lost assets:

> It is often very hard to reconstruct whether an item was lost or stolen. We treat the two the same in risk analysis (ID 21, Round 2).

One outlier on the high end of the range (suggesting 10%) argues that this happens frequently:

> I've seen this in several healthcare organisations. In one particular case the PC in an addiction unit was deliberately stolen by drug dealers to provide them with a sales and marketing database of known addicts! (ID26, Round 2).

This remark illustrates one of the statements of this thesis to include the environment and local crime rates as factors in a risk analysis. As was discussed in the background chapter, the implementation of physical security controls is often limited to the controls proposed by the international standard BS7799. However, some areas within organisations or within close range of the premises could be at higher risk due to safety and crime factors and require a broader risk analysis.

For this scenario the consensus grew over the three rounds and the mean and median are close together. Figure 6-10 shows no data for Round 1 because the scenario was created in Round 1. In Round 3 the range was smaller than in Round 2 and the mean and median are almost equal. The one outlier at 10 causes a large range of answers (8).

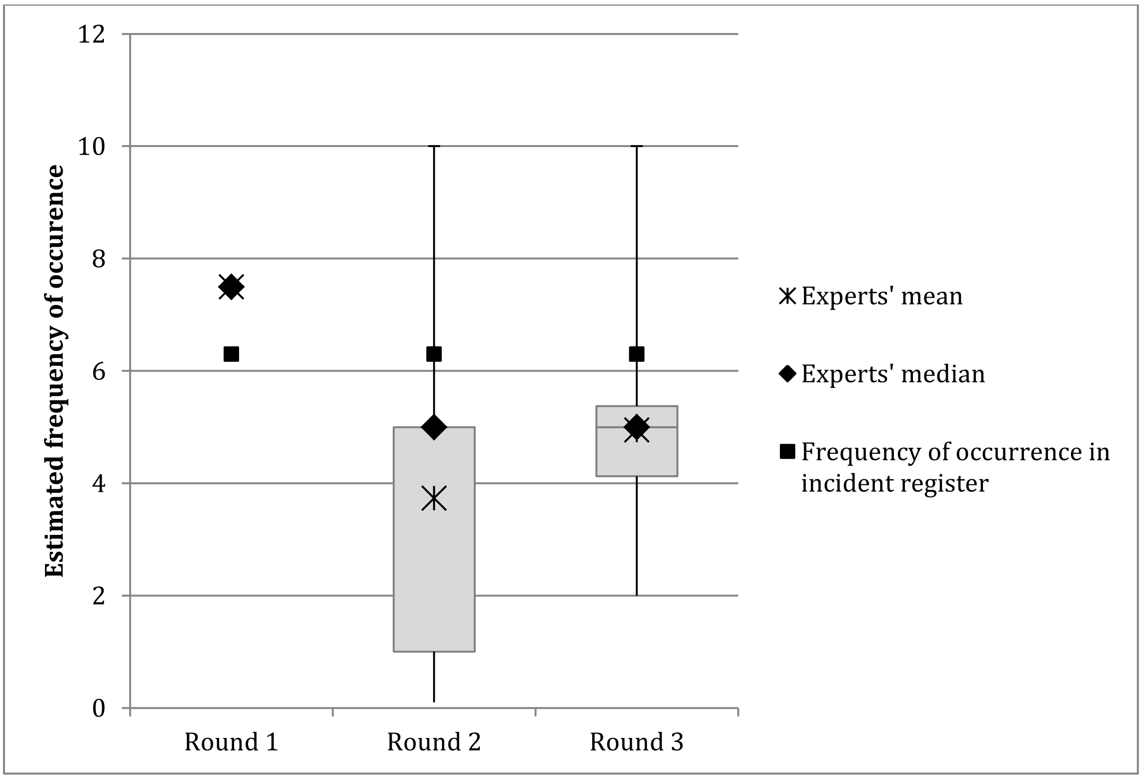


Figure 6-10 Distribution of estimated frequency of occurrence (scenario 4)

6.3.2.5 Scenario 5: Procedure not followed

Not following the formal procedures could lead to the disclosure of patient information to unauthorised persons, affecting compliance to regulation. A number of annual industry surveys recognize this scenario as one of the most frequent ones, and explain this type of scenario by lack of information security awareness. Awareness includes the behaviour, motivation, knowledge and skills of employees regarding information security. For instance, in the 2010 Kroll Fraud Solutions survey, the most frequently selected answer that would put data at risk was “lack of attention by staff to security policy” (Kroll Fraud Solutions, 2010).

The issues with policy and procedures were considered in the literature review in chapter 3. Several publications were discussed which suggested a number of possible causes of these issues. Amongst these issues were the style and wording of the policies, the compatibility with practice, communication and feedback, training, changing organisational structures, peer pressure and compliance. The experts confirm these issues, as their comments appear to discuss the same topics. Some of the comments made by the experts refer to staff often breaching policy and procedures but they can be unaware of it.

> Staff wouldn’t perceive themselves to be breaking the rules and hence may happen more often than is reported (ID19, Round 2).

Staff tend to be helpful and fix problems outside of procedures when there is an urgency.

> Not following procedures happens regularly. We tend to be helpful, fix problems outside of procedures. Procedures contain checks to contain and correct this behaviour. We are increasingly getting better at this - hence the number of instances should decrease (ID18, Round 1).

> Too often patient data handling urgency overrules the safe conduct; else staff is not aware of any policies (unskilled or low skilled staff) or does not have any interest (high or extremely specialised skilled staff)… (ID13, Round 1).

However, if the procedure is compatible with the practice, the adoption rate increases.

> We specify more and better procedures covering more work activities. Procedures contain checks, so they are increasingly more fault-resistant. As staff finds that following procedures leads to better results, adoption rate increases. All leading to better results than in the past (ID21, Round 2).

Proper training, security awareness programmes and sanctions are suggested to have a positive influence in controlling this scenario.

> It all depends on user awareness, training, sanctions, and perhaps the motivation for intentional disclosure (ID15, Round 1).

> Ignorance or seeing rules as 'getting in the way' will always ensure that this is a high risk. It can only be countered by good security awareness training programmes (ID12, Round 1).

Over the three rounds, the range of frequency estimations shrank but was still large. Figure 6-11 shows that Round 2 had outliers with higher estimations and lower estimations and Round 3 only had one outlier on the top. The individual with the higher estimation motivated his estimation with commenting that it may occur more frequently but it is often not reported.

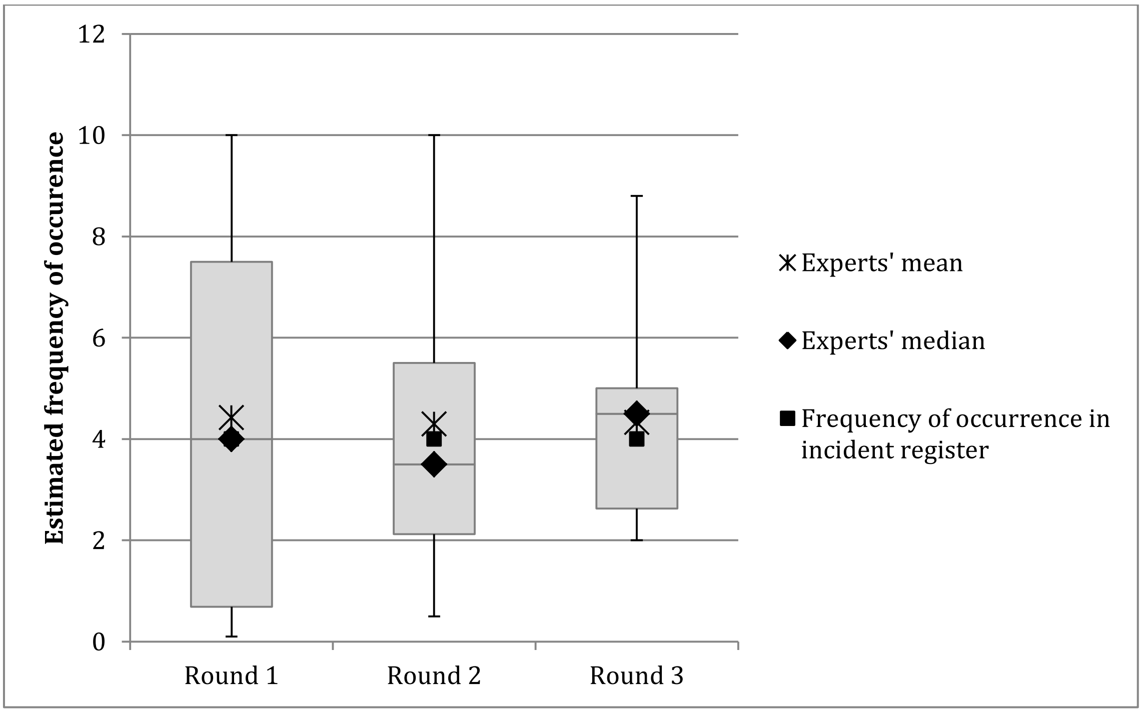


Figure 6-11 Distribution of estimated frequency of occurrence (scenario 5)

The experts estimated the possible frequency of occurrence of this scenario as almost similar to the frequency of past incidents (which was 4%). Eighty percent of the experts in the panel estimate the frequency to be between 1% and 5%. Table 6.2 showed that the median and mean are close together and that the standard deviation is still large, but got lower over the three rounds and 80% of the estimations are now within the same interval.

6.3.2.6 Scenario 6: Wrong privileges set

This scenario describes how flaws in the settings of authorisations and privileges in systems can lead to confidentiality breaches because unauthorised employees receive or can read personal data they should not have access to. Table 6.3 showed that 100% of the panel estimates that this scenario will occur in 1% to 5% of all incidents. Figure 6-12 shows a small distribution of estimated frequencies.

Earlier, in Round 2 it had shown a few outlying answers. From the comments made by the experts who estimated the frequency of occurrence as high, it seemed that, according to them:

> Identity and access management and a proper implementation of authorization of electronic patient information has not been implemented very often and successfully (ID17, Round 1).
>
> I see it in many organisations. People accumulate access rights and the periodic review to clean that up does not happen (ID15, Round 1)

The profiles of these experts (ID14, ID15, and ID17 in Round 1) showed that these are the panel members with the highest expertise level in IT security. On the other hand, the experts who rated the frequency the lowest, refer in their comments to be confident that the procedures should cover this risk and to have confidence in the IT staff:

> IT staff is alert and need signatures before they give authorisations (ID 23, Round 2);
>
> Covered by procedures (ID19, Round 1);
>
> This is reviewed regularly (ID20, Round 1).

This relation was shown to the experts in Round 3, as it could influence their point of view on the scenario. In Round 3 indeed, the differences completely disappeared. Some of the experts suggest that the IT staff usually follows the procedure but the managers who authorize the privileges do not perform periodic review to cancel or change privileges when no longer necessary.

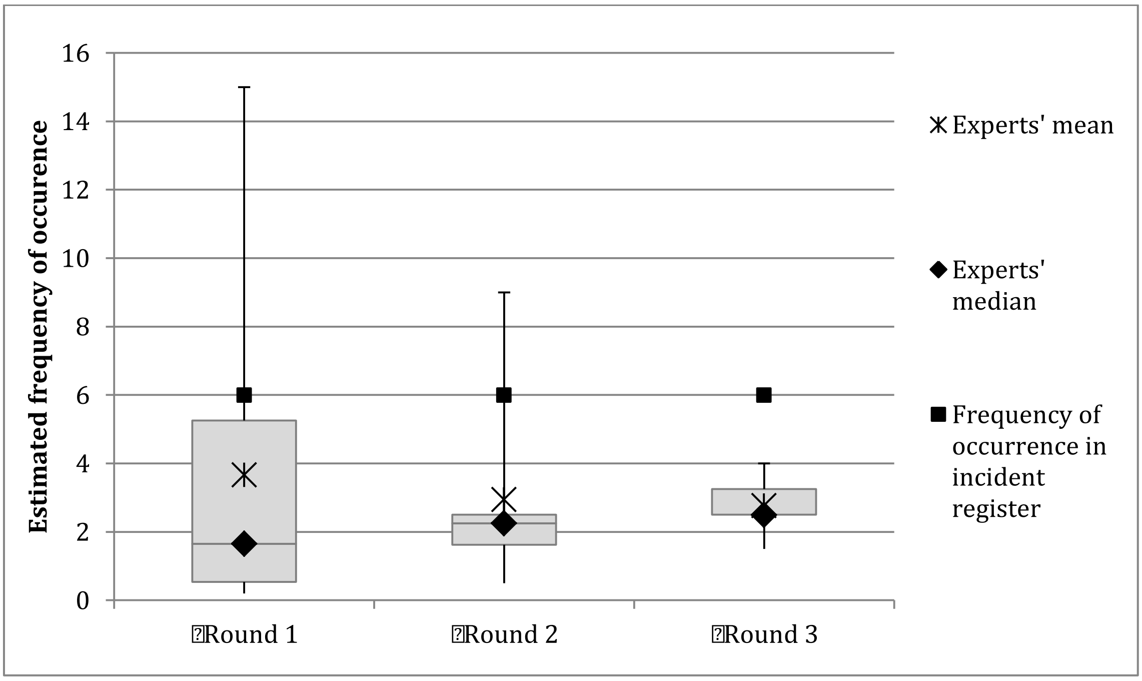


Figure 6-12 Distribution of estimated frequency of occurrence (scenario 6)

The experts estimate the possible frequency of occurrence to be lower than the frequency of past incidents showed (was 6%). The range of expert estimations decreased from 14.8 in Round 1 to 8.5 in Round 2 and dropped even more to 2.5 in Round 3. The estimations for this scenario had the lowest standard deviation of the scenarios (Table 6.2).

6.3.2.7 Scenario 7: High impact mistakes

This scenario involves situations where medical or other internal staff makes an unintended mistake, which affects a large number of 1,000 to 9,999 patient records. It is a scenario that was suggested by two experts on their blank sheet in Round 1. The scenario was presented to the group and although in Round 2 there was little consensus and a high range of answers, in Round 3 their opinions came much closer together with a 90% consensus that this scenario happens sometimes.

The register of past incidents did not show this scenario as frequently as the experts would have expected, "but it happens more often than we think" (ID 18, Round 3).

The experts commented that mistakes with high consequences are expected:

> Mistakes are made easily (ID13, Round 2).
>
> People are human. Given workloads and work scenarios of busy clinical staff, disclosure as a result of internal mistakes is a real risk. It does happen and will continue to do so (ID14, Round 3).
>
> Biggest risk is still internal mistakes, because of the high impact (ID18, Round 2).

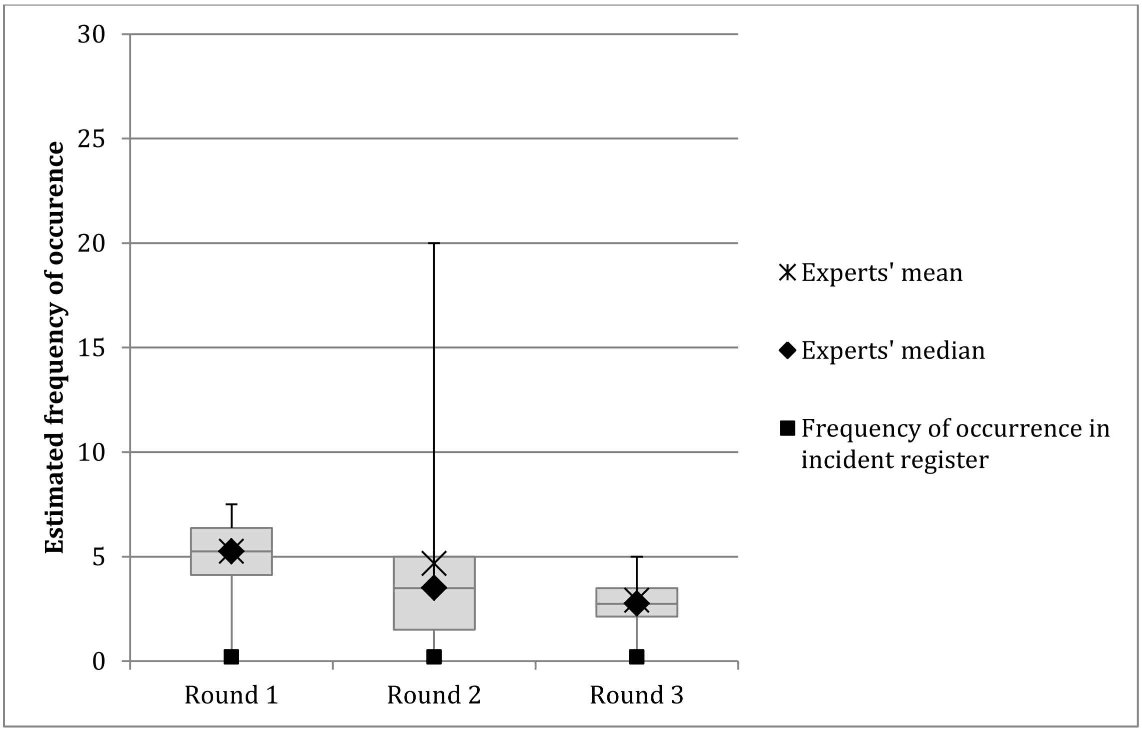


Figure 6-13 Distribution of estimated frequency of occurrence (scenario 7)

6.3.2.8 Scenario 8: Working in a public place

One expert suggested in Round 1 a scenario that involves:

> Medical staff working in a public place with a laptop or talking over the phone, and being overheard or seen, leading to the disclosure of personal data, affecting 0-9 patient records (ID12, Round 1).

He elaborated on this scenario with:

> Medical staff, in particular senior medical staff, still seem to have the attitude that they are above the law and that they should be able to work where and when they choose (ID12, Round 1).

There was no instant tendency to agreement amongst the experts in Round 2 but they came to a 100% consensus in Round 3 (Figure 6-14). Of all 19 scenarios, this scenario is one of those with the closest consensus and the lowest range between estimated frequencies.

This scenario is deemed hard to counteract:

> There will always be situations where public can see or hear medical staff discussing patients. Due to sheer size of NHS and older buildings this will never be 100% eliminated (ID14, Round 2).
>
> This happens more in hospitals than in GPs since GP surgeries are smaller and more easily controlled. A&E, on wards common to be overheard. Don’t think this will ever go away (ID14, Round 3).
>
> Theoretically this could apply to laptops connecting to open Wi-Fi hotspots - often a service offered at large facilities. But I think it is still more the case that we are not aware enough of our surroundings when discussing confidential details over the phone. It is not a choice of working where you choose; it is a consequence of rising work pressure (ID18, Round 2).
>
> I believe that medical staff still sees themselves as invisible or that people cannot hear, understand or are not interested in information they are talking about regarding other patients. It is a culture thing borne out of ward rounds, etc. (ID25, Round 2).

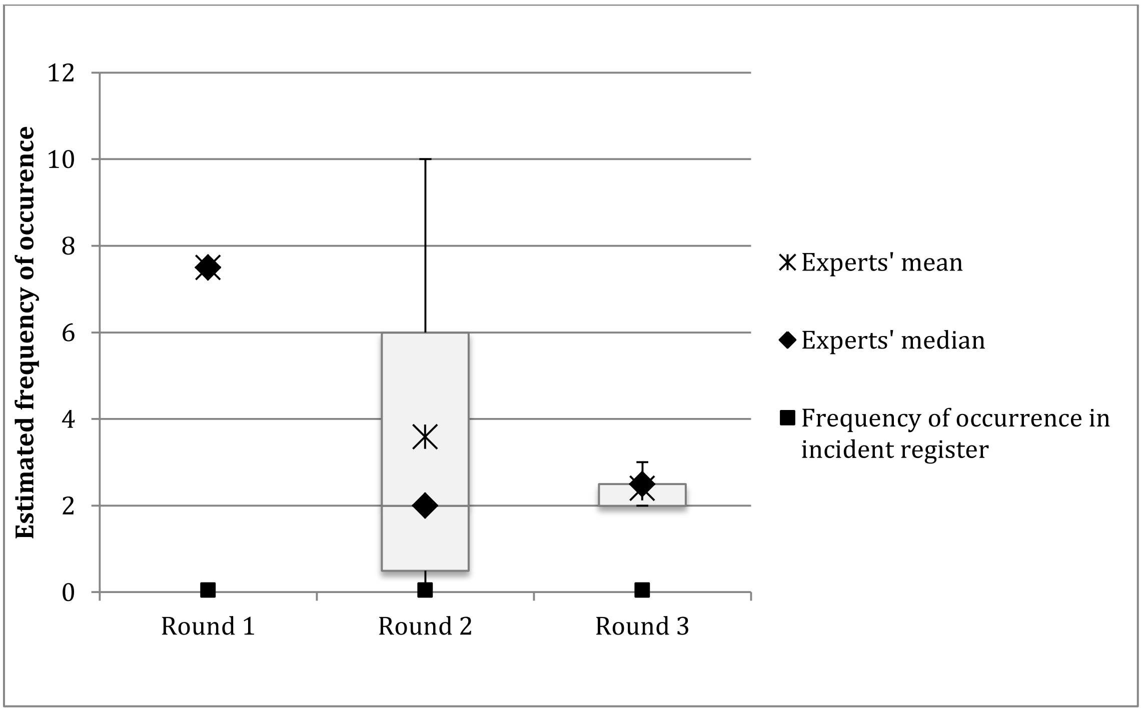


Figure 6-14 Distribution of estimated frequency of occurrence (scenario 8)

This scenario is related to three main factors: attitude of staff, the requirement to be able to work anywhere and the technical possibility to work anywhere. The background chapter discussed the growing possibilities of mobile working. Mobile working requires specific technical and social security controls. The attitude of staff and the awareness of the possibility of being overheard are main risk factors in this scenario.

6.3.2.9 Scenario 9: Unsecure remote 3rd party

This scenario was suggested by an expert in Round 1:

> An employee in a third party supplier or subcontractor making a mistake when using remote access from home or office and disclosing personal data, affecting 100-999 patient records (ID25, Round 1).

The experts responded that this can happen, but not as frequently as was suggested. Over the rounds, the experts estimated that it may happen in somewhere between 1% and 3% of all incidents. Although there is not a 100% consensus within a category of frequencies (Table 6.3), the range of answers is low (Figure 6-15).

The scenario is mostly related to outsourced IT services and the possibility for staff in that company to access all data, and this kind of scenario is expected to start occurring more frequently in the future.

> Outsourcing of maintenance or whatever IT services brings this issue to become a growing issue (ID19, Round 2).
>
> It will happen more and more often as more is outsourced and more and more business partners cannot prove or be controlled if they haven't these kind of incidents (ID 19, Round 3).

The causes of this scenario are suggested to be due to procedural errors and awareness.

> Given the large number of individuals who potentially could gain access when working for outsource IT supply companies, there is a likelihood of error leading to disclosure. The more remote the support is from the end user the less they are seen to own the data, hence easy to make procedural errors (ID14, Round 2).
>
> Unauthorised use of real data for testing and development purposes in an insecure environment (ID12, Round 2).

This scenario is important because "These incidents can have a large impact too" (ID18, Round 2).

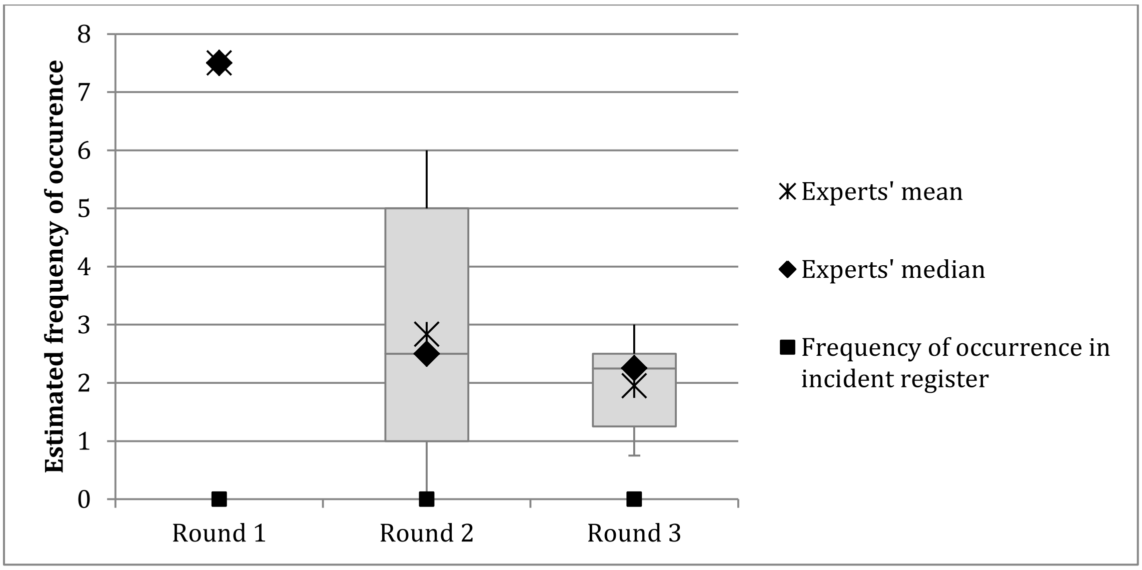


Figure 6-15 Distribution of estimated frequency of occurrence (scenario 9)

6.3.2.10 Scenario 10: Transportation of data

This scenario was created in Round 1:

> An unknown person breaching confidentiality by copying personal data on a storage medium and transporting this medium for convenience, affecting 100-999 patient records (ID19, Round 1).

As underlying causes, it was suggested that this happens because staff is working at home to complete their tasks.

> Staff take home personal data for research purposes and to allow them to produce reports (ID12, Round 3).
>
> This is getting increasingly simpler to do and increasing work pressure may make staff feel this is necessary to complete their tasks (ID18, Round 2).

It also happens within the premises of the organisation and the medium involved will increasingly consist of tablets:

> Depending upon network setup, could still allow use of external devices such as USB Keys (unlikely), but more commonly used are mobile tablets, PCs, ipad, etc., where record details are held. They can be moved around clinical team members as they move around their normal job tasks (ID14, Round 2).

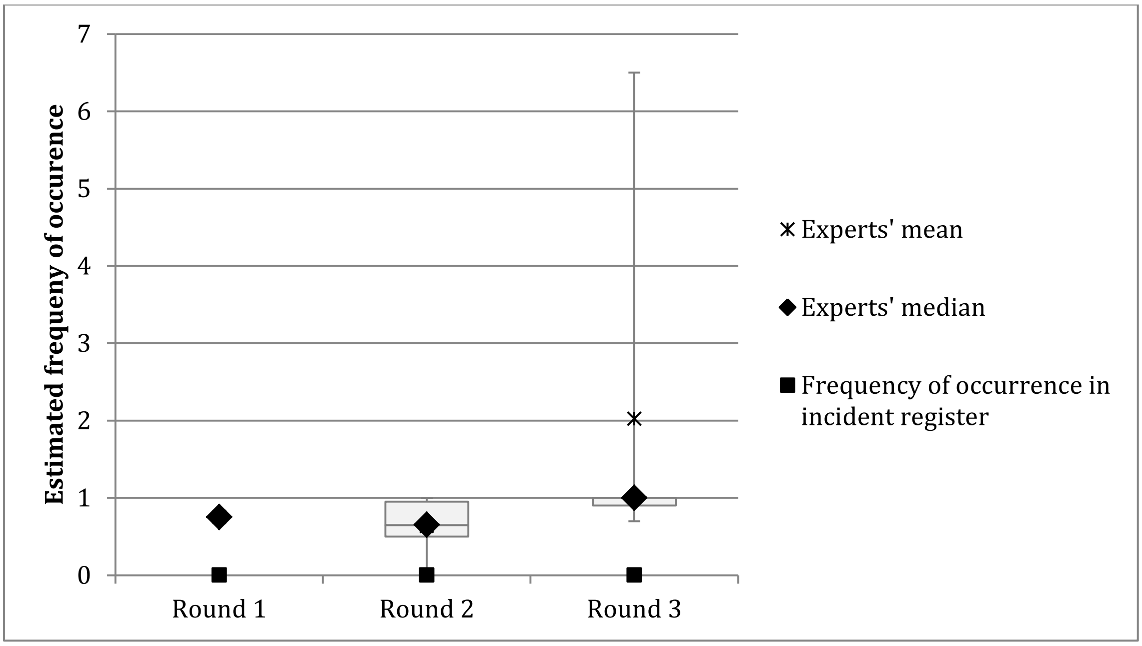


Figure 6-16 Distribution of estimated frequency of occurrence (scenario 10)

The consensus rate of 80% suggests some strong support for this scenario.

6.3.2.11 Scenario 11: Family of patient

In Round 1, this scenario was suggested by one the panel members:

> A family member/representative/carer of patient accessing the unattended patient's record unauthorised to gain knowledge (ID24, Round 1).

This scenario led to disagreement between the experts:

> I strongly disagree with the consensus here when it relates to a patient in hospital and the notes are left on the end of the bed for visitors to read. Likewise, mail to home is often read by family members or the envelope marking infers the contents, even if the envelope is not opened (ID12, Round 3).

> My experience is higher, much higher (ID 13, Round 3).

One expert insisted on a higher frequency of occurrence, which is visible in the higher range of estimations in Round 3.

There was not so much disagreement amongst their comments on why this kind of scenario happens:

> Curiosity killed the cat. Everyone tries to see what their doctor writes about them! So only natural to ask or look if paperwork or devices are nearby, so yes could see another patient's details easily. Proper observation of procedures should prevent this from happening but the reality is in a busy care environment where staff are under pressure and under resourced (ID14, Round 2).
>
> This is very human to do this. Records are often left unattended (ID 18, Round 2).
>
> Family can be easily overheard and so often breach confidentiality, even towards other patients (ID19, Round 2).

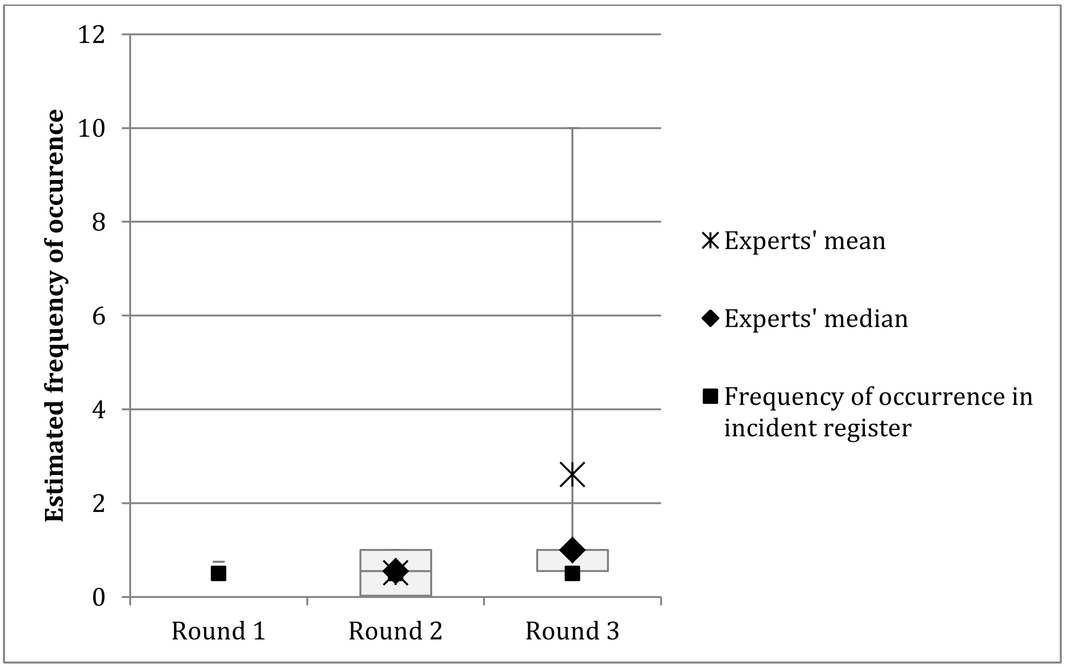


Figure 6-17 Distribution of estimated frequency of occurrence (scenario 11)

6.3.2.12 Scenario 12: Backup medium goes missing

This scenario was presented in Round 1 as the scenario from the past with the highest impact. In this scenario the loss of a portable backup medium during transport to the offsite storage facility affected the full database of patient's records, involving more than 10,000 records. Although the scenario was rare, the impact was very high. Most experts acknowledge the existence of this scenario:

> Some of the engineers have lost/got stolen from their backup medium out of the car (ID13, Round 2),

and estimate it to be more frequent that past experience would suggest (Figure 6-18). Sixty percent of the experts agree that it happens in less than 1% of the cases.

Preventive measures were suggested by the experts and they expect that this scenario will grow ever rarer:

> Given recent press coverage, backup devices used now are encrypted (ID14, Round 1).
>
> With increasing deployment of Private Cloud data centres in NHS the standard solution includes […] to encrypt all backups, snapshots and snapmirrors for security. […] No need for tape ID14, Round 2).
>
> Manageable with policies, encryption, no mobile backups but only back data up onto the network (i.e. no external harddisks or such). Tapes are becoming obsolete, for offsite backup storage - consider a private cloud or a cloud solution dedicated to healthcare industry (ID15, Round 1).

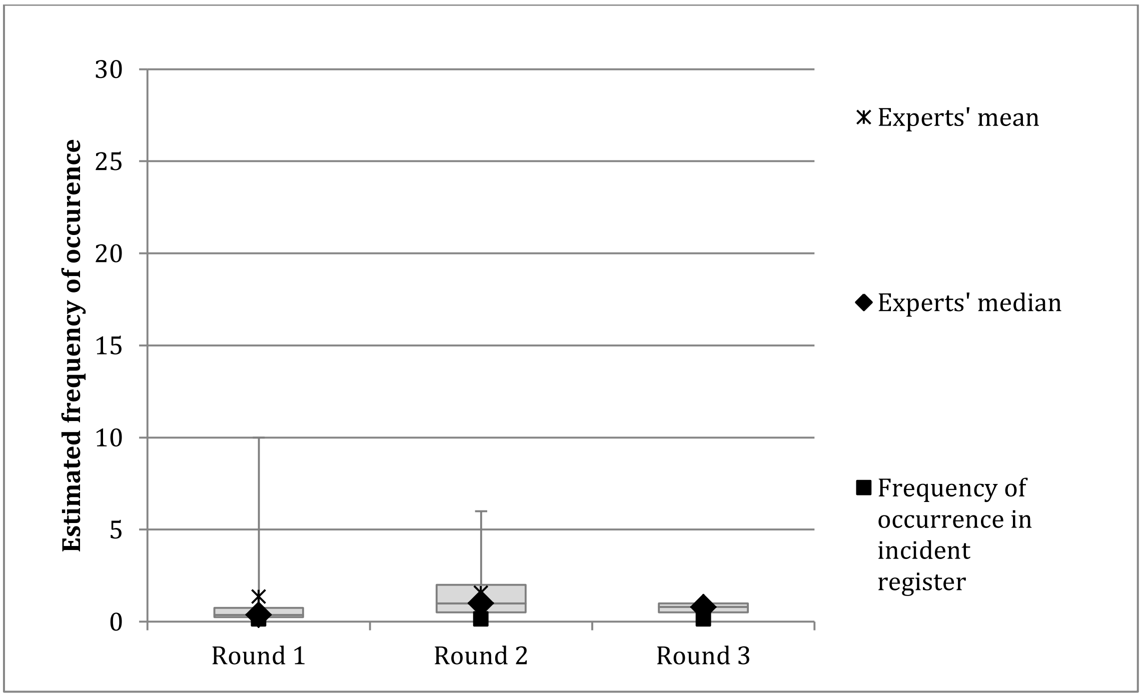


Figure 6-18 Distribution of estimated frequency of occurrence (scenario 12)

6.3.2.13 Scenario 13: Improper disposal

In Round 1, this scenario was suggested by one the panel members:

> An employee in a third party supplier or subcontractor is not taking due care when clearing out a building or destructing records, affecting 100-999 (ID20, Round 1).

These records can be paper-based or digital.

> Many organisations still do not have proper procedures for destruction of faulty/failed media; on such media a disk cleansing program cannot run (ID12, Round 3).

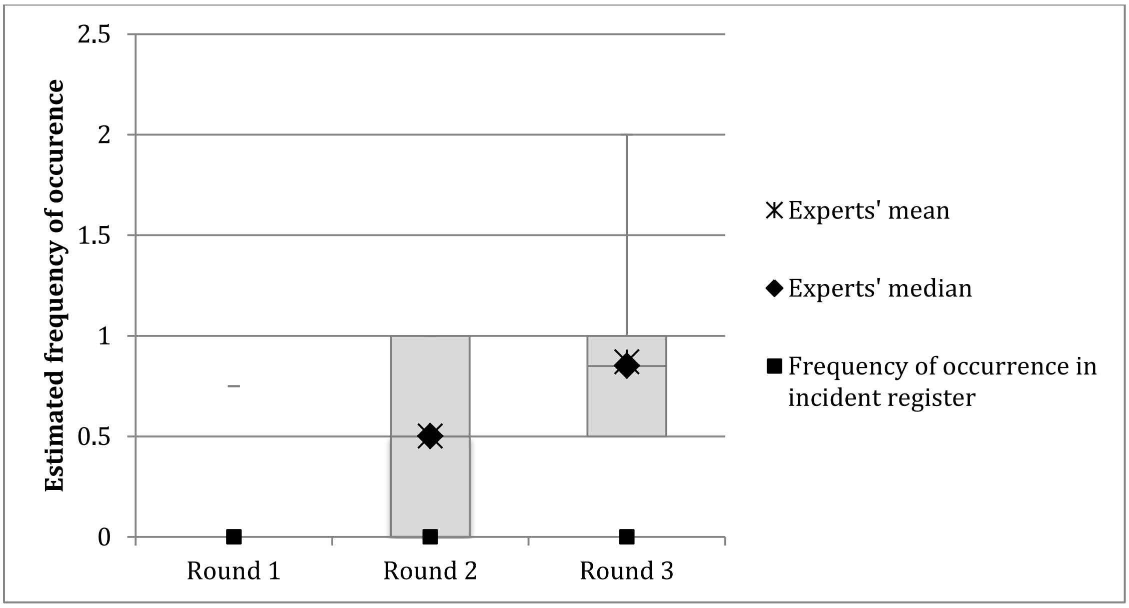


Figure 6-19 Distribution of estimated frequency of occurrence (scenario 13)

The range of answers is small, and no expert expects this to occur more than in 2% of all incidents. The causes seem to be found in the attitude of the outsourcing partner towards the security of the records and the lack of control the healthcare organisation has over this partner.

> With third parties involved, if staff is poorly paid, they are not paid enough to take care. They don't own the data, are remote from the source, and therefore don't perceive it as theirs and don't treat data the same as they would their own (ID14, Round 2).
>
> This would be common with building work, renovations or office moves. Items are misplaced. People are human but IG now features heavily in contracts (ID14, Round 3).
>
> This happens rather often. I myself had the opportunity to gather piles of information, while collecting my old status. The area was not secured at all, and I was left alone for hours (ID19, Round 2).
>
> It will happen more and more often as more is outsourced and more and more business partners cannot be controlled (ID19, Round 3).

6.3.2.14 Scenario 14: Third party discloses data

Three experts suggested a similar scenario on their blank sheet in Round 1:

> Incidents that involve a third party supplier or subcontractor unintentionally copying data leading to the disclosure of personal data, to the loss of availability and affecting the integrity of data, involving 1,000 to 9,999 patient records (ID12, ID14, ID23, Round 1).

The panel agreed that this happens, but it happens very rarely. The main cause of this scenario is again IT suppliers or subcontractors (like scenario 9) not taking appropriate controls. Testing systems with real data instead of test-data is mentioned as a cause:

> The big issue that, still and all too often, live personal information is used for testing purposes. The test environment is often not secured to the extent as the production environment. It is against the Data Protection Act that live personal information is used for testing purposes (unless explicit permission has been obtained), but it still occurs very widely (ID12, Round 1).
>
> The main risk comes from the unauthorised (illegal) use of personal information for testing or training purposes. In these environments, the data is often not properly protected (ID12, Round 2).
>
> Personal data is often used in testing and gets out of the production security regime that way. Also, audit evidence is another leak of data out of production environments. This leads to personal data ending up on laptops or portable hard disk drives (ID18, Round 2).

The frequency of occurrence is perceived as low.

> Viewed as a low risk due to the physical and procedural environment in which suppliers operate (ID12, Round 3).
>
> Most contractors obliged to meet ISO standards when dealing with IT Systems - we are and we work throughout the NHS. If this behaviour occurs contracts are not renewed so this is low as a source of risk (ID14, Round 3).

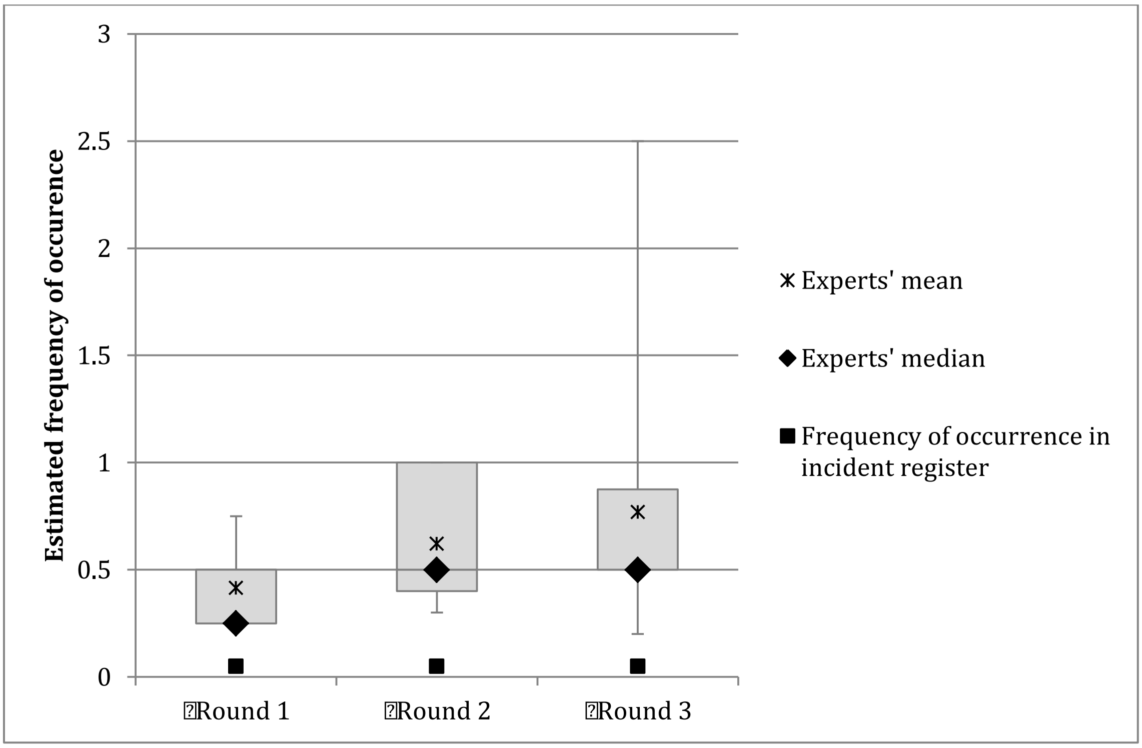


Figure 6-20 Distribution of estimated frequency of occurrence (scenario 14)

However, when the scenario does occur, it affects a large number of records.

> The disclosure itself is not so often, but the amount of data compromised is (ID19, Round 2).

6.3.2.15 Scenario 15: Unsecured remote working environment

This scenario was suggested on the blank sheet and it refers to the physical environment when one is:

> Working from outside the premises. Staff looses data unintentionally, and it involves 10-99 records. Remote working is not for hospital employees so often active. But growing and becoming more and more an issue! (ID19, Round 1).

There is some agreement that remote access to the systems is secure, but the issues are the non-electronic activities and home security.

> This will occur more often with medical papers of patients because medical people need to read them. For the electronic version of this information this will be less due to thin client computing capabilities (ID17, Round 3).
>
> Most remote working occurs through encrypted VPN or using logon tokens, therefore this is a very secure system. Movement of paper based data and memory sticks…hmmm… (ID14, Round2).

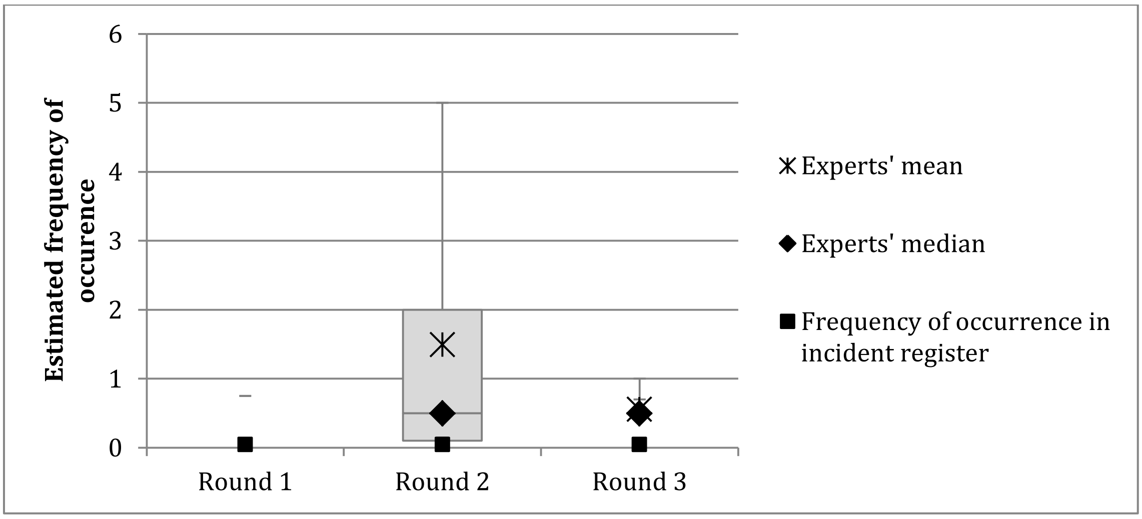


Figure 6-21 Distribution of estimated frequency of occurrence (scenario 15)

6.3.2.16 Scenario 16: External groups

The scenario involving external groups or activists wanting to steal, access, abuse or manipulate data was proposed by two experts on their blank sheet in Round 1 (ID13, ID18).

The panel agree that this could happen, but very rarely. One expert commented that in his country this is not likely to happen:

> Reports in press and FOI requests indicate this doesn't happen very often in Scotland hence I would reassess this question as unlikely to occur therefore frequency must be less than 5 (ID14, Round 2).

However, others state that it is generally likely to occur:

> Read the newspapers of the last weeks, you will read quite a lot of examples of it happening nowadays (ID17, Round 3).
>
> The 'major hack' will happen, and when it happens it will affect a large number of patient records. It is hard to estimate how likely this is, hence I am reserved (ID 18, Round 1).
>
> Medical data is an attractive target for high profile hackers. This will happen and when it happens it will have a substantial impact (ID18, Round 2).

The range of estimations is small and all experts estimate this scenario to be lower than 1% of all incidents.

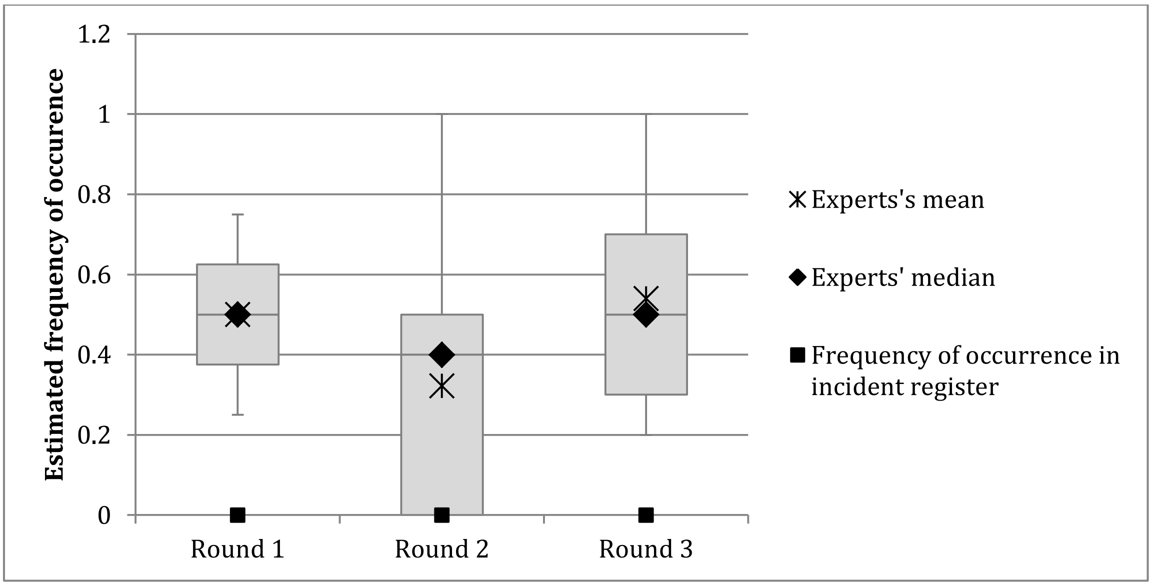


Figure 6-22 Distribution of estimated frequency of occurrence (scenario 16)

6.3.2.17 Scenario 17: Trainee breaching confidentiality

This scenario where trainees unintentionally access patient records unauthorised was suggested in Round 1 (ID24). There were not many comments about this scenario, but it was the cause of some confusion amongst the experts because of the word 'unintentionally':

> The key word here is 'unintentionally'. When it happens, it happens intentionally, like looking up a celebrity's status (ID18, Round 2).
>
> They are eager telling about their new job (ID19, Round 2).

It was also suggested that this scenario is strongly related to other scenarios:

> Based on knowledge of how student nurses are trained, the sharing of passwords is standard practice. The passwords are being shared with novice staff and hence their appreciation of potential consequences tends to be poor; likewise they are more prone to making mistakes than experienced staff (ID14, Round 1).
>
> Like scenario presented earlier: links trainee nurse using another's credentials. (Other scenario staff sharing logons.) Think this occurs more than is reported since trainee will be told of procedure to follow rather than be entered into incident log (ID14, Round 3).

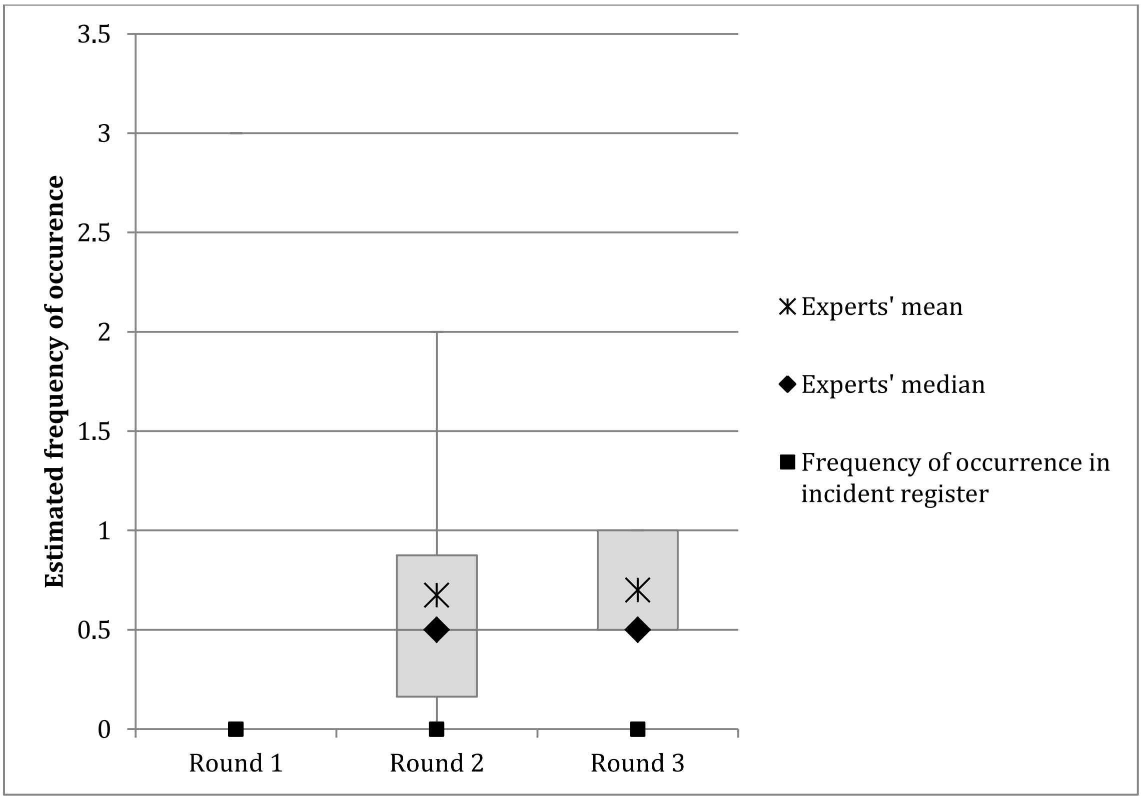


Figure 6-23 Distribution of estimated frequency of occurrence (scenario 17)

6.3.2.18 Scenario 18: Breach at the patient's home

Another scenario suggested in Round 1. In this scenario a breach happens at the home of a patient. This could be initiated by healthcare staff and other patient facing staff talking to each other, believing that the other person already knows everything about the patient.

Only a few comments were made:

> I'll stick with past experience. It is hard to control the patient's home environment. Impact will be low, however, as it will involve the patient's own data (ID18, Round 2).
>
> Information regarding patients left out on view to assist continuity of care is often not marked confidential or restricted to specific carers and often is generated by the patient's/user's friends or relatives (ID25, Round 2).
>
> I would rate this as 5% or higher, since devices are updated on home visits by clinicians and care teams to patient homes. Whilst on those premises less awareness of security (no notices on every door warning of security), more informal environment yet care team under pressure due to severity of problems, overwork, lack of staff or other resources so may easily lead to breach of a small set of data current or previous patient data (ID14, Round 2).

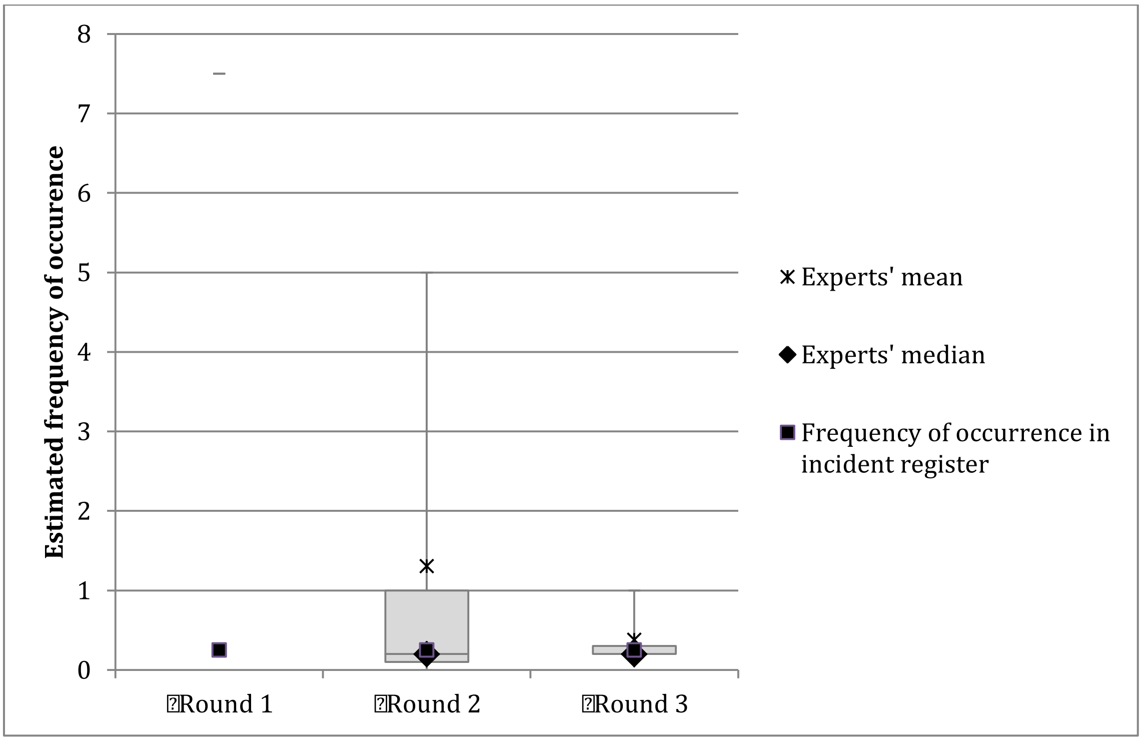


Figure 6-24 Distribution of estimated frequency of occurrence (scenario 18)

6.3.2.19 Scenario 19: Covering up errors

This scenario, suggested by ID15 in Round 1, involves medical staff accessing data, reports or notes to insert data, modify notes or remove parts of reports to cover up their errors.

The consensus in the panel tends to be with a very low frequency of occurrence, although one expert is convinced this happens more often than the consensus rate:

> Given incidence of malpractice, pressure from managers, culture around surgeons & GPs, easy to close ranks and loose or amend data. Would rate as a very real problem. Difficult to quantify, as we wish these details not to be made public as this leads to legal claims. It happens more often than the public perceive (ID14, Round 2).
>
> This happens particularly when threat of litigation. Clinicians protect themselves (ID14, Round 3).

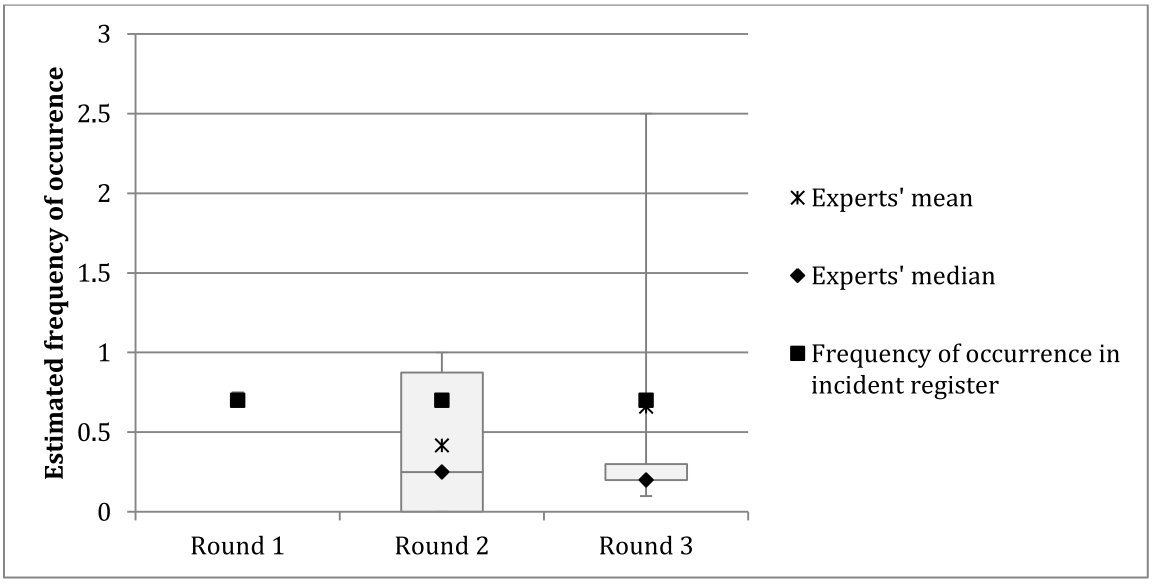


Figure 6-25 Distribution of estimated frequency of occurrence (scenario 19)

6.3.3 Risk map

The final output after the Delphi study is a risk map. This risk map is an overview of risk scenarios and their expected frequency in the future. It is created by calculating the average of the experts' mean after Round 3 and the frequency of occurrence in incident register. The map is a hypothetical model of which scenarios could be expected in a participating organisation in the near future. Figure 6-26 shows the 19 most important scenarios and the expected frequency and damage on a grid. The numbers on the map refer to the following scenarios:

1. Unattended asset goes missing: an internal employee located on the premises leaves an asset unattended and consequently the asset goes missing. The asset contains personal information of a few patients.
2. Password, user ID or access token sharing: an internal employee located on the premises shares his log on credentials leading to disclosure of patient information to an unauthorised person.
3. Email to unauthorised recipient: an internal employee located on the premises sends an email to an addressee unauthorised to access the patient data included, and consequently discloses the personal details of a few patients.
4. Theft on the premises: the theft of assets from the premises, containing personal data from 10-99 patients.
5. Procedure not followed: an internal employee located on the premises does not follow the formal procedures leading to disclosure of patient information.
6. Wrong privileges set: an internal employee located on the premises was given the wrong authorisations/privileges, causing disclosure of personal patient information to unauthorised persons.
7. High impact mistakes: an internal employee located on the premises makes a mistake that affects the security of 1,000 to 9,999 patient records.
8. Working in a public place: staff working in public place with a laptop or talking and being overheard or seen, leading to the disclosure of personal data of a few patients.
9. Unsecure remote 3rd party: an employee in a third party supplier or subcontractor makes a mistake when using remote access from home or office and discloses patient data, affecting 100-999 records.
10. Transportation: an unknown person breaches security by copying personal data on a storage medium and transports this medium out of the premises, affecting 100-999 records.

11. Family breach: a family member or carer of a patient accesses the unattended patient record without authorisation to gain knowledge about the patient.
12. Backup medium goes missing: the loss of a portable backup medium during transport to the offsite storage facility, containing the full database of patients' records, affecting more than 10,000 patient records.
13. Improper disposal: an employee in a third party supplier or subcontractor is not taking due care when clearing out a building or destroying records.
14. Third party discloses data: an employee in a third party supplier or subcontractor copies and discloses personal data, affecting 1,000 to 9,999 patient records.
15. Unsecure remote working: internal employee loses data through an unsecure remote working environment.
16. External groups: incidents involving external groups or activists wanting to steal, access, abuse or manipulate personal data.
17. Trainee breach: a trainee unintentionally accesses a patient record without authorisation.
18. Patient's home: an internal employee causes a security breach of a patient record at a patient's house.
19. Covering up errors: staff makes changes to data, reports or notes to gain status or to cover up medical errors.

The forecasting ability of the map was tested in a case study. The aim was to discover if the incident scenarios that occurred in the case organisation fall in the same quadrants as the scenarios on the map. Chapter 7 discusses these results.

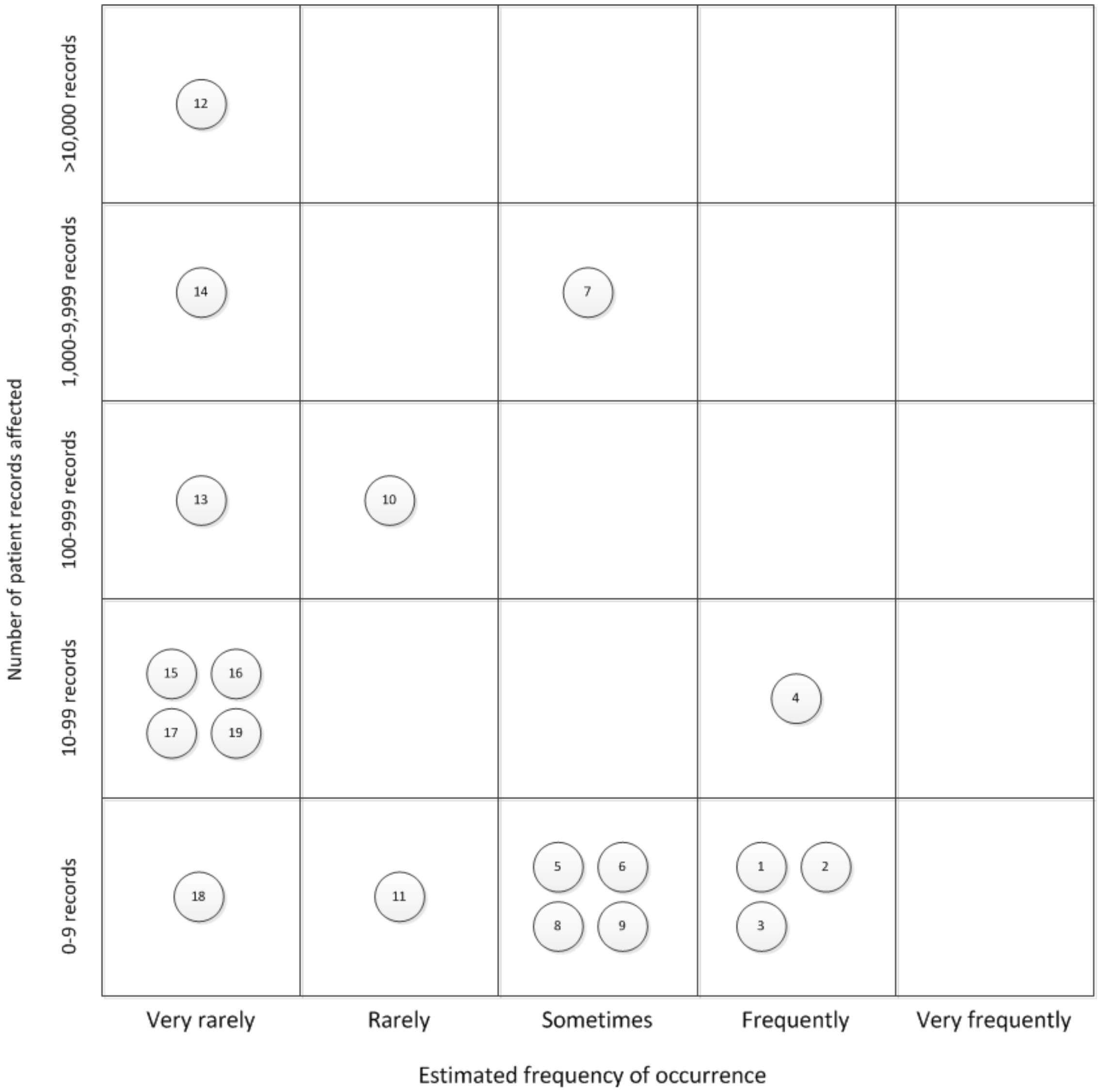


Figure 6-26 Risk map of expected security risk scenarios

6.4 Conclusion

This chapter demonstrated the use of the HI-risk method and explained how each step in the development was completed. It was shown how the different research methods each delivered data that was used to perform the method. The classification, which is the foundation of the incident registration, was presented; it was shown how the scenarios were calculated by means of tree mapping; and the results of a three-round Delphi study were presented. The final output was a risk map with the 19 most important scenarios. This risk map was tested in a case study and the results of that test are discussed in the next chapter.

7 Case study test results

7.1 Introduction

The previous chapter resulted in a risk map (presented in Figure 6-26). The risk map showed the estimated frequency of occurrence of 19 scenarios. The accuracy of these estimations and the completeness of the risk factor classification in Table 5.6 were tested in a case study. The case study was performed at the Speech and Language Therapy (SLT) department in a large hospital in the UK and included interviews, observations, documentation study, a survey and an analysis of incident data. Details of the approval process and the methodological design of the case study were described in section 4.4.4 of this thesis. This chapter now reports the results. The first section describes the setting of the organisation where the interviews and observations were held. Then, the next section discusses the results of the quantitative analysis of incident data. Finally, the results of the interviews, observations and survey are discussed and it is explained how these results influenced the risk factor classification and how the findings relate to the research literature. In the conclusion of this chapter it is stated that it is possible to state that the HI-risk method could be a helpful approach to information security risk forecasting.

7.2 Setting

The observed department operates from a number of separate locations. The observations and interviews were held at two different sites. Site 1 is a modern building that was recently opened. In contrast, site 2 is an older building that will be closed within a couple of years. This contrast in settings provided valuable input for the test of the classification of risk factors, as it was possible to observe similar processes being performed in very different environments.

At the time of the visits, the department was in the transition from a paper-based case notes system to an electronic patient record system. This transition made information security an important topic of discussion amongst staff. All staff that was involved in the research were cooperating enthusiastically.

The interviews were held with the Information Governance leads for the department (further indicated as Interviewee 1 and 2). They have not been involved in the development of any corporate policies but they are responsible to ensure that the department adheres to the policies. The structure within the department is that one lead takes responsibility within one area of the services and they are working together with clinical specialists and take people on board to help with the process at certain times. They have been charged to review all these policies and to find out how they relate to their working practices. There is regular communication with the IT security manager to gain advice about the implementation of the policies and for situations that are not covered by the policy. For instance, typical for the department is the use of voice recordings as part of their therapy sessions. Specific guidelines on whether these recordings are part of the medical record or not, had to be created.

The Information Governance leads work close together with the IT security manager. The IT security manager was interviewed at his office and provided the incident data to test the HI-risk forecast. The IT security manager reports to the Information Governance manager.

7.3 Quantitative analysis of the incident data and risk forecast

The case organisation supplied an overview of 512 security events registered by the IT service desk and a number of additional incidents that were registered by the security manager over the years 2011 and 2012. This timeframe was selected because the risk map was based on data collected in 2010 and 2011 and thus would forecast the risks occurring in 2011 and 2012. The registers included incidents from the whole organisation, including the SLT department. As this department is quite small in relation to the organisation as a whole, individual incidents for this department were not analysed separately because there was not enough data available.

The list of events in the case organisation was interpreted and translated into the HI-risk classification, identical to the previous research step when the incident data of NHS organisations was entered into the database (as described in section 6.2). It appeared that the IT service desk registered security events that did not count as an incident. Examples of these events were registered calls from users asking for advice or ordering assets. After careful consideration, a total of 503 events were analysed.

The analysis was performed in two ways. First the frequencies of security risk and incident factors (as listed in Table 5.6) that occurred in the case organisation were compared against the frequencies in the database of past incidents (which was presented before in sections 5.5 and 6.2). The frequencies were compared as percentages of the total and in absolute numbers. Then, the incident scenarios of the case organisation were placed on the risk map (Figure 6-26) to compare them with the positions of the scenarios that were forecasted.

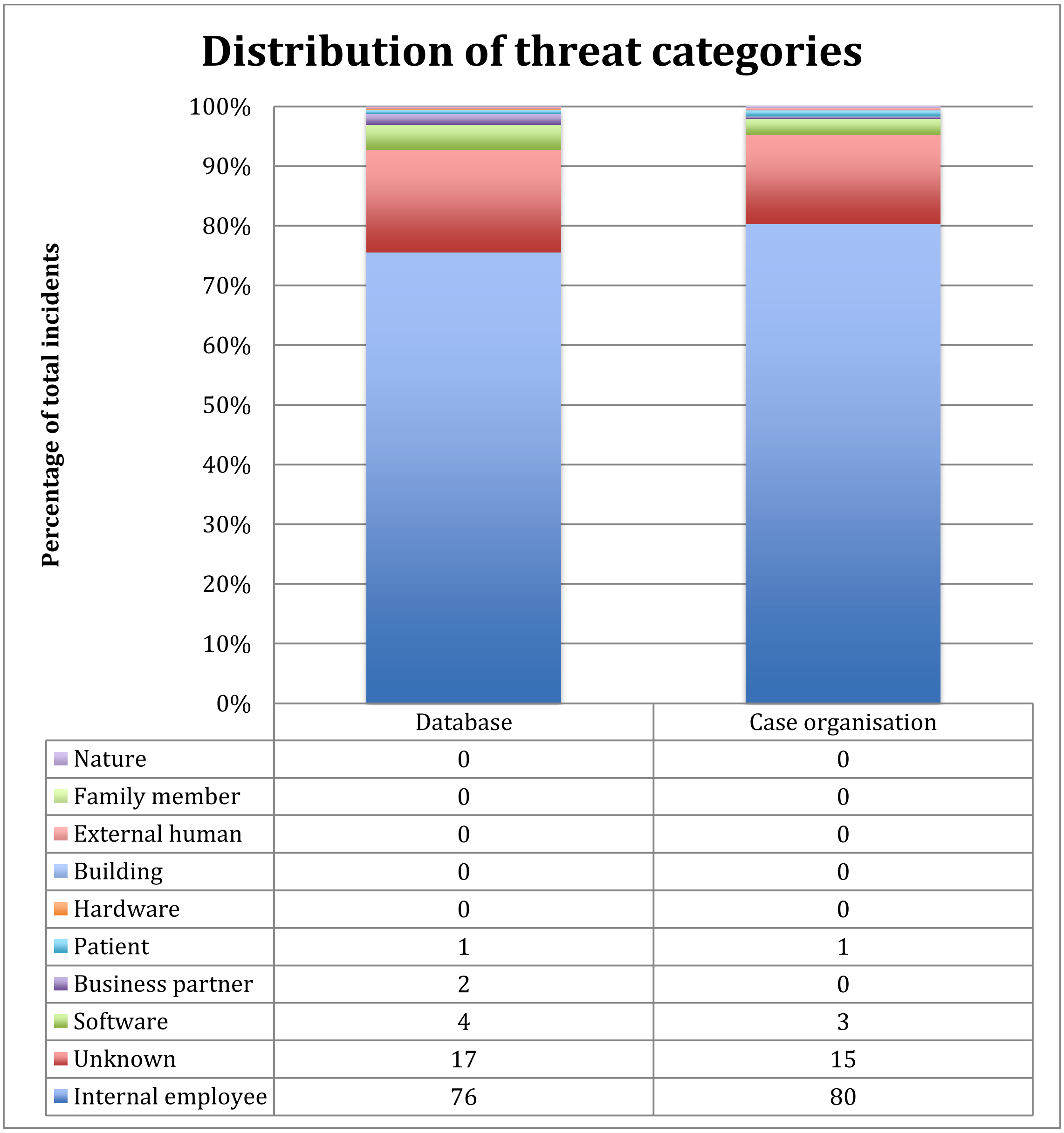
7.3.1 Comparison of frequencies of risk factors

The classification of security risk and incident factors (Table 5.6) contains 5 main categories: threat; method; weakness; event and damage. For each category, the relative frequency of occurrence of each sub-category (the percentage of the total incidents that would fall into the shown sub-categories) was calculated from the numerical counts (frequencies). These percentages express the frequency as a proportion of the whole. Percentages tend to be easy to interpret and a good way to compare between categories. The distribution of frequencies in the incident database was compared with the distribution in the case organisation.

For the categories threat, method, weaknesses and events, the case organisation showed a similar distribution of sub-categories as the database (Figure 7-1 to 7-4).

The distribution of threat categories in the database was presented before in Figure 6-2 as a pie-chart. Figure 7-1 now visualises the same proportions of frequencies in the database, and compares them with distribution of the categories in the case organisation. The case-organisation shows a very similar distribution of proportions. For instance, the sub-category **internal employee** was involved in 76% of all incidents in the past. In the case organisation, 80% of the incidents involved internal employees. The other sub-categories showed that the case organisation experienced very similar relative reported frequencies as compared to the database.

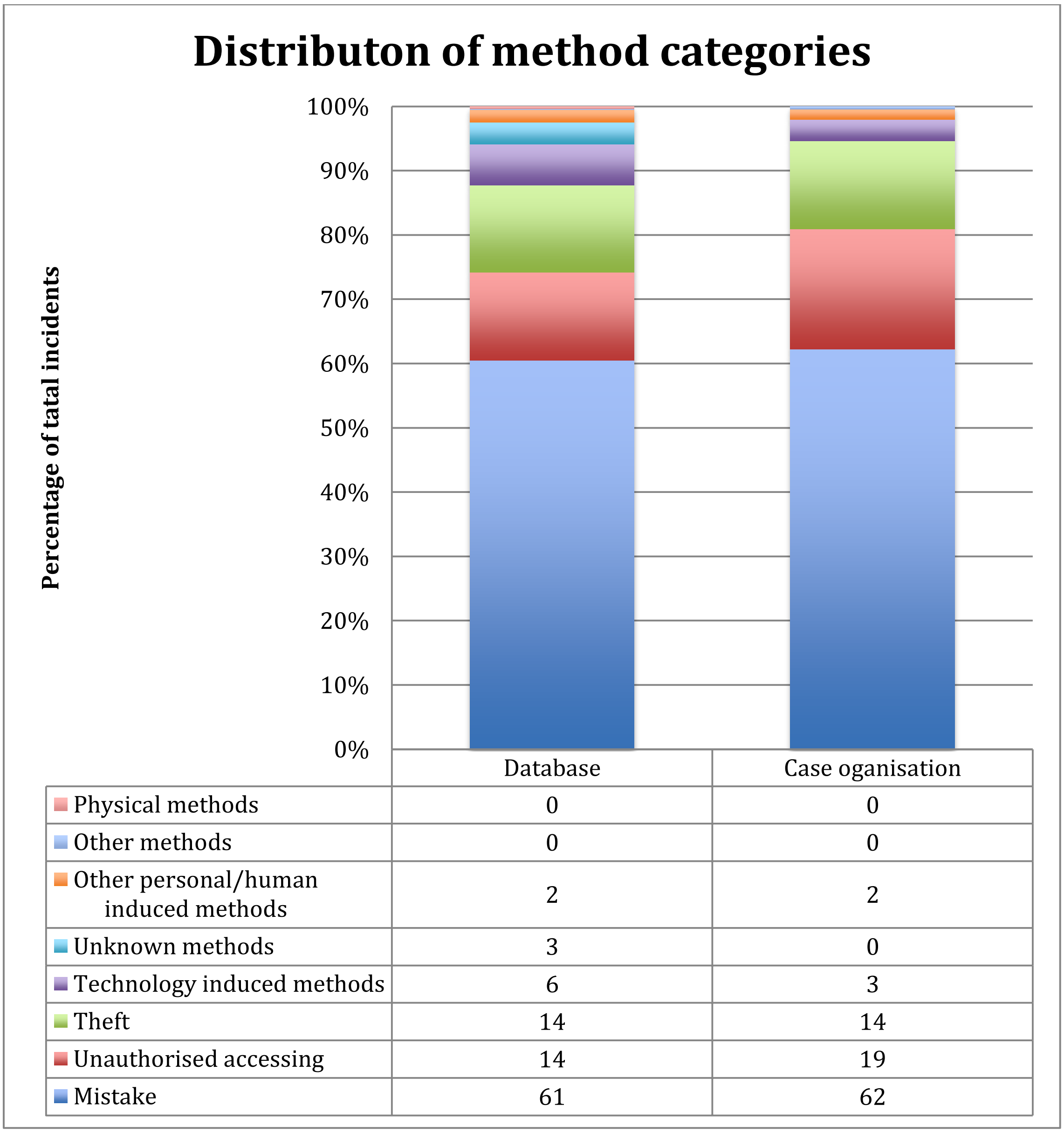
Equal patters are shown for method, weakness and event (Figures 7-2 to 7-4). The categories for damage could not be compared, as the case organisation did not register details about the damage that was suffered. Most incidents would classify as near misses or very low impact incidents and were therefore registered within the sub-category of **0-9 records affected**.



	Database	Case organisation
🟪 Nature	0	0
🟩 Family member	0	0
🟥 External human	0	0
🟦 Building	0	0
🟧 Hardware	0	0
🟦 Patient	1	1
🟪 Business partner	2	0
🟩 Software	4	3
🟥 Unknown	17	15
🟦 Internal employee	76	80

Figure 7-1 Distribution of threat categories

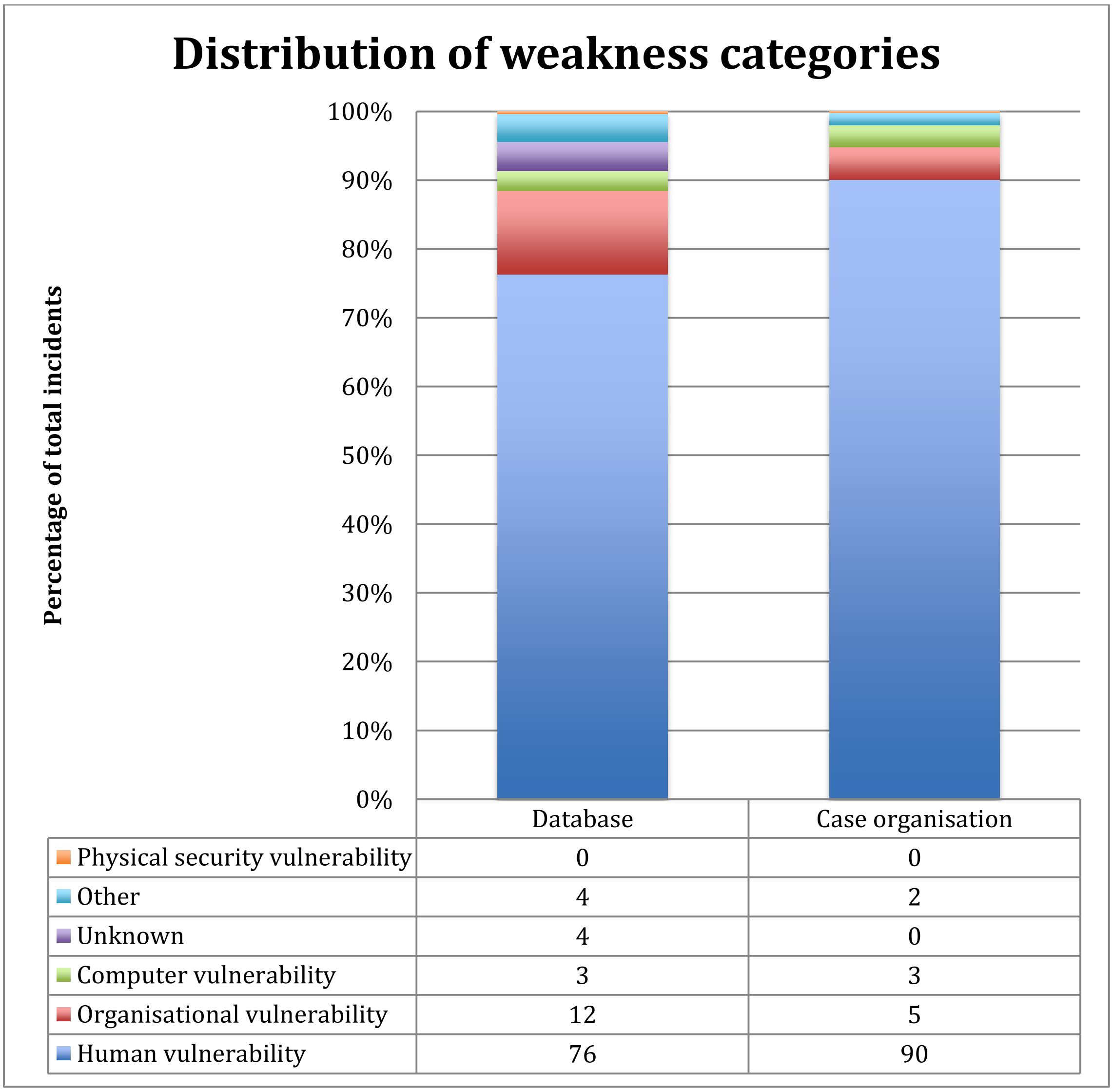
One noticeable difference between the database and the case organisation is that the case organisation did not register any **unknown methods** (Figure 7-2). This may be caused by the professionalism of the registration of incident by the service desk. The description of security events was complete in all of 503 analysed events, while the database of past incidents contained some unknown methods when the registering organisation did not know (or did not investigate) what caused the incident.



	Database	Case oganisation
🟥 Physical methods	0	0
🟦 Other methods	0	0
🟧 Other personal/human induced methods	2	2
🟦 Unknown methods	3	0
🟪 Technology induced methods	6	3
🟩 Theft	14	14
🟥 Unauthorised accessing	14	19
🟦 Mistake	61	62

Figure 7-2 Distribution of method categories

The distribution of weakness categories (Figure 7-3) shows that human vulnerabilities are the largest portion in both datasets, but that the case organisation registered relatively more human vulnerabilities than the average in the database. The sub-category **human vulnerability** can be broken down into further detail to evaluate more precisely what caused this higher proportion. Table 7.1 shows the sub-categories and indicates that the largest proportion can be found in **procedure/policy not followed**. For the case organisation this could be important management information to relate to measures of control, such as process improvement plans, audits and information security awareness.



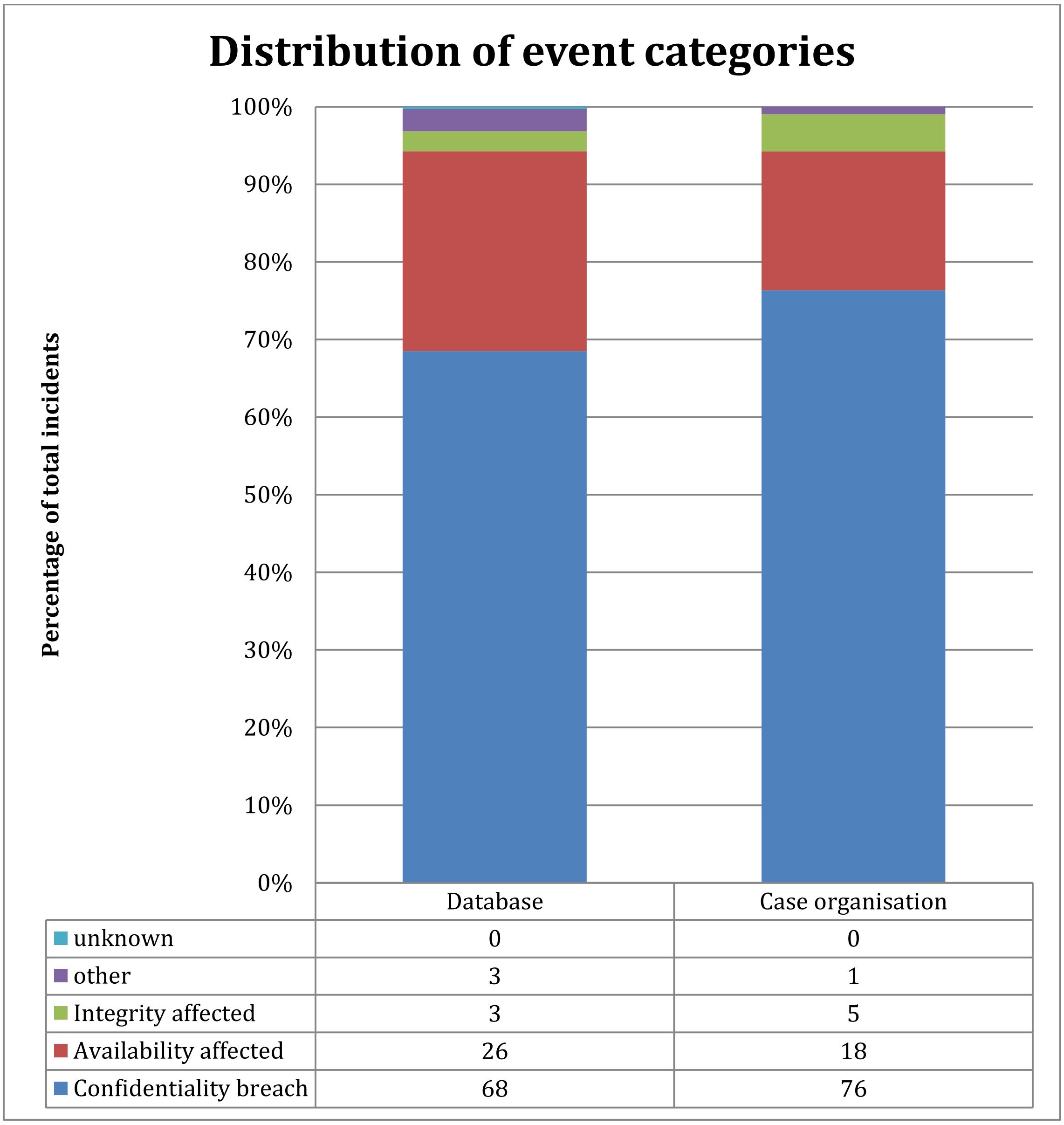
	Database	Case organisation
🟧 Physical security vulnerability	0	0
🟦 Other	4	2
🟪 Unknown	4	0
🟩 Computer vulnerability	3	3
🟥 Organisational vulnerability	12	5
🟦 Human vulnerability	76	90

Figure 7-3 Distribution of weakness categories

Table 7.1 Details of human vulnerability categories in case study

Human vulnerabilities	**Percentage**
Procedure/policy not followed (n=410) - Unattended asset or record (86) - Security facility not used (0) - Sharing of password or access token (71) - Sharing personal details with IT support (218) - Unsecure disposal of data carrying assets (1) - Other (34)	91%
Situational circumstances (1)	0%
Mistakes (42)	1%
Mental state of staff	0%
Unknown	0%

The distribution of event categories (Figure 7-4) again shows a similar distribution, with a slightly smaller portion in the category **availability affected**. This is caused by a lower frequency of **loss of data/asset** (a sub-category of availability) in the case organisation, as compared to other organisations in the database.



	Database	Case organisation
🟦 unknown	0	0
🟪 other	3	1
🟩 Integrity affected	3	5
🟥 Availability affected	26	18
🟦 Confidentiality breach	68	76

Figure 7-4 Distribution of event categories

The comparison of the distribution of categories showed that the distribution of frequencies over the categories showed similar patterns in the case organisation and in the database with incident data from a large group of comparable organisations. This could indicate that policy makers and healthcare organisations are likely to benefit from sharing and aggregating information security incident data, and use data analysis to decide on which areas should get priority when investing in risk controls.

The HI-risk model not only gathered incident data from a group of organisations, it also uses expert knowledge to further improve the reliability and to make forecasts. As we have seen, by means of a three-round Delphi study, an expert panel analysed the knowledge from the database and the two sources were combined to form a forecast on a risk map. The next section reports from the test that aimed to prove that this combined knowledge risk map delivers an accurate risk forecast.

7.3.2 Risk map test

The map of risk scenario forecasts (described in section 6.3 of this thesis) was compared with the case organisation's incident registers of 2011 and 2012. The aim was to test the hypothesis that:

> The frequency of occurrence of the incident scenarios in the case organisation falls within the same range of expected frequencies generated by the HI-risk method.

The positions of the scenarios on the risk map study were compared with the positions of the scenarios from the case organisation. The results are presented on the risk map in Figure 7-5. The scenarios from the case organisation are presented by a square and the original forecasts are shown in circles. The numbers in the circles/squares refer back to the numbers of the scenarios listed in section 6.3. It is visible that there occurs some overlap and some differences.

Not all scenarios from the map occurred in the case organisation. Only scenarios 1 to 6 and 16 (as listed in section 6.3.3) could be compared. The scenarios 5, 6, and 16 are positioned in the expected range. It is clear that scenarios 2, 3 and 4 happened more frequently than expected and scenario 1 occurred less frequently. Scenario 4 and 16 had a lower number of records affected, but this is explained by the fact that the case organisation did not register the damage and therefore all incidents fell in the '0-9 records affected' category. The differences of the scenarios 1 to 4 are discussed in the next sections.

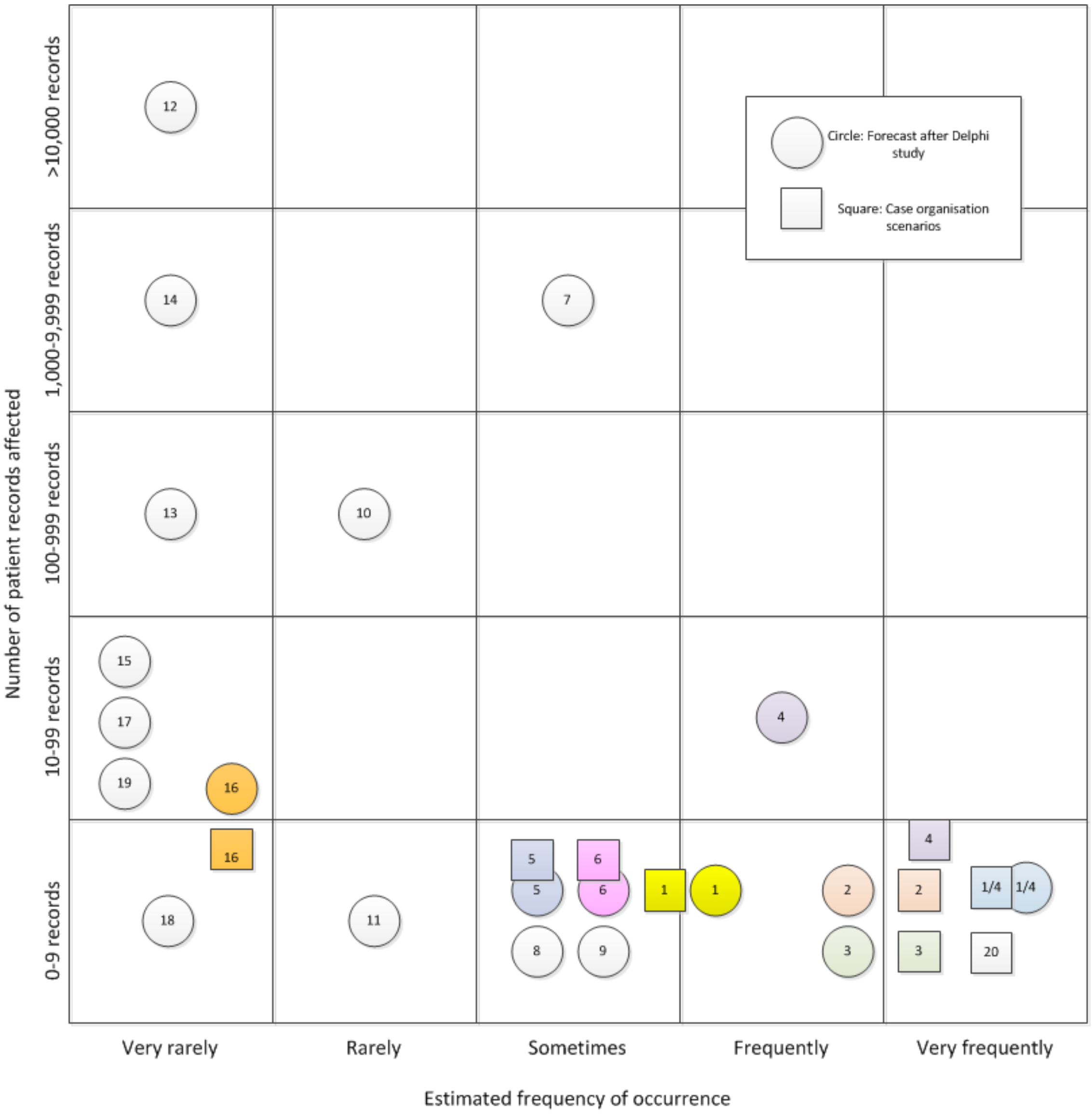


Figure 7-5 Case organisation's incident scenarios positioned on risk map

7.3.2.1 Discussion of scenario 1 and 4

The scenario where unattended assets go missing (scenario 1) occurred less frequently than expected in the case organisation, while scenario 4 (theft of assets) occurred more frequently. The case organisation made a distinction in their incident register between burglary from the premises and missing assets and that made it clear to make the distinction between these scenarios. This is also shown in the organisation's data breach policy, the policy in which it is explained to staff what to do in case of an incident, as it mentions the loss or theft of data as one type of incident that needs to be reported:

> The loss or theft of personal identifiable data, whether held on paper or electronic form must immediately be reported to your Line Manager/Director

> and notified to the Information Governance Department […] in the first instance (p.5 section 4).

However, in an earlier stage of the research, the expert panel pointed out that it is often difficult to identify a missing asset as stolen or being lost. They stated that in many organisations these incidents are being treated as one scenario. For that reason, it could be that the database of past incidents is somewhat 'soiled' because the data that was put in was not always completely certain if an asset was simply mislaid or stolen from the premises. That could be an explanation for the 'gone missing' category having somewhat higher frequencies than it should have as it includes unclear cases as well.

To rule out this distortion, a recalculation was done by treating scenario 1 and 4 as one scenario. After combining the two possible scenarios into one, the combined scenario (assets going missing or being stolen from premises) from the database would be placed in the 'very frequently' grid (18% of all incidents). A similar result would happen for the case organisation, as the combination of the scenarios places it in the 'very frequently' grid as well (15%). In Figure 7-5 this combined scenario is indicated with blue figures with the number 1 / 4.

7.3.2.2 Discussion of scenario 2

Scenario 2 (password, user ID or access token sharing) happened more frequently in the case organisation. The organisation is aware of that risk and it is being reported frequently to the IT service desk. From the interviews, it was learned that a possible explanation of this higher occurrence could be the recent history of merging 9 organisations together, leading to the current situation where the IT systems are not yet fully integrated and subject to migrations and changes:

> We are a conglomerate of 9 organisations. Each organisation had its own IT people and policies and procedures. We are still trying to integrate different areas. Our organisation is so big and some controls are fundamentally missing. We have no HR system; we don't know who is who. That is why we have no single-sign on. Once our systems are better we will be able to know our organisation better, and then we will be able to understand our risks better. In healthcare we need access to many more different systems than in other types of organisations and users find it difficult to remember all the different passwords (IT Security Manager in interview).

The higher frequency of occurrence of scenario 2 in the case organisation is explainable due to temporary circumstances after organisational changes. It is expected that the scenario will occur less in the future, when all changes stabilise. For future estimations, it remains important for the expert panel to be knowledgeable of changes in the healthcare system and of any foreseen mergers of health boards. Plans for large scale changes influence scenarios like these, and should affect the experts' estimated frequency.

Within the SLT department, this scenario was also recognised. There had been some password sharing in the past:

> There has been some password sharing at times in the past, but not to access patient information. It was to access our stats. But I am aware that there is a risk if you have a culture of password sharing (Interviewee 1).

The department is also aware that the risk remains high in the near future:

> We are moving very soon to an electronic case note record. Some principles about security will still maintain but they will be interpreted differently within an electronic record than they would be with a paper record. That will be a big change for our security management. There will be a different emphasis; we will look at logging off and passwords instead of locking case notes at night (Interviewee 2).

This scenario is likely to be temporarily regarded as a higher risk in the case organisation than was forecasted by the HI-risk method, and it is expected to lower once the new organisation has settled down.

7.3.2.3 Discussion scenario 3

Scenario 3 (email to unauthorised recipient) occurred more frequently in the case organisation. Staff report system or user errors to the service desk by email. In the email they explain that there is a problem with a record of a patient and they include the name, number and sometimes diagnoses in the email. The organisation is aware of that scenario and the service desk staff register these as events as security incidents. The IT security manager always talks to the staff involved, with the aim of educating them and to prevent it from happening again. The high frequency in this case is very likely caused by concise registration and high awareness of this specific event.

> One of the most frustrating things that keeps happening is that our Service Desk is an external company. When something is faulty with a record, staff is not allowed to share this information with the Service Desk, but they do. The Information Commissioner has said we can't do it, the Caldicott Guardian has said we can't do it and they still do it (IT Security Manager).

Scenario 3 includes all situations where confidential information is sent to persons who are not authorised to receive that information. The scenario in the case organisation, where the email was sent to a specific unauthorised group of people (the IT service desk) also occurred in the database of security incidents from the NHS organisations (as discussed in section 6.2 of this thesis). This led to the conclusion that scenario 3 could be split into two scenarios:

1. Email containing confidential or personal identifying data sent to IT service desk (scenario 20).
2. Email containing confidential or personal identifying data sent to other unauthorised recipients (scenario 3).

After this correction, scenario 3 fell in a closer range to the expected frequency. The new scenario, numbered as 20, is a security risks scenario that could provide interesting feedback to other organisations. The fact that the case organisation registers these scenarios separately might trigger other organisations to evaluate the situation at their IT service desk, and to analyse if they experience identical breaches of the Data Protection Act but just have not realised that yet.

7.4 Test of the classification of security risk and incident factors

The classification of security risk and incident factors (as shown in Table 5.6) was evaluated for its completeness and usability during the observations, interviews and a review of the organisation's security policies. These research activities provided the model with important additions and healthcare specific vocabulary for the classification. Every change to the classification was compared to the classification requirements of Amaroso (1994), as listed in section 5.4 of this thesis.

7.4.1 Findings from observations

During the observations on site 1, a post-it was observed on the wall behind a computer in a consultation room. It had a user ID written on it and a combination of numbers/letters written underneath it (resembling very much a password). If this was a real and working user ID/password combination, this particular event would fit into the existing classification under the existing element: 'sharing of user ID, password or access token'. Furthermore, this event would also fit in the category 'procedure not followed' as the organisation has a policy against sharing passwords and against writing them down. To improve the classification and to ensure that the categories are **mutually exclusive**, it was decided that 'policy or procedure not followed' is a sub-category of 'human vulnerability' and the sharing of passwords is an element within this sub-category. This reorganisation improved the organisation of the whole 'human vulnerability' category, as it forced the other elements to be regrouped into sub-categories as well and improved the **exhaustiveness** of the sub-categories.

Another observation on site 1 was that a staff member's Personal Development Plan (PDP) folder was on the shelf in a shared staff room. A PDP folder typically includes personal data about skills development and personal strengths and weaknesses that are part of someone's development and could be potentially considered private to the person involved. The data item type 'Employee's personal information' exists in the model and storing this data item unsecured could lead to an incident when the folder goes missing or is accessed by someone.

On site 1, storage boxes with patient case notes that had just been moved from another site were stored in an office that is not locked during working hours. There was no facility to store these paper records at the time of observation. The office is accessible by patients and staff and during the observations I could walk in and out of the room without being seen by staff. The category 'physical security vulnerability' did not include this element and 'Storage facility' was added as a sub-category with new elements: 'lack of lockable space', 'lack of secure filing cabinets'. When a door lock is installed but not used by staff, this event would fall under the category 'procedure not followed'. A general element was added: 'security facility not used'. This observation also led to an adjustment in the category: 'organisational weakness' where 'relocation to new site' was added. Overall, this observation led to improvement of **exhaustiveness** of the physical security category.

A final observation on site 1 was a computer that was not logged off or password locked. It displayed patient's information on the screen and on the desk in the staff room, where I was able to walk in and out of the room without being seen by staff at that moment. I was alone in the room for about 5 minutes. Not adhering to clear desk policies falls under the existing category 'procedure not followed'. Even if the user forgets to manually lock the screen when walking away for a short while, the computer should automatically lock itself when idle, which is a basic security control that can be set by any computer user. This event would fit into the new category mentioned about: 'security facility not used'. In combination with a lack of physical security controls, this event could potentially lead to a risk. As a result, the category 'lack of visual control on entrance point' was added as an element under 'physical security vulnerability', meaning that people could walk in and out of the area without being seen. Although CCTV was installed in the main corridor, there were no cameras after the entrance door to the department. The absence of visual control on the door could also potentially cause a safety risk to staff.

In the main entrance hall of site 1, there were many people walking in and out to different areas. I noticed volunteers and technicians walking around freely into different parts of the building and all sorts of people were carrying all kinds of documents and devices (papers, boxes, handheld devices). In the threat category ‘initiator’ added: ‘volunteers’ to ‘internal staff’ as well as ‘technicians’, ‘cleaners’, ‘IT staff’ and ‘restaurant/catering staff’. During the observations, I realised that I myself was a potential threat to the organisation as well. I had visible access to several weaknesses of the organisation. Therefore the element ‘researcher’ was added. Healthcare organisations and patients are constant topics of research and the integrity of the researchers and their manners to keep research data secure is an important element to information security. Adding these sub-categories is **useful** to gain insight in to initiators of threats and incidents.

On site 2 the work environment looked messy as the building showed broken ceilings, buckets to catch water from leaks, tables and shelves full of papers and stuff. In a ‘messy environment’ assets can be lost or damaged easily. A ‘messy environment’ can be caused by not adhering to clear desk policies, the individual’s work practices or by the deterioration of the physical space itself. The classification was expanded with ‘untidiness’ to ‘human vulnerability’ and ‘lack of maintenance to building and facilities’ to ‘physical security vulnerability’.

In the public entrance hall on site 2 there was an open door (held open by a door stopper), giving a visual of a corridor where paper patient records were piled up against the wall waist-high over a length of about 3 meters. There were numerous people in the corridor and the offices facing that corridor. With my sponsor [NHS term for contact person], we walked through the corridor without being stopped or questioned. This situation was not classifiable in the model before, but is now covered with the new elements that were added as noted above: in the category ‘physical security vulnerability’ as: ‘lack of lockable space’ and ‘lack of secure filing cabinets’ and in the category ‘human vulnerability’ as ‘security facility not used’.

On both sites it was not always easy to identify visually who is staff, or who is a patient, carer, researcher, vendor and so on. This is a general security risk in public buildings that could have indirect implications for information security. When a healthcare organisation is located in an area with high criminality levels, the characteristic openness of this organisation could make it an easily accessible target with many vulnerable people inside. The classification was **lacking** this element and therefore, in the treat category 'social' it was added: 'regional/national security alert state' and 'regional crime levels'.

7.4.2 Findings from documents review

Some changes were made to the classification after examination of the organisation's policies. The case organisation allowed insight in a number of policy documents related to information security. These documents led to the addition of a few specific elements to make the classification more **exhaustive**. The social media policy led to the addition of the element 'social media' to 'method', as social media can be used as a method to disclose data. The 'E-mail acceptable use policy' led to some new elements. In the 'possible damage' category: feelings of anxiety, humiliation, awkwardness or distress. Additional methods were added, such as: verbal threats, offensive jokes, offensive language, personal comments about a person's physical appearance or character. Finally, to 'event' was added: 'breach of ethical norms or code', with sub-classes: spreading illegal material, publication of harmful material. In the background chapter of this thesis (chapter 2), these issues related to norms and values were already identified as influential to the perception of dangers and annoyances as information security risks.

7.4.3 Findings from interviews

A few final changes to the classification were made after the interviews to make the classification more **useful** for healthcare and better **accepted**. Some elements were added in the category 'data item': Medical recordings: illustrations, video, voice, scans, x-rays, photos, ultrasound picture. Furthermore, after one of the interviewees mentioned that 'case notes were not delivered in the right location by the porters', the new element 'porters' was added to the threat category 'human'. Finally, the interviews provided additional confirmation of the importance of security facilities and of the environment on information security risks:

> One of the reasons for different practices was also caused by the environment of the different buildings, some areas are very enclosed without other people walking in the area, but here with CCTV in the corridors and an extra external door it is not likely that anyone wanders in. We have been aware of where boxes of discharged case notes have been stored maybe not properly locked up, but we did not have anywhere to put them away properly in some sites (Interviewee 1).

> We had an incident with an answering machine close to the waiting area for patients so when someone left a message it would have been possible for the patients to overhear that. That was typical for the site because of the building (Interviewee 2).

7.5 The future of information security risks in healthcare

Opinions from information security staff and information governance staff about emerging risks in healthcare and about some of the features of the HI-risk method were gathered during the interviews and through a short survey.

Healthcare experiences many developments in systems for patients that are linked to the web and to devices that connect to it. Risks are foreseen in all stages of the lifecycle of these developments.

Risks can be controlled as well as triggered from national policies. Changes in national policies cause changes in the healthcare organisation and staff has to adapt to each change. Furthermore, on a national level is where 'thinking ahead' is important so that healthcare can prepare for future developments in technology and policy. Future-proofed, clearly described, international, and tougher national information security policy is deemed needed to form a foundation for risk management in healthcare.

> We have not been thinking ahead enough. Nationally we are not quite there. National policies are a risk in a way as well; if policies change we will have to tell the staff. The names that are used in the new marking scheme (as imposed from national level) are inconsistent and different from ours. It will have repercussions for us, as it will change how we handle information. It was protected and suddenly it is not protected (IT Security manager in interview).
>
> Government is likely to merge health boards. If this happens the information about each patient will be accessible by a significant number of people. This is both good and bad - good that the patient can be treated in a wider range of locations and their records more readily shared by the staff looking after the patients, but bad in that the information may be inappropriately accessed (Respondent A, survey).
>
> Tougher regulation regime, increase in fines available to the ICO Inspection/audit regime of IT for healthcare organisations, similar to financial audits. Tougher penalties for those convicted of breaching data protection/computer misuse acts. More international cooperation on cybercrime, scope needs to be global (Respondent B, survey).
>
> Government policy is encouraging systems to open up to allow patients to see information but not on how much or where or how (Respondent C, survey).

Budgets allocated to health boards are seen as an important factor to manage information security risks.

> The risks depend on the finances of the health board (Interviewee 1).

On the organisational level, information security policies, budget and time continuously influence compliance and risks in the departments.

> We were trying to harmonise procedures, they had been risk assessed some time ago and not in line as we were doing it. And we did it in a period that a lot of new policies were coming out: as soon as we finished one there appeared another new policy (Interviewee 1).
>
> If staff could have time, there are competing pressures. The priority for information security varies from person to person. Rather than just giving the folders and taking a part of the time in a meeting, if we could spend more time we could get their buy-in more. Ideally, people are more likely to use the good practice if they understand the risks. It has to be embedded in their thinking (Interviewee 1)

Security risks need to be assessed and solved during the development phase of new technological solutions to support care processes. However, some security risks cannot always be solved.

> Many developments are happening in systems for patients that have to access their data in order to monitor their test results and to manage their way of living. That is published on the Internet in a way they can have access and of course that will bring risks. There is more and more of that coming along. Tele-health is particularly important in the Highlands where there is no easy access to healthcare. There are a number of pilots going on. There are risks that go with that and not all of them can be solved (IT Security Manager).

All interviewees and survey respondents mentioned the same possible future risk: mobile devices, or i-things, or Bring Your Own Device (BYOD). These devices support the care processes in many ways and they may carry personal identifiable information, or have the potential to connect to the national network and systems in the organisation.

> Mobile devices and i-things will become an issue as well. We have things connecting to the national system as well and these have interesting security complications. Doctors have sometimes two devices, and this has not been addressed yet (IT Security Manager).
>
> Mobile devices, especially BYOD. I do not think that management will be able to differentiate between a specific mobile device being secure for one application but not another. In Scotland we are seeing systems being shared across health boards and between health boards. This is to the benefit of the patients, however it introduces a greater risk of information being inappropriately accessed. Monitoring the access will become more difficult (Respondent A, survey).
>
> Increasing use of BYOD, where users are wanting to use their own choice of computing platform Agile/flexible working, where sensitive information is with the worker, rather than kept at a place of work (Respondent B, survey).

> As more data is being made available for mobile devices, the security or loss of the device will be more significant than when it not is just about a phone or laptop with the data on it, but about the data it can get to (Respondent C, survey).

> That probably depends on the finances of the health board and what systems they have. They used to talk about people walking around with tablets and walking around making notes as they go from ward to ward. I suspect loss or theft of mobile devices could be the risk (Interviewee 1).

The outsourcing partners who support the IT processes in the organisation are a source of possible risks as well. It is not always clear where responsibilities lie and which controls partners have implemented. Furthermore, some technological solutions are hard to grasp:

> Cloud computing - outsourcing data to 3rd party providers, hard to identify any physical resource where the data resides (Respondent B, survey).

At the end of a lifecycle of a system or device, there is a risk that personal data remains in the memory of the asset. This causes a risk if the asset is not properly disposed of at the end of the lifecycle:

> IT Asset disposal - increasing number of devices have potential to hold data, either physical hard disk or flash memory - .e.g. tablets, smartphones, USB memory sticks, printers/MFD's, PDA's, etc. More important therefore to have adequate control on what is being passed for disposal/recycling and that any 3rd party involved is appropriately regulated and monitored (Respondent B, survey).

In the situation where a risk has materialised (an incident has occurred), it is considered important to investigate what went wrong, how it went wrong and who was responsible. This is not only important to prevent it from happening again, but vital in the situation where legal steps need to be taken:

> For exceptional circumstances in the future, we need a proper forensic investigation approach. When one person is misbehaving in one area, there are usually a lot of things going on. The way we now investigate things is not able to stand in a criminal court (IT Security Manager).

Auditing is also seen as a means to improve awareness and to prevent incidents:

> And time to audit, to look at how people make decisions on site and to make sure that it is continuing. That would take it forward. We are responsible for audit and it is part of the role that we have been given (Interviewee 2).

The future of risk management is seen in technological solutions, where the technology itself takes audit trails and can trace and erase assets.

> Databases/Clinical systems may start to have monitoring software to check on who and where rather than once you have logged in (Respondent B).

> Increasing use of ‘smart’ technologies:
>
> > - Network tools such as SCCM alerting to mobile assets not connecting for extended period, ‘fixed’ assets such as desktop PCs changing location as defined by IP subnet.
> >
> > - RFID tagging - Mobile devices with 3G tracked and if necessary remotely erased over mobile network (Respondent C).

> Ideally in the future you would have some the system saying: this patient is in your hospital and now you can access his record and if the patient is somewhere else, then that hospital can access the record (IT Security Manager).

> We have a system that takes audit trails. It can say who has looked at a health record of somebody (IT Security Manager).

> I would love a system; we are primarily clinicians and not experts in information security. If there was a tool that is user friendly and that would be better than our approach (Interviewee 1).

However, the boundaries, rules and policies that need to be defined before such tools are implemented, are human decisions made by management or governments, based on possible risks. To support those decisions, a formal risk management approach and mandate to take measures is still required.

> More formal risk management will be introduced and resourced. Currently there is in real terms little more than lip service offered. The powers of the Information Commissioner will increase and this will force the hand of management (Respondent A, survey).

The HI-risk method is characterised by certain features that could support a national risk management policy as well as an individual healthcare organisation. Table 7.2 illustrates how the respondents (n=3, as described in section 4.4.4 of this thesis) showed some interest in these characteristics.

Table 7.2 Survey results risk assessment features

Which of the following characteristics would you be interested in adding to the information risk assessment approach?	**Interested**	**Neutral**	**Not interested**
A comparison against risks identified by other organisations.	2	1	
A comparison of each risk register against the actual suffered incidents.	3		
A comparison against the opinions of security experts and trend watchers.	2	1	
A special list of human and organisation-related risks.	2	1	
A healthcare sector wide risk overview.	2	1	

A final remark is that all survey respondents and interviewees agreed that the information security risks in the case organisation are expected to be similar to the risks in any other NHS organisation.

> We all have the same worries, we share the same issues. Our risks are similar, our incidents are similar (IT Security Manager).
>
> There is certainly common ground within the profession; we all have the same worries about storing case notes and so on (Interviewee 1).

This enforces one of the basic concepts behind the HI-risk method: the assumption that healthcare organisations face similar risks and therefore can learn from sharing information about risks, incidents and possible controls.

7.6 Findings related to research literature

In chapter 2 it was argued that information security risks in society could be identified and better understood by studying information society discourse. From studying the works of information society thinkers such as Beck, Castells and Lyon, it was argued that the scope of information security risks is global and infinite, through the connections in socio-technical networks. Healthcare organisations in the United Kingdom are strongly networked through their national governance and the national infrastructure for health ICT systems. There are many regional collaboration structures between primary and secondary health and social care institutions. Their importance in society is felt by a number of groups such as patients, politicians, insurance companies, businesses and so on. For these groups it is not always easy to differentiate between individual healthcare organisations. For instance, patients might blame the NHS for a confidentiality issue that occurred at a local dentist. The survey respondents and interviewees in the case study confirmed this perception that related organisations deal with very similar risks and that a security event in one organisation may affect others. This was also reinforced by the similarity between the incident scenarios from the Delphi study and the security incidents suffered by the case organisation.

The background chapter also argued that traditional information security risk perceptions are limited in explaining risks that affect more than an organisation and its business, ICTs and staff. The global entanglement of people, ICTs, organisations and cultural norms and ethics calls for risk approaches that are wider than technology or business risks. An information security risk is not ‘a thing’ that can be singled out and contained. It is partly related to perception of dangers, norms, and values. This perception is socially constructed by international power systems and struggles, (lack of) public information policy, mass media and culture. Interviewees in the case study added the economic factor to risk perception. Time and budget allocated to healthcare staff are short and it was suggested that additional time to train staff in information security procedures and risk management contributes to more awareness and knowledge and thus helps to prevent incidents.

The conclusions of the literature review suggested that risks associated with information security in healthcare are not being systematically and consistently assessed beyond the scale of specific contexts. This was confirmed in the case study organisation: the IT department assesses the risks of certain systems and the clinicians assess the risks in the operational procedure. However, they do not bring these together nor do they compare their findings with other departments. Analysing risks within the context of a system or one asset is not meaningful in modern networked organisations. The context is infinite and includes technical, environmental and social (including people, organisation, society) factors.

Risk information is currently not gathered collectively, and the knowledge of healthcare staff and patients, security experts, and data from past incidents is not a part of the risk analysis scope of best practice methods. Participants in the case study indicated an interest in a collective registration and analysis and confirmed a shared exposure to similar risks.

The review of the literature about issues with confidentiality, availability and integrity of information provided some insight into negative information security events in healthcare. These were summarised in the traditional confidentiality, integrity and availability triad of information security:

1. Confidentiality events: patients avoiding care, financial loss, embarrassment/stigma or discrimination;
2. Integrity events: issues with quality of care, billing and patient safety;
3. Availability events: constraints to self-determination and patient empowerment, aging technology, information ownership and responsibility.

The findings from the analysis of the information security incident data, one of the conclusions of the background chapter (information security risk is partly related to perception of dangers and annoyances and norms and values**)** and the review of policy documents in the case study added a possible fourth negative event to the risk factor classification:

4. Breach of ethical norms or code: harm to the feelings of an individual as a result of the spreading or publication of illegal or harmful material.

Information security risks include technology risks, business risks and society risks and these risks influence and complement each other. This thesis took a socio-technical view on information security risks. The focus was on human factors influencing security (e.g. behaviour, motivation, ICT skills and so on) and it included factors from the environment that influence security (such as public policy, social norms and ethics, crime rates, building or neighbourhood security, and so on). These factors were identified by evaluating existing classifications of information security threat and vulnerabilities models and through interviews and observations of healthcare staff and their environment. In the interviews it was confirmed that environmental vulnerabilities could cause information security incidents.

7.7 Conclusion

This chapter reported the case study that included interviews, observations, a survey, and an analysis of the information security incident register. The observations and interviews led to a number of improvements to classification of information security risk factors. These improvements were mainly related to exhaustiveness of the categories, as some situations could not be fitted in the categories, and to the usefulness of the categories by adding healthcare-specific terminology. The analysis of the information security incident register made it possible to evaluate the forecasting ability of the method. It was shown that benchmarking of the incidents, which occurred in the case organisation, against the collective database of incidents support the analysis of the proportional contributions of variables to the total of incidents, but it cannot predict the absolute frequencies.

A more reliable forecast occurred after the combination of experts' knowledge with the knowledge derived from the collective database of past incidents. The expected and observed frequencies of occurrence were very similar. There were some minor differences in the expected risk scenarios. The differences could be explained by influences of the data collection method and the incident registration procedure in the case organisation.

The case study proved to be an important step in the research. The observations and interviews on locations gave additional insight in the reality of healthcare information security. It provided the ability to test the value of the HI-risk method and contributed significantly to its quality.

The subsequent chapter will conclude this thesis and describe potential future research directions.

8 Conclusion

8.1 Introduction

This chapter concludes the thesis and evaluates the progress towards achieving the objectives. The main findings of the research are pointed out as well as some conclusions on the research process itself. Lastly, suggestions for the focus of future research and development are given.

8.2 Evaluation of research objectives

This thesis explored information security risks in healthcare. The aim was to investigate the possibility of designing a novel approach that would enable organisations to learn lessons from each other and to unite in the prevention of recurring breaches. The requirements and objectives of the new approach were not clear at the beginning of the research project. The objectives were identified by the exploration of the problems with current traditional information security practice. Information security is a diverse discipline and the definition and scope vary amongst practitioners. A literature study into different lines of thinking was helpful to define the information security philosophy that forms the foundation of the new approach. Furthermore, healthcare is an industry that may encounter different information security problems than for instance the financial sector. Specific information security risks and issues in healthcare were researched by a second literature study and the results of both studies led to the specification of objectives of the new approach to information security risks in healthcare.

The first objective was to gather and evaluate information security incidents from multiple organisations and to discover the most frequently occurring scenarios. It was learned that it was not possible to use secondary incident databases for this purpose. There was not enough healthcare data available and the more generic reports about data breaches and survey reports that were collected with different classifications and taxonomies lacked detail. Eventually, this objective was met by an alternative approach to collect incident data from NHS organisations directly. The incident data was requested with reference to the FOI act. This led to a good response rate, but the researcher is aware that without the support of this legislation, it would have been very difficult to gather this data. The calculation of the most frequent scenarios was largely done in a spreadsheet, which was a laborious and slow process. The number of scenarios allowed this method, but in future situations when larger sets of data need to be analysed, this process should be automated to prevent calculation errors and to save time.

The second objective was to analyse and relate the contribution of social, technical and environmental risk factors to information security incidents. It was learned that a detailed analysis of incidents can only be performed if the incidents are investigated and reported in detail as well. From the 132 incident registers that were sent to the researcher, only 83 could be used in the analysis. Hundreds of incidents could not be added to the register because of the lack of detail in the reporting.

The method was able to analyse risk factors from different categories that occurred together. For instance, it was possible in most cases to count the co-occurrence of a single threat category, a single weakness, a single method, event and the damage. However, the method could not adequately analyse the co-occurrence of multiple sub-categories within the main categories of threat, weakness, method, event and damage. For instance, in the case that multiple threat factors occur at the same time, with multiple weaknesses, the frequency could not be calculated using the manual method. Furthermore, the incident registers were not detailed enough to actually discover any simultaneously occurring sub-categories, and in a future situation this limitation could create less accurate forecasts.

The third objective to involve experts in the forecasting was achieved through the Delphi study. The composition of the expert panel is an important factor in delivering reliable results. The panel was composed of 12 experts in information security, with many years of experience in healthcare, risk management and information governance. The selection of the panel was the most difficult objective to achieve, as the quality and enthusiasm of the experts is essential for the success of the approach. Most experts perform senior positions in organisations and it is a lot to ask for their commitment over three surveys. Fortunately, 10 experts completed all three rounds and they delivered a reasonably reliable forecast.

The last objective was to explicate risks in a clear and understandable manner. Describing risks in scenarios prove to be useful during the Delphi study. For two scenarios it became clear that several organisations find it difficult to differentiate between them. This concerned the example of scenarios when assets disappear and it is not clear if an item was stolen or just misplaced. For the purposes of the research project it was decided to combine these two different scenarios, but in reality this practice proves the above-mentioned issue with the lack of detail in the reporting of incidents. When a situation is not clear, an organisation should try to investigate in more detail what caused the incident, and not try to combine scenarios because it is easier.

The overall conclusion is that the main objectives were achieved at a reasonable level, mainly because of the reliance of legislation to gather the incident data, and because of the quality and commitment of the experts in the Delphi panel. A point of attention for the future is the often-lacking detailing in the incident investigation and reporting in organisations.

8.3 Evaluation of the research process

The HI-risk method was designed following the rigorous process of design science research. Hevner at al. (2004) state that for design science research to be effective, it must provide clear contributions in the areas of the designed artefact, design construction knowledge, and/or design evaluation knowledge (such as methodologies). Design science research holds the potential for 3 types of research contributions based on the novelty, generality, and significance of the designed artefact. According to the authors, one or more of these contributions must be found in a given research project. The following list shows these three types of contributions and relates them to the HI-risk method:

1. *The designed artefact*. The contribution of the design science research presented in this thesis is the artefact itself: the HI-risk method. This method provides a solution to learn from information security incidents, to share these lessons and enables policymaking and cooperation between related organisations.
2. *Foundations*. The creative development of novel, appropriately evaluated constructs, models, methods, or instantiations that extend and improve the existing foundations in the knowledge base are also important contributions. In the HI-risk classification of information security risk factors, existing knowledge is presented in a novel way and combined with new risk factors that were found in related disciplines and during observations of real environments.
3. *Methodologies*. Finally, the creative development and use of evaluation methods (e.g., experimental, analytical, observational, testing, and descriptive) and new evaluation metrics provide design science research contributions. The HI-risk method combines data analysis of past information security incidents with the Delphi method for experts’ forecasting of future incidents.

8.4 Main findings and contribution to knowledge

This research designed a new method to assess information security risks. The literature review had showed that few information security risk assessment methods developed specifically for healthcare exist (Appari & Johnson, 2010). Furthermore, at the start of the dissertation, a specific classification for healthcare that included social, technical and environmental risk factors could not be retrieved. In chapter 5 it had shown how a new classification was created to include these different conceptions of risk factors. The classification in the HI-risk method is based on a combination of existing classifications and improvements from interviews and observations in the case study. This part of the research has delivered a contribution to the existing range of information security risk classifications.

The classification is a tool that can be used to report and analyse the socio-technical information security incidents in healthcare. It can be used to compare the frequency of occurrence of a risk factor in an individual organisation with the average frequency of occurrence in similar organisations. It was found that counting frequencies of single security elements from a collective incident database forms a reasonable foundation to make indications of occurrence of these elements in an individual organisation. This insight can be used to evaluate why a certain incident occurs more or less often in one organisation, as compared to others and what measures of control should be invested in.

It was also found that the most frequently occurring threats came from either a member of staff or unidentified persons within the premises of the organisation. Accidental human mistake, theft of assets and unauthorised access to information were the most frequently reported methods in incident scenarios. Regular weaknesses that were exploited were unattended assets, issues with emails (technical security and user errors) and procedures that were not followed. Most of the negative outcomes of incidents could be related to confidentiality issues (disclosure of information); availability issues (loss of data or assets) and integrity issues (faulty data and contamination of systems with malicious software). The majority of the incidents (93%) led to compromises of the personal data of less than 10 patients, while incidents affecting huge amounts of personal data were reported to be very rare (0.14%).

A collective incident register can provide input for national or regional information policy. The classification in HI-risk included numerous people-related and organisation-related threats, methods and vulnerabilities. It did not include details for the computer and network security categories. As many good existing technical classifications exist, in the future these can be added to HI-risk without much effort.

A three-round Delphi study was conducted to gather experts' opinions about information security risk scenarios in healthcare. The estimations of the panel appear to agree with a number of future risks highlighted in industry reports. The most frequent scenarios are directly caused by human actions and related to human behaviour, management style, organisational culture and personal motivation. The risks associated with sharing data with third parties such as suppliers, outsourcing partners or other healthcare providers are on the experts' radar, thus showing a form of awareness of networked organisations and interconnectivity. One observation from the comments made by the experts and the scenarios they added in the blank sheet, is that none of the panel members indicated any risks linked to society, public policy or human-artefact integration (such as online patient monitoring systems, RFID chips or implants). This is surprising, as it was shown in chapter 3 that researchers have indicated that this is where information security experts should engage.

The Delphi study also appeared to be a learning curve for the participants. The combination of being informed from incidents in the past with continuous input from other experts in the field caused the opinions of the participants to converge over the rounds. This was visible in the frequency estimations they made as well as in the comments. Where in some scenarios the comments in Round 1 were very diverse, in Rounds 2 and 3 they showed more understanding of other opinions and some participants changed their own opinions. Delphi has proven to be a useful technique to support learning about emerging risks and could be used in a risk monitoring system that continuously is updated with the data from incidents and expert opinions.

The five most frequent information security risk scenarios that were found are:

1. Unattended asset goes missing: an internal employee located on the premises leaves an asset unattended and consequently the asset goes missing. The asset contains personal information of a few patients.
2. Password, user ID or access token sharing: an internal employee located on the premises shares his log on credentials leading to disclosure of patient information to an unauthorised person.

3. Email to unauthorised recipient: an internal employee located on the premises sends an email to an addressee unauthorised to access the patient data included, and consequently discloses the personal details of a few patients.
4. Theft on the premises: the theft of assets from the premises, containing personal data from 10-99 patients.
5. Procedure not followed: an internal employee located on the premises does not follow the formal procedures leading to disclosure of patient information.

Combining the scenarios with the experts' input created the risk map. The map forms a partially reasonable foundation to make predictions of the frequency of occurrence of these scenarios in an individual organisation. It was argued in chapter 7 that healthcare organisations face similar risks and incidents, while the frequency of occurrence differs in some cases. However, even with deviations in the forecast, the results of the risk map can still be inspirational to participants. Deviations can trigger an individual organisation to analyse why they have a deviation. It could mean that it is an area that they could improve on, or it concerns an area specific to other organisations that they have not identified yet and can learn from.

Overall, the HI-risk method has the potential to contribute to information security practice in healthcare because of the following characteristics:

1. It enables the benchmarking of information security events in one organisation against a group of similar and related organisations.
2. It provides a collective information security incident register.
3. It enables regional and sectorial information security incident analysis.
4. It methodologically gathers the knowledge of experts to identify future trends.
5. It provides input for organisational information security policy and for policy that covers a wider context.

8.5 Suggestions for future work

The HI-risk method shows some promising results as well as some indicators for improvement and future work. The activities were performed with the support of basic software such as Access and Excel, as no existing tool was either suitable or available to support the data analysis. This problem was overcome by a lot of manual data entry and manual data analysis by the researcher. Future work will focus on the development of an automated system for data entry and analysis.

The automated system could for example be used by information security officers, a panel of experts, or by policy makers. Figure 8-1 illustrates how these different users could be related to the system. In a participating organisation, the security officer registers all information security incidents in the system. This registration would follow the classification of risk factors that was presented in chapter 5. The system could provide reports and list of the organisation's incidents to the security officer for internal use in the organisation. The method assumes that multiple organisations use the system. The system automatically calculates the most frequent scenarios of the aggregated list incidents (from all participating organisations) to present to a panel of experts. The panel of experts could be experts from the participating organisations, as well as experts from the government, researchers or specialists in related organisations. The experts rank the scenarios and add possible new scenarios. The system generates a risk map that can be retrieved by managers and policy makers to use for policy planning and decision-making.

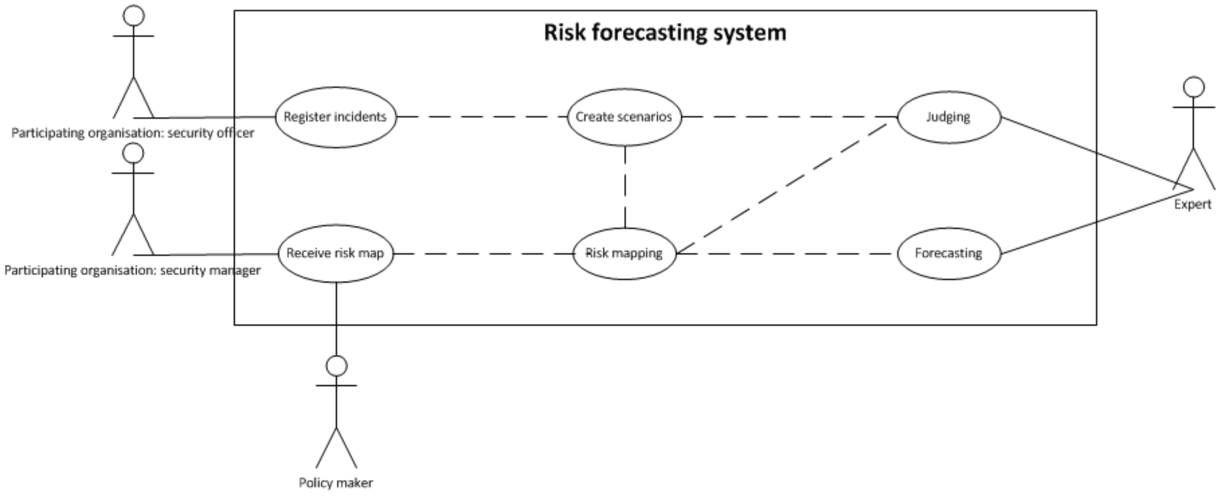


Figure 8-1 Risk forecasting system and its users

The system design will have to consider the following unsolved issues with the HI-risk method:

1. Time: the research made a snapshot of information security risks at the time of the research. This took several years to complete, while risks appear, change or disappear every moment. The design of the future expert systems should incorporate the continuous deletion or reduce the importance of past incidents after a certain period, and provide updates of new incidents.

2. Simultaneous occurrence of multiple sub-categories within one scenario could not be modelled with the basic supporting software in the simulation. A future system must build in this feature where multiple threats co-occur with multiple vulnerabilities, methods, events, and damage.

3. To prevent personal interpretations and errors during the incident registration, the registration process must be supported with clear instructions and a possibility for feedback from participants when a category is not clear. There is also a direct relationship with the forensic investigation process in the organisation. For the success of the HI-risk method, incidents should be carefully investigated and reported. The better the quality of the data during the input, the better the forecast will be.

For future academic studies of information security risks in general, it is suggested to focus on the gap in knowledge about environmental risk factors. Knowledge about security within disciplines such as building architecture, health and safety, social geography, or urban planning might be able to contribute significantly to environmental risk factor classifications, as might sociology, political science and legal studies.

Furthermore, a suggestion for future research is to include Library and Information Science (LIS) in information security research. Information Security Management Systems require organisations to create a classification of sensitive information with the aim to balance the level of access to data and the strength of security controls with the level of sensitivity of that information. However, humans conceptualise sensitivity in different ways. LIS research investigates tagging and categorizing as central issues in the organisation of information, and this work supports classifications. This field has particular relevance to the understanding of sensitivity classifications and security decision-making.

Finally, studies of human behaviour and norms and values may contribute to a better understanding of security behaviour and perception of risks. These studies have been mainly conducted in western cultures. ICT services outsourced to Asian and eastern European countries, for example, involve cultural differences and different interpretations of tasks and management style. Crossler et al. (2013) have recently suggested that future information security studies may need to include cross-cultural differences such as uncertainty avoidance, issues of collectivism versus individualism, and power distance relationships. Regional and country level cultural assessments could provide findings that may be helpful to understanding how people perceive information security in a certain region. The understanding and management of information security risks will become increasingly important in a networked, global information society.

9 Bibliography

Abbott, R. P., Chin, J. S., Donnelley, J. E., Konigsford, W. L., Takubo, S., & Webb, D. A. (1976). *Security analysis and enhancements of computer operating systems*. In T. A. Linden (Ed.). Washington: Institute for Computer Sciences and Technology.

Abbott, W., Blankley, N., Bryant, J., & Bullas, S. (2004). *Information in healthcare*. Swindon: BCS HIC.

Abdullah Al-Awadi, M. (2009). *A study of employees' attitudes towards organisational information security policies in the UK and Oman.* Ph.D. thesis, University of Glasgow, Glasgow.

Acquisiti, A. (2008). Identity management, privacy, and price discrimination. *IEEE Security & Privacy, 6*(2), 46-50.

Adler, N., & Docherty, P. (1998). Bringing business into sociotechnical theory and practice. *Human Relations, 51*(3), 319-345.

Amoroso, E. (1994). *Fundamentals of computer security technology.* Upper Saddle River, NJ: Prentice-Hall Inc.

Anderson, J. M. (2003). Why we need a new definition of information security. *Computers & Security, 22*(4), 308-313.

Anderson, J. P. (1972). *Computer Security Technology Planning Study*. Volume 2. Springfield: NTIS U.S. Department of Commerce.

Anderson, R. (2001, December). Why information security is hard - an economic perspective. Paper presented at the *Computer Security Applications Conference 2001*, New Orleans, Louisiana.

Anderson, R., & Moore, T. (2006). The economics of information security. *Science, 314*(5799), 610-613.

Anderson, R., & Moore, T. (2009). Information security: where computer science, economics and psychology meet. *Philosophical Transactions of the Royal Society, 367*(1898), 2717-2727.

Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: current state of research. *International Journal Internet and Enterprise management, 6*(4), 279-310.

Armitage, P., Berry, G., & Matthews, J. N. S. (2002). *Statistical methods in medical research* (4th ed.). Massachusetts: Blackwell Publishing Company.

Asaro, P. V., Herting, R. L., Roth, A. C., & Barnes, M. R. (1999, November*). Effective audit trails - A taxonomy for determination of information requirements.* Paper presented at the *Annual Symposium of the American Medical Informatics Association*, Washington, D.C.

Asley, J. (2010, 26 March). Non-medical staff 'have access to health records'. *BBC News online*. Retrieved 1 August 2013 from http://news.bbc.co.uk/2/hi/health/8587898.stm.

AS/NZS ISO (2009). *AS/NZS ISO 31000:2009. Risk management – Principles and guidelines.* Sidney, Australia.

Baker, S., Waterman, S., & Ivanov, G. (2010). *In the crossfire. Critical infrastructure in the age of cyber war*. London: McAfee.

Baker, W., Hutton, A., Hylender, C. D., Pamula, J., Porter, C., & Spitler, M. (2011). *Verizon Data Breach Investigations Report*, Verizon. Available at: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf [accessed 1 September 2013].

Baker, W., Hylender, C. D., & Valentine, J. A. (2008). *2008 Data breach investigations report*. Verizon Business Risk team. Available at: www.verizonenterprise.com/resources/security/databreachreport.pdf [accessed 2 May 2010].

Bansal, G., Zaheid, F.M. & Gefen, D. (2007). The impact of personal dispositions on privacy and trust in disclosing health information online. *Proceedings of Americas Conference on Information Systems (AMCIS 2007).* Keystone, CO. Paper 57.

Batchelor, R., Bobrowicz, A., Mackenzie, R., & Milne, A. (2012). Challenges of ethical and legal responsibilities when technologies' uses and users change: social networking sites, decision-making capacity and dementia. *Ethics and Information Technology, 14*(2), 99-108.

Bath, P. A. (2008). Health informatics: current issues and challenges. *Journal of Information Science, 34*(4), 501-518.

Bava, M., Cacciari, D., Sossa, E., Zotti, D. & Zangrando, R. (2009, July). Information Security Risk Assessment in Healthcare: the Experience of an Italian Paediatric Hospital. Paper presented at the *First International Conference on Computational Intelligence, Communication Systems and Networks*. Indore, India.

Baysari, M., Mcintosh, A.S. & Wilson J.R. (2008). Understanding the human factors contribution to railway accidents and incidents in Australia. *Accident Analysis and Prevention, 40*(5), 1750-1757.

Braman, S. (2011). Defining Information Policy. *The journal of information policy, 1*, 1-5. Available at http://jip.vmhost.psu.edu/ojs/index.php/jip/issue/view/3 [accessed 1 September 2013].

Beck, U. (1992). *Risk Society. Towards a new modernity.* London: Sage Publications Ltd.

Beck, U. (2002a). The cosmopolitan society and its enemies. *Theory Culture & Society, 19*(1-2), 17-44.

Beck, U. (2002b). The terrorist threat - World risk society revisited. *Theory Culture & Society, 19*(4), 39-55.

Beck, U. (2006). Living in the world risk society. *Economy and Society, 35*(3), 329-345.

Beck, U. (2007). *World at risk*. Cambridge: Polity Press.

Beech, M. (2007). Confidentiality in health care: conflicting legal and ethical issues. *Nursing standard, 21*(21), 42-46.

BERR. (2008). *Information Security Breaches Survey*. Technical report. Available at: http://www.bis.gov.uk/files/file45714.pdf [accessed 1 October 2010].

Bolle, S. R., Hasvold, P., & Henriksen, E. (2011). Video calls from lay bystanders to dispatch centers - risk assessment of information security. *BMC Health Services Research, 11*(244). Available at: http://www.biomedcentral.com/1472-6963/11/244 [accessed 1 October 2013].

Boritz, J. E. (2005). IS practitioners' views on core concepts of information integrity. *International Journal of Accounting Information Systems, 6*(4), 260-279.

Brann, M., & Mattson, M. (2004). Toward a typology of confidentiality breaches in health care communication: an ethic of care analysis of provider practices and patient perceptions. *Health Communication, 16*(2), 231-251.

Brann, M. (2007). Health care provider’s confidentiality practices and perceptions: expanding a typology of confidentiality breaches in health care communication. *Qualitative research reports in communication, 8*(1), 45-52.

Brinkerhoff, D. W., & Bossert, T. J. (2008). Health Governance: concepts, experience, and programming options *Policy Brief*: Health Systems 20/20 USAID.

Buchanan, W.J., Kwecka, Z., & Ekonomou, E. (2012). A Privacy Preserving Method Using Privacy Enhancing Techniques for Location Based Services. *Mobile Networks and Applications* (Special Issue on Mobility of Systems, Users, Data and Computing)1-10. [Online]. Available at: http://link.springer.com/article/10.1007%2Fs11036-012-0362-6 (accessed 1 October 2013)

Buchanan, W.J. (2011). *Introduction to security and network forensics.* London: CRC Press.

Buckley Owen, B., Cooke, L., & Matthews, G. (2012). Information policymaking in the United Kingdom: the role of the information professional. *Journal of Information Policy, 2*(March), 51-78. Available at: http://jip.vmhost.psu.edu/ojs/index.php/jip/article/view/82. [Accessed 1 October 2013].

Cabinet Office. (2012). *Open Data white paper: unleashing the potential*. London: TSO. Retrieved from: https://www.gov.uk/government/publications/open-data-white-paper-unleashing-the-potential (accessed 1 September 2013).

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security, 11*(3), 431-448.

Carthey, J., & Clarke, J. (2010). Implementing human factors in healthcare. *Patient safety first!* Retrieved from Patient safety first website: http://www.patientsafetyfirst.nhs.uk/ashx/Asset.ashx?path=/Intervention-support/Human Factors How-to Guide v1.2.pdf.

Casper, C. (2007). *Examining the feasibility of a data collection framework*. Retrieved from: http://www.enisa.europa.eu/publications/archive/examining-the-feasibility-of-a-data-collection-framework.

Castells, M. (1996). *The rise of the network society*. Oxford: Blackwell.

Castells, M. (1997). *The power of identity*. Malden, Mass; Oxford: Blackwell.

Castells, M. (1998). *End of millennium*. Malden, Mass; Oxford: Blackwell Publishers.

Castells, M. (2000). *The rise of the network society* (2nd ed.). Oxford: Blackwell.

Castells, M. (2011). *Communication power*. Claremount, W.A.: Ebooks Corporation.

Castells, M. (2012). *Networks of outrage and hope: social movements in the Internet Age*. Cambridge: Polity Press.

Chen, T. M., & Ubu-Nimeh, S. (2011). Lessons from Stuxnet. *IEEE Computer, 44*(4).

Chhanabhai, P., & Holt, A. (2007). Consumers are ready to accept the transition to online and electronic records if they can be assured of the security measures. *Medscape General Medicine, 9*(1), 8.

Cho, S. (2003). *Risk analysis and management for information security.* Ph.D. thesis, Royal Holloway, University of London, London.

Choucri, N. (2012). *Cyberpolitics in International Relations*. Cambridge, MA: MIT press.

Choucri, N., & Goldsmith, D. (2012). Lost in cyberspace: Harnessing the Internet, international relations, and global security. *Bulletin of the Atomic Scientists, 68*(2), 70-77.

Cleghorn, W. (2013). *The proposals for all-sector personal data breach notification in Europe*. Brussels, European Privacy Association. Available at: http://www.europeanprivacyassociation.eu/public/news/EPA%20Editorial%20-%20Data%20Breach%20Notif%20-%20Cleghorn%20May%202012%20(1).pdf (accessed 1 February 2014).

Clemen, R. T., & Winkler, R. L. (1997). *Combining probability distributions from experts in risk analysis.* Duke University. Durham, NC.

Coleman, J. (2004). Assessing information security risk in healthcare organizations of different scale. *Proceedings of the 18th International congress and Exhibition of CARS 2004: Computer Assisted Radiology and Surgery*. Chicago, USA, 1268, 125-130.

Coles-Kemp, L. (2008). *The anatomy of an information security management system.* Ph.D. thesis, King's College London, London.

Coles-Kemp, L. (2009). Information security management: An entangled research challenge. *Information Security Technical Report*, *14*(4), 181-185.

Collmann, J. (2001). HIPAA and the Military Health System: Organizing technological and organizational reform in large enterprises. *Proceedings of Medical Imaging 2001: PACS and Integrated Medical Information Systems: Design and Evaluation*, San Diego, USA, 4324, 126.

Collmann, J. (2005). Assessing information security risk in dual-use health information systems. *Proceedings of 19th International congress and Exhibition of CARS 2005: Computer Assisted Radiology and Surgery.* Berlin, Germany, 1281, 296-301.

Colwill, C. (2009). Human factors in information security: the insider threat - who can you trust these days? *Information Security Technical Report 14*(4), 186-196.

CompTIA. (2012). 9th Annual Information Security Trends study. Chicago: CompTIA inc. Retrieved from: http://www.comptia.org/research/security.aspx.

Conn, J. (2007, 12 August 2009). Paper records more secure. Retrieved from: http://www.modernhealthcare.com/article/20070502/FREE/70502003.

Cooke, R. M. (1991). *Experts in uncertainty: Opinion and subjective probability in science.* Oxford: Oxford University Press.

Cosby, K.S. (2003). A framework for classifying factors that contribute to error in the emergency department. *Annals of Emergency Medicine, 42*(6), 815-823.

Cozens, P. M., Saville, G., & Hillier, D. (2005). Crime prevention through environmental design (CPTED): a review and modern bibliography. *Property Management, 23*(5), 328-356.

Crinson, I. (2008). Assessing the 'insider-outsider threat' duality in the context of the development of public-private partnerships delivering 'choice' in healthcare services: A sociomaterial critique. *Information Security Technical Report, 13*(4), 202-206.

Crossler, R., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioural information security research. *Computers & Security 32*(February), 90-101.

CSI. (2011). *CSI Computer crime and security survey*. (15th annual ed.). New York.

Cullen, J. (1998). The needle and the damage done: research, action research, and the organizational and social construction of health in the "information society". *Human Relations, 51*(12), 1543-1564.

Custers, B., Calders, T., Schermer, B., & Zarsky, T. (Eds.), (2013). *Discrimination and privacy in the information society.* Available at: http://www.springer.com/engineering/computational+intelligence+and+complexity/book/978-3-642-30486-6, Heidelberg: Springer-Verlag [accessed 1 October 2013].

Dalkey, N. C. (1969). *The Delphi method: an experimental study of group opinions*. The RAND Corporation.

de Lusignan, S., Chan, T., Theadom, A., & Dhoul, N. (2007). The roles of policy and professionalism in the protection of processed clinical data: A literature review. *International Journal of Medical Informatics, 76*(4), 261-268.

Delbanco, T., Walker, J., Bell, S. K., Darer, J.D., Elmore, J.G., Farag, N., Feldman, H.J., Mejilla, R., Ngo, L., Ralson, J.D., Ross, S.E., Trivedi, N., Vodicka, E., & Leveille, S.G. (2012). Inviting Patients to Read Their Doctors' Notes: A Quasi-experimental Study and a Look Ahead. *Annals of Internal Medicine, 157*(7), 461-470.

Delbecq, A.L., van de Ven, A.H. & Gustafson, D.H. (1975). *Group techniques for program planning: a guide to nominal group and Delphi processes.* Glenview, IL, Scott, Foresman & Company.

Department for Business Innovation & Skills (2013). *2013 Information security breaches survey. Technical report*. Available from www.gov.uk/bis. [Accessed 20 October 2013].

Department of Health (2007*). Information security management: NHS Code of practice*. Retrieved 12 November 2012 from http://systems.hscic.gov.uk/infogov/codes/securitycode.pdf.

Department of Health (2010a). *Checklist for Reporting, Managing and Investigating Information Governance Serious Untoward Incidents*. Retrieved 1 October 2013 from http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/links/suichecklist.pdf.

Department of Health (2010b). Information Governance Toolkit - Glossary. Retrieved 5 February 2013, from https://http://www.igt.hscic.gov.uk/Glossary/Glossary.pdf.

Department of Health (2012). *The power of information: putting all of us in control of the health and care information we need*. Retrieved 1 October 2013 from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/213689/dh_134205.pdf.

Department of Health and Human Services (2012). *Breaches affecting 500 or more individuals.* Retrieved 16 September, from http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html.

Department of Health and Human Services (2013). *Health Information Privacy*. Retrieved 28 January 2013, from http://www.hhs.gov/ocr/privacy/index.html.

Dhillon, G., & Backhouse, J. (2000). Information system security management in the new millennium. *Communications of the ACM, 43*(7), 125-128.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal, 11*(2), 127-153.

Dimitropoulos, L. (2007). *Privacy and security solutions for interoperable health information exchange*: *nationwide summary analysis.* Research Triangle Park. Retrieved 1 October 2013 from https://www.rti.org/pubs/avas_execsumm.pdf.

Doherty, N. F., & Fulford, H. (2005). Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis. *Information Resources Management Journal, 18*(4), 21-39.

Donaldson, A., & Walker, P. (2004). Information governance - a view from the NHS. *International Journal of Medical Informatics, 73*(3), 281-284.

Dourish, P. & Anderson, K. (2006). Collective Information Practice: Exploring privacy and security as social and cultural phenomena. *Human-Computer Interaction, 21*(3), 319-342.

Duff, A.S. (2008). The normative crisis of the information society. *Cyberspychology: Journal of Phychosocial Research on Cyberspace*, *2*(1) [online]. Available at: http://cyberpsychology.eu/view.php?cisloclanku=2008051201 (accessed 2 July 2013).

Duff, A. S. (2012). *A normative theory of the information society.* London: Routledge.

Edge, K., Raines, R., Grimaila, M., Baldwin, R., Bennington, R., & Reuter, C. (2007). The use of attack and protections trees to analyse security for an online banking system. Paper presented at the *40th Annual Hawaii International Conference on System Sciences*, Hawaii.

Elevant, K. (2011). Climate information crowdsourcing - a bottom-up practice for sustainability and growth. *Proceedings of the IADIS international conference e-Society 2011*, Avila, Spain.

ENISA (2010). *Inventory of Risk Management / Risk Assessment Tools*. Retrieved 6 January 2010, from http://www.enisa.europa.eu.

ENISA (2013). *ENISA's work in the field of CERTs / CSIRTs*. Available at: http://www.enisa.europa.eu/activities/cert (accessed 1 October 2013).

ENISA (2013). *ENISA Threat Landscape. Responding to the evolving threat environment*. Available at: http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape/at_download/fullReport (accessed 1 February 2014).

Ericsson, G. N. (2010). Cyber Security and Power System Communication-Essential Parts of a Smart Grid Infrastructure. *IEEE Transactions on Power Delivery, 25*(3), 1501-1507.

Eriksson, J., & Giacomello, G. (2007). Closing the gap between international relations theory and studies of digital-age security. In J. Eriksson & G. Giacomello (Eds.), *International Relations and Security in the Digital Age*. New York: Routledge.

European Commission (2013). *Commission Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications.* Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32013R0611:EN:NOT (accessed 1February 2014).

Fan, L., Buchanan, W., Thuemmler, C., Lo, O., Khedim, A., Uthmani, O., Khedim, A., Uthmani, O., Lawson, A., & Bell, D. (2011). DACAR Platform for eHealth Services Cloud. Paper presented at the *IEEE 4th International Conference on Cloud Computing*. Washington, USA.

Farrell, A. E., Zerriffi, H., & Dowlatabadi, H. (2004). Energy infrastructure and security. *Annual Review of Environment and Resources, 29*(November), 421-469.

FBI. (2011). Financial crime report to the public fiscal year 2010-2011. Retrieved 1 September 2013, from http://www.fbi.gov/stats-services/publications/financial-crimes-report-2010-2011.

Fernando, J. I., & Dawson, L. L. (2009). The health information system security threat lifecycle: An informatics theory. *International Journal of Medical Informatics, 78*(12), 815-826.

Ferreira, A., Cruz-Correia, R., Antunes, L., Farinha, P., Oliveira-Palhares, E., Chadwick, D. W., & Costa-Pereira, A. (2006). How to break access control in a controlled manner. Paper presented at *the 19th IEEE International Symposium on Computer-Based Medical Systems*, Salt Lake City, USA.

Fitzgerald, T. (2012). *Information Security Governance Simplified: From the Boardroom to the Keyboard.* Boca Raton: CRC Press Inc.

Franqueira, V. N. L., van Cleeff, A., van Eck, P., & Wieringa, R. (2010). External Insider Threat: a Real Security Challenge in Enterprise Value Webs. Paper presented at the *Fifth International Conference on Availability, Reliability, and Security: Ares 2010*, Krakow, Poland.

Gady, F.-S., & Austin, G. (2010). *Russia, the United States, and cyber diplomacy. Opening the doors*. New York: EastWest Institute.

Gagnon, M. P., Shaw, N., Sicotte, C., Mathieu, L., Leduc, Y., Duplantie, J., Maclean, J. & Legare, F. (2009). Users' perspectives of barriers and facilitators to implementing EHR in Canada: A study protocol. *Implementation Science, 4*

(20). Available at: http://www.implementationscience.com/content/4/1/20 [accessed 1 October 2013].

Gerber, M., & von Solms, R. (2005). Management of risk in the information age. *Computers and Security, 24*(1), 16-30.

Ghaffarian, V. (2011). The new stream of socio-technical approach and main stream information systems research. *Proceedings of the World Conference on Infroamtion Technology,* Istanbul, Turkey 3, 1499-1511.

Goel, S., & Shawky, H. A. (2009). Estimating the market impact of security breach announcements on firm values. *Information & Management, 46*(7), 404-410.

Gold, S. (2010). Securing the National Health Service. *Computer Fraud & Security, 2010*(5), 11-14.

Gordon, T. J. (1994). The Delphi Method. *Futures Research Methodology*. Retrieved from http://test.scripts.psu.edu/students/d/j/djz5014/nc2if/04-Delphi.pdf.

Greene, K., Thomsen, D., & Michelucci, P. (2012). Massively collaborative problem solving: new security solutions and new security risks. *Security Informatics, 1*(12), 17.

Grunske, L., & Joyce, D. (2008). Quantitative risk-based security prediction for component-based systems with explicitly modelled attack profiles. *Journal of Systems and Software, 81*(8), 1327-1345

Guo, K. H., & Yuan, Y. (2012). The effects of multilevel sanctions on information security violations: A mediating model. *Information & Management*, *49*(6), 320-326.

Gürbüz, F., Özbakir, L., & Yapici, H. (2009). Classification rule discovery for the aviation incidents resulted in fatality. *Knowledge-Based Systems, 22*(8), 622-632.

Haislmaier, E. (2006). Health care information technology: getting the policy right (1131) *The Herigate Foundtiation, Research WebMemos*, 16 June 2006. Available at: http://www.heritage.org/research/reports/2006/06/health-care-information-technology-getting-the-policy-right [accessed 1 October 2013].

Hall, H. (2009). *Writing a literature review*. Available at: https://intranet.institute.napier.ac.uk/iidi/wiki/File:Phd_lit_review_training.pdf [accessed 1 October 2013].

Hasson, F., & Keeney, S. (2011). Enhancing rigour in the Delphi technique research. *Technological forecasting and social change, 78*(9), 1695-1704.

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The Law of Cyber-Attack. *California Law Review, 100*(4), 817-885.

Hawn, C. (2009). Take two aspirin and tweet me in the morning: how Twitter, Facebook, and other social media are reshaping health care. *Health Affairs, 28*(2), 361-368.

Hazelhoff Roelfzema, N. (2011, March). A comparative review of information security risk assessment methodologies for health care. *Proceedings of the IADIS International conference e-Society*, Avila, Spain, 141-149.

Healey, J. (2011). *Statistics for social research* (9th ed.). Belmont, USA: Wadsworth, Cengage learning.

Health and Social Care information centre (2013). *Information Governance FAQs*. Retrieved 15 July 2013, from http://systems.hscic.gov.uk/infogov/igfaqs.

Hedström, K., Dhillon, G. and Karlsson, F. (2010). Using Actor Network Theory to Understand Information Security Management. In Rannenberg, K., V., V. and Weber, C., (Eds). *25th IFIP TC-11 International Information Security Conference, SEC 2010*. Brisbane, Australia, Springer, 43-54.

Hedström, K., Kolkowska, E., Karlsson, F., & Allen, J. P. (2011). Value conflicts for information security management. *Journal of Strategic Information Systems, 20*(4), 373-384.

Heller, F. (1997). Sociotechnology and the environment. *Human Relations, 50*(5), 605-624.

Helms, R., Costanza, S. E., & Johnson, N. (2012). Crouching tiger or phantom dragon? Examining the discourse on global cyber-terror. *Security Journal, 25*(1), 57-75.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154-165.

Herold, R. (2011). *Managing an information security and privacy awareness and training program* (2nd ed.). Boca Raton: Taylor and Francis Group/CRC Press.

Hevner, A.R., Salvatore, M. T., Park, J. and Ram, S. (2004). Design Research in information systems research. *MIS Quarterly, 28*(1), 75-105.

Hillestad, R., Bigelow, J., Bower, A., Girosi, F., Meili, R., Scoville, R., & Taylor, R. (2005). Can electronic medical record systems transform health care? Potential health benefits, savings, and costs. *Health affairs, 24*(5), 1103-1117.

HIMSS Analytics. (2012). *2012 HIMSS Analytics 2012 report: Security of patient data*. Retrieved 1 October 2013 from http://www.krollcybersecurity.com/media/Kroll-HIMSS_2012_-_Security_of_Patient_Data_040912.pdf.

Hitchings, J. (1995). Deficiencies of the traditional approach to information security and the requirements for a new methodology. *Computers & Security, 14*(5), 377-383.

Hoffman, S., & Podgurski, A. (2007). In sickness, health, and cyberspace: protecting the security of electronic private health information. *Boston college law review, 48*(2), 331-386.

Hogarth, R. M. (1978). A note on aggregating opinions. *Organizational Behavior and Human Performance, 21*(1), 40-46.

Hogganvik, I. (2007). *A graphical approach to security risk analysis.* Ph.D. thesis, University of Oslo, Oslo.

Hogganvik, I., & Stølen, K. (2006). A Graphical Approach to Risk Identification, Motivated by Empirical Investigations. Paper presented at *the 9th international conference on Model Driven Engineering Languages and Systems,* Genova, Italy, 4199, 574-588.

Hollnagel, E. (1998). *Cognitive reliability and error analysis method.* Oxford, Elsevier Science Ltd.

Holvast, J. (2009) History of privacy. In Matyáš, V. et al. (Eds.). *The Future of Identity in the Information Society* (pp. 13-42). Brno, Czech Republic.

Howard, J. D. (1997). *An analysis of security incidents on the Internet 1989-1995.* Ph.D. thesis, Carnegie Mellon University, Pittsburgh.

Howard, J. D., & Longstaff, T. A. (1998). *A common language for computer security incidents*. Albuquerque and Livermore: Sandia National laboratories.

HRSA. (2011). *What are the privacy and security risks of electronic v. paper health records?* Retrieved 15 September, 2011, from http://www.hrsa.gov/healthit/toolbox/HealthITAdoptiontoolbox/PrivacyandSecurity/securityrisks.html

Hubbard, D. W. (2010). *How to measure anything: finding the value of "intangibles" in business* (2nd ed.). Hoboken, New Jersey: Wiley & Sons.

IGZ/CBP. (2008). *Informatiebeveiliging in ziekenhuizen voldoet niet aan de norm*. Den Haag: College Bescherming Persoonsgegevens/Inspectie voor de Gezondheidszorg. Retrieved March 2009 from http://www.cbpweb.nl/downloads_rapporten/rap_2008_informatiebeveiliging_ziekenhuizen.pdf.

Information Commissioner (2011, 28 November 2011). Monetary penalties served to councils for serious email errors.   Retrieved 16 September 2012, from http://www.ico.gov.uk/news/latest_news/2011/monetary-penalties-served-to-councils-for-serious-email-errors-28112011.aspx.

Information Commissioner's Office (2010). Security Breaches reported to the ICO, V.6 15/06/2010.   Retrieved 27 April, 2011, from http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/breach_notification_spreadsheet.pdf.

Information Commissioner's Office (2013). *Privacy impact assessment and risk management*. Retrieved 1 September 2013 from http://www.ico.org.uk/~/media/documents/library/Corporate/Research_and_reports/pia-and-risk-management-full-report-for-the-ico.pdf.

International Telecommunication Union (2003). *Access to Information is a Fundamental Right in Information Society.* Retrieved 1 September 2013, from http://www.itu.int/newsroom/press_releases/2003/08.html.

Internetworldstats (2013). *Internetworldstats*. Available at: www.Internetworldstats.com [accessed 13 August 2013].

ISACA (2009). *COBIT 5 for information security*. Rolling Meadows: ISACA.

ISO/IEC (2004). *ISO/IEC 13335-1:2004. Information technology — Security techniques — Management of information and communications technology security. Part 1: Concepts and models for information and communications technology security management.* Geneva: International organisation for standardisation.

ISO/IEC (2008). *Health informatics — Information security management in health using ISO/IEC 27002*. Geneva: International organisation for standardisation.

ISO/IEC (2009). *ISO-IEC 15408-1. Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model.* Geneva: International organisation for standardisation.

ISO/IEC (2009). *ISO-IEC 21827. Information technology – Security techniques – Systems Security Engineering – Capability Maturity Model ® (SSE-CMM®).* Geneva: International organisation for standardisation.

ISO/IEC (2009). *ISO/IEC 27000:2009(E) Information Technology - Security Techniques - Information Security Management Systems - Overview and vocabulary*. Geneva: International organisation for standardisation.

IT Governance Institute. (2006). *Information security governance: guidance for boards of directors and executive management*. (2nd ed.). Rolling Meadows, IL.

Jackland, D. (2009). *Information Communication and Technology Strategy 2009-2014,* Welsh Ambulance Service NHS Trust.

Jain, A. K., Ross, A., & Pankanti, S. (2006). Biometrics: A tool for information security. *IEEE Transactions on Information Forensics and Security, 1*(2), 125-143.

Johnson, E. M. (2009). Data haemorrhages in the health-care sector. Paper presented at the *13th International Conference on Financial Cryptography and Data Security*, Accra Beach, Barbados, 5628, 71-89.

Kahn, H., & Wiener, A. J. (1967). *The year 2000. A framework for speculation on the next thirty-three years.* New York: Macmillan.

Kaiser, J. (2006). Patient privacy: rule to protect records may doom long-term heart study. *Science, 311*(5767), 1547-1548.

Kalichman, S. C., Weinhardt, L., Benotsch, E., & Cherry, C. (2002). Closing the digital divide in HIV/AIDS care: development of a theory-based intervention to increase Internet access. *Aids Care-Psychological and Socio-Medical Aspects of Aids/Hiv, 14*(4), 523-537.

Kankanhalli, A., Teo, H.-H., Tan, B. C. Y., & Wei, K.-K. (2003). An Integrative Study of Information Systems Security Effectiveness. *International journal of information management, 23*(2), 139-154.

Kavaler, F., & Spiegel, A. D. (2003). *Risk Management in Health Care Institutions. A strategic approach* (second ed.): Jones and Bartlett Publishers.

Keeney, S., Hasson, F., & McKenna, H. (2006). Consulting the oracle: ten lessons from using the Delphi technique in nursing research. *Journal of Advanced Nursing, 53*(2), 205-212.

Keeney, S., Hasson, F., & McKenna, H. (2011). *The Delphi technique in nursing and health research*. Oxford: Wiley-Blackwell.

Keller, S., Powell, A., Horstmann, B., Predmore, C., & Crawford, M. (2005). Information Security threats and practices in small businesses. *Information systems management, 22*(2), 7-19.

Khan, B., Alghathbar, K. S., Nabi, S. I., & Khan, M. K. (2011). Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management*, *5*(26), p. 10862-10868.

Khansa, L., Cook, D. F., James, T., & Bruyaka, O. (2012). Impact of HIPAA provisions on the stock market value of healthcare institutions, and information security and other information technology firms. *Computers & Security, 31*(6), 750-770.

King, D. A. (2008). *Confidentiality for all*. Response in discussion forum on BMJ article. Retrieved 11 March 2013, from http://www.bmj.com/content/336/7649/888?tab=responses.

Kinkel, S., Armbruster, H., & Schirrmeister, E. (2006). Szenario-Delphi oder Delphi-Szenario? Erfahrungen aus zwei Vorausschaustudien mit der Kombination dieser Methoden. In J. Gausemeier (Ed.), *Vorausschau und Technologieplanung: 2. Symposium für Vorausschau und Technologieplanung* (pp. 109-137). Paderborn: Heinz-Nixdorf-Institut.

Kling, R. (1987). Defining the boundaries of computing. In: Boland, R.J. & Hirschheim, R.A. (Eds.). *Critical issues in information systems research*. Chichester, Wiley.

Kluge, E.H.W. (2008). Ethical aspects of future health care: globalisation of markets and differentiation of societies - ethical challenges. *Studies in Health Technology Informatics, 134*, 77-87. Retrieved 13 September 2013 from http://ebooks.iospress.nl/publication/11451.

Kluge, E.H.W. (2004). *Informed consent to the secondary use of EHRs: Informatic rights and their limitations.* Paper presented at the Medinfo 2004, San Francisco, USA.

Koppel, R., Metlay, J.P., Cohen, A., Abaluck, B., Localio, A.R., Kimmel, S.E. & Strom, B.L. (2005). Role of computerized physician order entry systems in facilitating medication errors. *Journal of American Medical Association, 293*(10), 1197–1203.

Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. *Information & Management, 41*(5), 597-607.

KPMG (2012). *Shifting viewpoints. Call for action*. KPMG Advisory N.V. Available at: http://www.kpmg.com/nl/en/issues-and-insights/articlespublications/pages/shifting-viewpoints.aspx [accessed 1 October 2013].

Kroll Fraud Solutions (2010). *2010 HIMSS Analytics report: security of patient data*, Kroll Fraud Solutions. Retrieved from http://www.krollcybersecurity.com/about-kroll/himss-security-patient-data-report.aspx [accessed 4 March 2011).

Krsul, I.V. (1998). *Software vulnerability analysis*. Ph.D. thesis. Purdue University, West Lafayette, Indiana.

Kuechler, W. & Vaishnavi, V. (2012). A framework for theory development in design science research: multiple perspectives. *Journal of the association for inofmation systems, 13*(6). Retrieved 1 September 2013 from http://aisel.aisnet.org/jais/vol13/iss6/3/.

Kushniruk, A. W., Bates, D. W., Bainbridge, M., Househ, M. S., & Borycki, E. M. (2013). National efforts to improve health information system safety in Canada, the United States of America and England. *International Journal of Medical Informatics, 82*(5), 149-160.

Kuusi, O. (1991). *Expertise in the Future Use of Generic Technologies. Epistemic and Methodological Considerations Concerning Delphi Studies.* Helsinki: HeSE Print.

Lackey, R. D. (1974). Penetration of computer systems, an overview. *Honeywell Computer Journal, 8* (2), 81-85.

Landeta, J. (2006). Current validity of the Delphi method in social sciences. *Technological Forecasting and Social Change, 73*(5), 467-482.

Latour, B. (2005). *Reassembling the social. An introduction to Actor-Network-Theory*. New York: Oxford University Press.

Leonardi, P. M. (2012). Materiality, Sociomateriality, and Socio-Technical Systems: What Do These Terms Mean? How Are They Different? Do We Need Them? In P. M. Leonardi, B. A. Nardi & J. Kallinikos (Eds.), *Materiality and organizing: social interaction in a technological world*. Oxford: Oxford University Press.

Leveille, S. G., Walker, J., Ralston, J. D., Ross, S. E., Elmore, J. G., & Delbanco, T. (2012). Evaluating the impact of patients' online access to doctors' visit notes: designing and executing the OpenNotes project. *BMC Medical Informatics and Decision Making, 12*(32). Available at: http://www.biomedcentral.com/content/pdf/1472-6947-12-32.pdf [accessed 1 October 2013].

Levy, G., Blumberg, N., Kreiss, Y., Ash, N., & Merin, O. (2010). Application of information technology within a field hospital deployment following the January 2010 Haiti earthquake disaster. *Journal of the American Medical Informatics Association, 17*(6), 626-630.

Libenson, E. (2007). The threat from within. Implementing secure access controls helps organizations protect sensitive patient information from insider threat. *Healthcare Informatics, 24*(7), 54.

Liginlal, D., Sim, I., & Khansa, L. (2009). How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *Computers & Security, 28*(3-4), 215-228.

Lim, S., Oh, T. H., Choi, Y. B., & Lakshman, T. (2010). *Security issues on wireless body area network for remote healthcare monitoring.* Paper presented at the *IEEE International conference on sensor networks, ubiquitous, and trustworthy computing*, Newport Beach, California.

Linstone, H. A., & Turoff, M. (1975). *The Delphi method: techniques and applications*. London: Addison-Wesley.

Lips, M., Taylor, J. A., & Bannister, F. (2005). Public administration in the information society: essays on risk and trust. *Information Polity, 10*(1), 1-9.

Lorence, D. P. (2003). The perils of data misreporting. *Communications of the ACM, 46*(11), 85-88.

Lough, D. L. (2001). *A taxonomy of computer attacks with applications to wireless networks.* Ph.D. thesis, Virginia Polytechnic Institute and State University Blacksburg, Virginia.

Lund, M. S., Solhaug, B., & Stølen, K. (2011). Model-driven risk analysis. The CORAS approach. Berlin Heidelberg: Springer-Verlag.

Lyon, D. (2007). *Surveillance studies: An overview.* Cambridge: Polity Press.

Lyon, D., & Wood, D. M. (2012). Security, Surveillance, and Sociological Analysis. *Canadian Review of Sociology/Revue canadienne de sociologie, 49*(4), 317-327.

Macdonald, G. (2005). *NHS Scotland information security policy,* NHS Scotland.

Magrabi, F., Aarts, J., Nohr, C., Baker, M., Harrison, S., Pelayo, S., Talmon, J., Sittig, S.J. & Coiera, E. (2013). A comparative review of patient safety initiatives for national health information technology. *International Journal of Medical Informatics, 82*(5), 139-148.

Magrabi, F., Ong, M. S., Runciman, W., & Coiera, E. (2011). Patient safety problems associated with healthcare information technology: an analysis of adverse events reported to the US Food and Drug Administration. Paper presented at the *AMIA Annual Symposium*, Washington, DC.

Mair, J. (2011). Who owns the information in the medical record? Copyright issues. *Health Information Management Journal, 40*(3), 31-37.

Malin, B. (2007). A computational model to protect patient data from location-based re-identification. *Artificial Intelligence in Medicine, 40*(3), 223-239.

Malin, B., & Airoldi, E. (2007). Confidentiality preserving audits of electronic medical record access. *Studies in Health Technology and Informatics, 129*(Pt 1), 320-324.

March S. T. and Smith G. F. (1995). Design and natural science research on information technology. *Decision Support Systems, 15*(4), 251-266.

McGowan, J. J., Cusack, C. M., & Bloomrosen, M. (2012). The future of health IT innovation and informatics: a report from AMIA's 2010 policy meeting. *Journal of the American Medical Informatics Association, 19*(3), 460-467.

Meingast, M., Roosta, T., & Sastry, S. (2006). Security and privacy issues with health care information technology. *Proceedings from the 28th IEEE EMBS annual international conference*, New York, 30 August–3 September 2006, pp. 5453-5458.

Miller, A.R. and Tucker, C.E. (2009). Privacy protection and technology diffusion: the case of electronic medical records. *Management Science, 55*(7), 1077–1093.

Mohammad, Y. M. (2010). *Information security strategy in telemedicine and e-health systems: a case study of England's shared electronic health record system.* Ph.D. thesis, Brunel University.

Moorhead, S. A., Hazlett, D. E., Harrison, L., Carroll, J. K., Irwin, A., & Hoving, C. (2013). A new dimension of health care: systematic review of the uses, benefits, and limitations of social media for health communication. *Journal of Medical Internet Research, 15*(4), e85.

Morse, E. A., Raval, V., & Wingender Jr., J. R. (2011). Market price effects of data security breaches. *Information Security Journal: A Global Perspective 20*(6), 263-273.

Moulton, R., & Coles, R. S. (2003). Applying information security governance. *Computers & Security, 22*(7), 580-584.

Mueller, M., Schmidt, A., & Kuerbis, B. (2013). Internet security and networked governance in international relations. *International Studies Review, 15*(1), 86-104.

Mutch, A. (2013). Sociomateriality — Taking the wrong turning? *Information and Organization, 23*(1), 28-40.

Myers, J., Frieden, T., Bherwani, K., & Henning, K. (2008). Ethics in public health research: privacy and public health at risk: public health confidentiality in the digital age. *American Journal for Public Health, 98*(5), 793-801.

National Patient Safety Agency (2008). *A risk matrix for risk managers*. London: NHS National Patient Safety Agency.

Ness, R. B. (2007). Influences of the HIPAA privacy rule on health research. *Journal of American Medical Association, 298*(18), 2164-2170.

Neter, E., & Brainin, E. (2012). eHealth Literacy: Extending the Digital Divide to the Realm of Health Information. *Journal of Medical Internet Research, 14*(1), e19. [online]. Available from: http://www.jmir.org/2012/1/e19/ [Accessed 1 October 2013].

Neumann, P. G. (1978). Computer security evaluation. Paper presented at the *AFIPS Conference Proceedings*, Arlington, USA, 47, 1078-1095. Available from: www.csrc.nist.gov/publicatoins/history [accessed March 2010).

NHS 24 (2013). *NHS 24 Risk management strategy 2013/2014*. Available from: http://www.nhs24.com/AboutUs/NHS24Board/AgendasAndPapers/2013/~/media/NHS24/Agendas%20and%20Papers/2013/Mar/20130328BoardItem73B.ashx [accessed 1 October 2013].

NHS (2009). NHS Information risk management. *Digital information policy*. Available from: http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/security/risk/inforiskmgtgpg.pdf. [Accessed 1 September 2011].

NHS (2012). *Does my project require review by a research ethics committee?* Available from: http://www.nres.nhs.uk/applications/approval-requirements/ethical-review-requirements/ [accessed 1 March 2013]

NHS (2013). *Will I be charged to access my health records?* Available from: http://www.nhs.uk/NHSEngland/thenhs/records/healthrecords/Pages/what_to_do.aspx [accessed 14 January 2013].

NHS Commissioning Board (2012). *Health and Safety policy*. Available from: http://www.england.nhs.uk/wp-content/uploads/2013/03/health-safe-pol.pdf.

NHS National Institute for Health research (2013). *Your health records save lives. What? How? Why?* Available from: http://www.nhs.uk/Conditions/Clinical-trials/Documents/Research1.pdf. [accessed 1 January 2014]

Niazkhani, Z., Pirnejad, H., van der Sijs, H., & Aarts, J. (2011). Evaluating the medication process in the context of CPOE use: the significance of working around the system. *International Journal Of Medical Informatics, 80*(7), 490-506.

Nielsen, D.S., Platz, O. & Runge, B. (1975). A cause-consequence chart of a redundant protection system. *IEEE Transactions on reliability R-24*(1), 8-13.

NIST (1996). *An introduction to computer security: the NIST handbook*. National Institute of Standards and Technology. Retrieved 1 April 2009 from http://csrc.nist.gov/publications/nistpubs/800-12/.

NIST (2002). *History of computer security*. Retrieved 1 August 2013, from http://csrc.nist.gov/publications/history/.

Nunamaker, J.F., Chen, M. & Purdin, T. (1991). System development in information system research. *Journal of Management Information Systems, 7*(3), 89-106.

Obama, B. (2011). Strategy to Combat Transnational Organized Crime: Letter from the President. *Strategy to combat transnational organized crime: Addressing Converging Threats to National Security.* Retrieved 1 September 2013, from http://www.whitehouse.gov/administration/eop/nsc/transnational-crime/letter

Offermann, P., Levina, O., Schönherr, M. and Bub, U. (2009). Outline of a design science research process. *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology (DESRIST '09)*. Malvern, PA. 7th-8th May. ACM Press, 1-11.

Orlikowski, W. J. (2010). The sociomateriality of organisational life: considering technology in management research. *Cambridge Journal of Economics, 34*(1), 125-141.

Orlikowski, W. J., & Scott, S. V. (2008). Sociomateriality: Challenging the Separation of Technology, Work and Organization. *The Academy of Management Annals, 2*(1), 433-474.

Orna, E. (2008). Information policies: yesterday, today, tomorrow. *Journal of information science, 34*(4), 547-565.

Padma, T., & Balasubramanie, P. (2009). Knowledge based decision support system to assist work-related risk analysis in musculoskeletal disorder. *Knowledge-Based Systems, 22*(1), 72-78.

Parker, D. B. (1998). *Fighting computer crime. A new framework for protecting information.* New York: Wiley Computer Publishing.

Patientprivacyrights (2013). *True stories*. Retrieved 1 September 2013, from http://patientprivacyrights.org/true-stories/

Peffers K., Tuunanen, T., Rothenberge, M. & Chatterjee, S. (2007). A Design Science Research methodology for information research. *Journal of Management Information Systems 24*(3), 45-78.

Peltier, T. R. (2005). *Information security risk analysis* (2nd ed.). Boca Raton, London: Auerbach Publications.

PerAda (2010, November 22-23). Workshop in security, trust and privacy. Rome, Foundations of adaptive networked societies of tiny artefacts. Available at: http://fronts.cti.gr/events/security-trust-perada.html (accessed 1 February 2014).

Ponemon (2011). *Second annual benchmark study on patient privacy & data security*. Ponemon Institute LLC. Available at: www.ponemon.org.

Porat, M. U. (1977). *The information economy: definition and measurement*. Washington: Office of Telecommunications (DOC).

Pulcini, J., Wilbur, J., Allan, J., Hanson, C., & Uphold, C. R. (2006). Determining criteria for excellence in nurse practitioner education: Use of the Delphi Technique. *Nursing Outlook*, *54*(2), 102-110.

Quigley, K., & Roy, J. (2012). Cyber-Security and risk management in an interoperable world: An examination of governmental action in North America. *Social Science Computer Review*, *30*(1), 83-94.

Ralston, J. D., Carrell, D., Reid, R., Anderson, M., Moran, M., & Hereford, J. (2007). Patient web services integrated with a shared medical record: Patient use and satisfaction. *Journal of the American Medical Informatics Association*, *14*(6), 798-806.

Ransbotham, S., & Mitra, S. (2009). Choice and Chance: A Conceptual Model of Paths to Information Security Compromise. *Information Systems Research, 20*(1), 121-139.

Rasmussen, J. (1997). Risk management in a dynamic society: a modelling problem. *Safety Science*, *27*(2/3), 183-213.

Reason, J. (1990). *Human error.* Cambridge, Cambridge University Press.

Reddy, K., Venter, H. S., Olivier, M., & Currie, I. (2008). Towards privacy taxonomy-based attack tree analysis for the protection of consumer information privacy. Proceedings of the *Sixth annual conference on privacy, security and trust*. New Brunswick Canada, 56-64.

Renaud, K., & Goucher, W. (2012). Health service employees and information security policies: an uneasy partnership? *Information management and computer security, 20*(4), 296-311.

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems, 21*(6), 11-25.

Rock, B., & Congress, E. (1999). The new confidentiality for the 21st century in a managed care environment. *Social Work, 44*(3), 253-262.

Rosenberg, M.A. (2001a). A decision theoretic method for assessing a change in the rate of nonacceptable inpatient claims. *Health Services and Outcomes Research Methodology, 2*(1), 19–36.

Rosenberg, M.A. (2001b). A statistical method for monitoring a change in the rate of nonacceptable inpatient claims. *North American Actuarial Journal, 5*(4), 74–83.

Rouse, W. B. (2008). Health care as a complex adaptive system: implications for design and management. *The Bridge, 38*(1), 17-25.

Rowe, G., & Wright, G. (2001). Expert opinions in forecasting: the role of the Delphi technique. In J. Armstrong (Ed.), *Principles of Forecasting* (pp. 125-144). Boston: Kluwer Academic.

Rowlands, I., Eisenschitz, T., & Bawden, D. (2002). Frame analysis as a tool for understanding information policy. *Journal of information science, 28*(1), 31-38.

RSA (2010). *Cybercrime and the healthcare industry*. RSA Security ltd. Retrieved 1 October 2013 from http://www.emc.com/collateral/white-papers/11030-cybhc-wp.pdf.

Ryan, J. J. C. H., Mazzuchi, T. A., Ryan, D. J., Lopez de la Cruz, J., & Cooke, R. (2010). Quantifying information security risks using expert judgment elicitation. *Computers & Operations Research 39*(4), 774-784.,

Samy, G. N., Ahmad, R., & Ismail, Z. (2009). Threats to Health Information Security. *Fifth International Conference on Information Assurance and Security*, Xi'an, China, vol. II, 540-543.

Sanfilippo, A., Gilbert, N., & Greaves, M. (2012). Technosocial predictive analytics for security informatics. *Security Informatics, 1*(8) [online]. Available at: http://www.security-informatics.com/content/1/1/8 (accessed 1 October 2013).

Sarbanes-Oxley Act 2002 (2002). *Sarbanes-Oxley Act of 2002* (116 stat. 745). Retrieved 1 October 2013 from http://www.gpo.gov/fdsys/pkg/PLAW-107publ204/pdf/PLAW-107publ204.pdf.

Schneier, B. (1999). *Attack Trees: Modeling Security Threats*. Retrieved 1 October 2013 from https://www.schneier.com/paper-attacktrees-ddj-ft.html.

Schneier, B. (2008). *Schneier on Security*. Indianapolis: Wiley Publishing.

Schneier, B. (2012). *Liars and outliers. Enabling the trust that society needs to thrive.* Indianapolis: John Wiley & Sons, Inc.

Schultz, E. E. (2002). A framework for understanding and predicting insider attacks. *Computers & Security, 21*(6), 526-531.

Scott, K. (2013). *NHS LCHS Trust. Network security policy*, Lincolnshire Community Health Services Trust Board.

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H.-J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education, 52*(1), 92-100.

Shorrock S.T. & Kirwan, B. (2002). Development and application of a human error identification tool for air traffic control. *Applied ergonomics, 33*(2002), 319-336.

Siponen, M.T. (2006). Information security standards focus on the existence of process, not its content. *Communications of the ACM, 49*(8), 97-100.

Siponen, M.T., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management, 46*(5), 267-270.

Siponen, M.T. (2005). Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods. *Information and Organization, 15*(4), 339-375.

Skulmoski, G.J., Hartman, F. T., & Krahn, J. (2007). The Delphi Method for graduate research. *Journal of information technology education. 6*, 1-21 [online]. Available at http://www.informingscience.us/icarus/journals/jiteresearch/publications.

Smit, M., McAllister, M., & Slonim, J. (2005). Building Public Trust for Electronic Health Records. Retrieved 12 August 2009, from Siteseer http://www.lib.unb.ca/Texts/PST/2005/pdf/smit.pdf

Smith, E., & Eloff, J. H. P. (1999). Security in health-care information systems. Current trends. *International Journal of Medical Informatics, 54*(1), 39-54.

Smith, E., & Eloff, J. H. P. (2002). A prototype for assessing information technology risks in health care. *Computers & Security, 21*(3), 266-284.

Smith, M.W. (2010). *IT security risk assessment in health care regulation amongst Scottish General Practises.* M.Sc. thesis, Edinburgh Napier University, Edinburgh.

Smith, M.W., Buchanan, W.J., Thuemmler, C., Bell, D., & Hazelhoff Roelfzema, N. (2010). *Analysis of information governance and patient data protection within primary health care.* Available at:

http://www.iidi.napier.ac.uk/c/publications/publicationid/13365537 (accessed 15 October 2013).

South Western Ambulance Service (2013). *Risk Management Strategy*. Retrieved 1 October 2013 from http://www.swast.nhs.uk/RiskMgmtStrategy.pdf.

Stahl, B. C. (2012). Morality, Ethics, and Reflection: A Categorization of Normative IS Research. *Journal of the Association for Information Systems, 13*(8), 636-656.

Stahl, B. C., Doherty, N. F., & Shaw, M. (2012). Information security policies in the UK healthcare sector: a critical evaluation. *Information Systems Journal, 22*(1), 77-94.

Standards Australia & Standards New Zealand (2004). AS/NZS 4360;2004 Risk management, (3rd ed.). Sidney, Australia, Wellington, New Zealand.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security, 24*(2), 124-133.

Stathiakis, N., Chronaki, C., Skipenes, E., Henriksen, E., Charalambus, E., Sykianakis, A., Vrouchos, G., Antonakis, N., Tsiknakis, M. & Orphanoudakis, S. (2003). Risk Assessment of a cardiology eHealth servcie in HYGEIAnet. *Computers in Cardiology*, Thessaloniki, Greece, 201-204.

Steinbart, P., Raschke, R., Gal, G., & Dilla, W. (2012). The relationship between internal audit and information security: An exploratory investigation. *International Journal of Accounting Information Systems, 13*(3), 228-243.

Sterbenz, J. P. G., Hutchison, D., Cetinkaya, E. K., Jabbar, A., Rohrer, J. P., Scholler, M., & Smith, P. (2010). Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks, 54*(8), 1245-1265.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22*(4), 441-469.

Sumsion, T. (1998). The Delphi Technique: an adaptive research tool. *British Journal of Occupational Therapy, 61*(4), 153-156.

Sunyaev, A., Atherton, M., Mauro, C., Leimeister, J., & Krcmar, H. (2009). Characteristics of IS Security approaches with respect to healthcare. Paper presented at the *Americas Conference on Information Systems (AMCIS),* San Francisco, California.

Takeda, H., Veerkamp, P., Tomiyama, T. & Yoshikawa, H. (1990). Modelling design processes. *AI Magazine, 11*(4), 37-48.

Terry, N., & Francis, L. P. (2007). Ensuring the Privacy and Confidentiality of Electronic Health Records *University of Illinois Law Review, 2007*(October), 681-735 [online]. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=886904 (accessed 1 October 2013).

Thompson, E. D., & Kaarst-Brown, M.L. (2005). Sensitive information: A review and research agenda. *Journal of the American Society for Information Science and Technology, 56*(3), 245-257.

Trottier, D. (2012). Policing social media. *Canadian review of sociology, 49*(4), 411-425.

United Nations (2013). *Comprehensive study on cybercrime*. Vienna: United Nations office on drugs and crime. Retrieved 1 October 2013 from www.unodc.org.

United States General Accounting Office (1998). *Executive Guide: Information Security Management. Learning From Leading Organizations*. Retrieved from http://www.gao.gov/assets/80/76396.pdf.

Uthmani, O., Buchanan, W., Lawson, A., Thuemmler, C., Fan, L., Scott, R., Lavery, A. & Mooney, C. (2010). Novel Information Sharing Syntax for Data Sharing Between Police and Community Partners, Using Role-Based Security. *Proceedings of the 9th European Conference on Information Warfare and Security*, Thessaloniki, Greece, 394-402. Retrieved 1 October 2013 from http://www.iidi.napier.ac.uk/c/publications/publicationid/13366481.

Vaishnavi, V.K. and Kuechler, W. (2004, Last updated November 11, 2012). *Design Science Research in Information Systems*. Available at: http://www.desrist.org/design-research-in-information-systems/ (accessed 1 October 2013).

Vaishnavi, V.K., & Kuechler, W. (2008). *Design science research methods and patterns. Innovating information and communication technology*. Boca Raton: Auerbach Publications. Taylor & Francis Group.

Vaishnavi, V.K., & Kuechler, W. (2012). Design research in information systems. Retrieved 1 September 2013 from http://desrist.org/design-research-in-information-systems/ - ovrDesRsch.

van Aken, J.E. (2004). Management research based on the paradigm of the design sciences: The quest for field-tested and grounded technological Rules. *Journal of Management Studies, 41*(2), pp. 219-246.

van Aken, J.E., Georges, A. & L. Romme (2012). A design science approach to evidence-based management. In Rosseau, D. M. (Ed.), *Handbook of evidence-based management.* New York: Oxford University Press, in press. Retrieved 1 October 2013 from http://www.cebma.org.

van der Linden, H., Kalra, D., Hasman, A., & Talmon, J. (2009). Inter-organizational future proof EHR systems A review of the security and privacy related issues. *International Journal of Medical Informatics, 78*(3), 141-160.

van Deursen, N., Buchanan, W. J., & Duff, A. (2013). Monitoring information security risks within healthcare. *Computers & Security, 37*(September), 31-45.

van Dijk, J. A. G. M. (2012). *The network society.* (3rd ed.). London: Thousand Oaks CA.

Verizon. (2012). *2012 Data breach investigations report*. Retrieved from http://www.verizonbusiness.com/about/events/2012dbir/

von Solms, B. (2006). Information security - The Fourth Wave. *Computers & Security, 25*(3), 165-168.

von Solms, R., & van Niekerk, J. (2013). From Information Security to Cyber Security. *Computers & Security, 38*(October), 97-102.

von Solms, R., & von Solms, B. (2004). From policies to culture. *Computers & Security, 23*(4), 275-279.

von Solms, S. H. (2010). The 5 Waves of Information Security - From Kristian Beckman to the Present. In Rannenberg, K., Varadharajan V. & Weber, C. (Eds.) *Security and Privacy - Silver Linings in the Cloud. Processings of the 25th IFIP TC11 International Information Security Conference.* Brisbane, Australia, *330*, 1-8.

von Solms, S. H., & von Solms, R. (2008). *Information security governance*. New York: Springer Science.

Vorster, A., & Labuschagne, L. (2005). A framework for comparing different information security risk analysis methodologies. *Proceedings of the 2005 annual research conference of the South African institue of computer scientists and informatin technologists on IT research in developing countries.* White River, South Africa, 95-103.

Walker, J., Leveille, S. G., Ngo, L., Vodicka, E., Darer, J. D., Dhanireddy, S., Elmore, J.G., Feldman, H.J., Lichtenfield, M.J., Oster, N., Ralston, D., Ross, S.E., & Delbanco, T. (2011). Inviting patients to read their doctors' notes: patients and doctors look ahead: patient and physician surveys. *Annals of Internal Medicine, 155*(12), 811-857.

Ward, R., Stevens, C., Brentnall, P., & Briddon, J. (2008). The attitudes of health care staff to information technology: a comprehensive review of the research literature. *Health information and libraries journal, 25*(2), 81-97.

Ware, W. (1970). Security controls for computer systems (U): Report of defense science board task force on computer security *Rand report R609-1*. Santa Monica, CA: The Rand Corporation.

Warren, M. J., Furnell, S. M., & Sanders, P. W. (1997). ODESSA: a new approach to healthcare risk analysis. *Proceedings of the IFIP TC11 13 international conference on Information Security (SEC '97) on Information security in research and business*, Copenhagen, Denmark.

Whitman, M.E., & Mattord, H.J. (2010). *Management of Information Security.* Boston: Course Technology Cengage Learning.

Whitman, M. E., & Mattord, H. J. (2012). *Principles of information security* (4th ed.). Boston: Course Technology Cengage Learning.

Whittaker, B. (1999). What went wrong? Unsuccessful information technology projects. *Information Management & Computer Security, 7*(1), 23.

Williams, P. A. H. (2008). In a 'trusting' environment, everyone is responsible for information security. *Information Security Technical Report, 13*(4), 207-215.

Williams, P. L., & Webb, C. (1994). Clinical supervision skills. A Delphi and critical incident technique study. *Medical Teacher, 16*(2-3), 139-157.

Willison, D. J., Schwartz, L., Abelson, J., Charles, C., Swinton, M., Northrup, D., & Thabane, L. (2007). Alternatives to project-specific consent for access to personal information for health research: What is the opinion of the Canadian public? *Journal of the American Medical Informatics Association, 14*(6), 706-712.

Winter, R. (2008). Design science research in Europe. *European Journal of Information Systems 17*(Special issue on Design science Research), 470-475.

Woody, C. (2006). *Applying OCTAVE: Practitioners report.* Technical Note, CMU/ EI-2006-TN-010. Available at: http://www.sei.cmu.edu/reports/06tn010.pdf

World Economic Forum (2012). *Global risks 2012.* Available at: http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2012.pdf (accessed 1 February 2014).

World Health Organization (2008). *Global assessment of national health sector emergency preparedness and response*. Retrieved 1 October 2013 from http://www.who.int/hac/publications/en/.

World Law Group (2013). *Global guide to data breach notifications, 2013.* Available at: http://www.cms-dsb.com/Hubbard.FileSystem/files/Publication/c5076485-320d-4479-b198-e01f5e37bbb1/Presentation/PublicationAttachment/1e1adb07-4748-4342-a863-77e0de97d04a/WLG%20Global%20Guide%20to%20Data%20Breach%20Notifications%202013_a.pdf (accessed 1 February 2014).

Woudenberg, F. (1991). An evaluation of Delphi. *Technological forecasting and social change, 40*(40), 131-150.

Wyatt, J. C. (2012). The new NHS information strategy. *British Medical Journal* [online] 344. Available at: http://www.bmj.com/content/344/bmj.e3807 (accessed 1 August 2013).

Yin, R. K. (2009). *Case Study Research. Design and Methods.* (4th ed.). Los Angeles: Sage.

Appendix A: List of FOI requests

The following NHS organisations were part of the survey described in the thesis section 6.2: Data collection for the incident database.

Name	Reply in
County Durham	07/10/2010
Ashton Leigh And Wigan	01/10/2010
Barking & Dagenham	20/10/2010
Barnet	05/10/2010
Barnsley	
Bath And North East Somerset	13/10/2010
Bedfordshire	22/10/2010
Berkshire East	20/09/2010
Berkshire West	08/10/2010
Birmingham East And North	15/10/2010
Blackburn With Darwen	28/10/2010
Blackpool	
Bolton	18/10/2010
Bournemouth And Poole	14/10/2010
Bradford & Airedale	18/10/2010
Brent	
Brighton And Hove City	24/09/2010
Bristol	12/10/2010
Bromley	11/10/2010
Buckinghamshire	14/10/2010
Bury	
Calderdale	15/10/2010
Cambridgeshire	18/10/2010
Camden	03/02/2011
Central And Eastern Cheshire	
Central Lancs	19/10/2010
City And Hackney	16/11/2011
Cornwall & Isles Of Scilly	18/10/2010
Croydon	11/10/2010
Cumbria	14/10/2010
Darlington	04/11/2010
Derby City	18/10/2010
Derbyshire County	18/10/2010
Devon	30/09/2010
Doncaster	15/10/2010
Dorset	
Dudley	
Ealing	19/10/2010
East & North Hertfordshire	13/01/2011
East Lancs	18/10/2010
East Riding Of Yorkshire	18/10/2010
East Sussex Downs & Weald	
Enfield	18/10/2010

Gateshead	
Gloucestershire	
Great Yarmouth And Waveney	11/02/2011
Halton & St Helens	15/10/2010
Hammersmith & Fulham	23/09/2010
Hampshire	
Haringey	12/10/2010
Harrow	
Hartlepool	18/10/2010
Hastings & Rother	
Havering	15/10/2010
Heart Of Birmingham	22/10/2010
Hertfordshire	19/10/2010
Heywood Middleton & Rochdale	15/10/2010
Hillingdon	21/10/2010
Hounslow	15/10/2010
Hull	
Islington	14/10/2010
Kensington And Chelsea	10/11/2010
Kingston	21/10/2010
Kirklees	23/09/2010
Knowsley	23/09/2010
Lambeth	25/01/2010
Leeds	18/10/2010
Leicester City	14/10/2010
Leicestershire County & Rutland	
Lewisham	
Lincolnshire	
Liverpool	
Luton	
Manchester	
Mid Essex	01/10/2010
Middlesbrough	18/10/2010
Milton Keynes	20/10/2010
Newcastle Upon Tyne	28/09/2011
Newham	19/10/2010
Bexley	19/10/2010
Eastern & Coastal Kent	23/11/2010
Greenwich	12/10/2010
Isle Of Wight	
Medway	13/10/2010
Nottinghamshire County	20/10/2010
West Kent	22/10/2010
Norfolk	25/10/2010
North East Essex	21/10/2010
North East Lincolnshire Care Trust Plus	
North Lancs	19/10/2010
North Somerset	13/10/2010
North Staffordshire	

North Tyneside	28/09/2011
North Yorkshire And York	26/10/2010
Northamptonshire	17/12/2010
Northumberland	28/09/2011
Nottingham City	27/10/2010
Oldham	21/10/2010
Oxfordshire	15/10/2010
Peterborough	25/10/2010
Plymouth	20/10/2010
Portsmouth City	22/10/2010
Redbridge	13/10/2010
Redcar And Cleveland	18/10/2010
Richmond & Twickenham	27/10/2010
Rotherham	14/10/2010
Salford	07/01/2011
Sandwell	22/12/2010
Sefton	19/10/2010
Sheffield	05/10/2010
Shropshire County	21/10/2010
Solihull	23/10/2010
Somerset	28/09/2010
South Birmingham	25/10/2010
South East Essex	21/12/2010
South Gloucestershire	02/01/2011
South Staffordshire	22/03/2011
South Tyneside	04/01/2011
South West Essex	22/12/2010
Southampton City	06/01/2011
Southwark	
Stockport	
Stockton On Tees	18/10/2010
Stoke-On-Trent	06/01/2011
Suffolk	05/01/2011
Sunderland	
Surrey	
Sutton & Merton	30/12/2010
Swindon	04/01/2011
Tameside And Glossop	14/12/2010
Telford & Wrekin	22/12/2010
Torbay	10/01/2011
Tower Hamlets	12/01/2010
Trafford	20/12/2010
Wakefield District	15/12/2010
Walsall Teaching	11/01/2011
Waltham Forest	13/01/2011
Wandsworth	
Warrington	29/12/2010
Warwickshire	18/01/2010
West Essex	21/12/2010

West Hertfordshire	13/01/2011
West Sussex	17/12/2010
Western Cheshire	05/01/2011
Westminster	30/12/2010
Wiltshire	
Wirral	12/01/2010
Wolverhampton City	10/01/2010
Worcestershire	06/01/2011
Ayrshire & Arran	
Borders	yes
Dumfries & Galloway	yes
Fife	yes
Forth Valley	yes
Grampian	yes
Greater Glasgow & Clyde	yes
Highland	yes
Lothian	yes
Lanarkshire	yes
Orkney	
Shetland	
Tayside	yes
Western Isles	yes

Appendix B: Scenarios retrieved from NHS incidents

threat	frequency	percentage	**location**	frequency	percentage	**method**	frequency	percentage	**weakness**	frequency	percentage	**event**	frequency	percentage	**Damage** (number of affected records)	frequency	percentage	Total %
building	3	0.00	on the premises	3	1.00	unknown	1	0.333	other building vulnerabilities	1	1.00	observe personal data	1	1	0-9	1	1	0.00
						water	1	0.333	other building vulnerabilities	1	1.00	damage personal data	1	1	0-9	1	1	0.00
						other	1	0.333	other building vulnerabilities	1	1.00	expose to loss	1	1	0-9	1	1	0.00
business partner	46	0.02	on the premises	4	0.09	human error	2	0.5	email not protected	1	0.50	possible disclosure of data	1	1	0-9	1	1	0.00
									lack of training	1	0.50	disclosure of information	1	1	0-9	1	1	0.00
						script or program	1	0.25	computer vulnerability	1	1.00	contamination	1	1	0-9	1	1	0.00
						unauthorised access	1	0.25	unattended asset/paper	1	1.00	observe personal data	1	1	0-9	1	1	0.00
			other	42	0.91	human error	41	0.976	email not protected	11	0.27	possible disclosure of data	9	0.82	0-9	8	0.89	0.00
															10-99	1	0.11	0.00
												disclosure of information	2	0.18	0-9	2	1.00	0.00
									transportation	3	0.07	expose to loss	1	0.33	0-9	1	1.00	0.00
												possible disclosure of data	2	0.67	0-9	2	1.00	0.00
									paper in post or internal mail	20	0.49	possible disclosure of data	19	0.95	0-9	19	1.00	0.01
												expose to loss	1	0.05	0-9	1	1.00	0.00

threat	frequency	percentage	**location**	frequency	percentage	**method**	frequency	percentage	**weakness**	frequency	percentage	**event**	frequency	percentage	**Damage** (number of affected records)	frequency	percentage	Total %
									user entry errors	4	0.10	possible disclosure of data	4	1.00	0-9	4	1.00	0.00
									lack of training	2	0.05	data on stick exposed to loss	1	0.50	0-9	1	1.00	0.00
												patient filmed without permission	1	0.50	0-9	1	1.00	0.00
									procedure not followed	1	0.02	possible disclosure of data	1	1.00	0-9	1	1.00	0.00
						fraud	1	0.024	insufficient supervision	1	1.00	record not available when needed	1	1.00	0-9	1	1.00	0.00
hardware	4	0.00	other	1	0.25	it-enabled process	1	1	design	1	1.00	disclosure of information	1	1.00	0-9	1	1.00	0.00
			on the premises	3	0.75	system error	3	1	other	2	0.67	delay process	1	0.50	0-9	1	1.00	0.00
												loss of data/asset	1	0.50	0-9	1	1.00	0.00
								1	system error	1	0.33	record not available when needed	1	1.00	0-9	1	1.00	0.00
internal employee	1569	0.74	on the premises	1127	0.72	unauthorised accessing	252	0.224	privileges	139	0.55	disclosure of information	134	0.96	0-9	127	0.95	0.06
															10-99	5	0.04	0.00
															100-999	2	0.01	0.00
												removal of information	2	0.01	0-9	1	0.50	0.00
															10-99	1	0.50	0.00

threat	frequency	percentage	**location**	frequency	percentage	**method**	frequency	percentage	**weakness**	frequency	percentage	**event**	frequency	percentage	**Damage** (number of affected records)	frequency	percentage	Total %
												modify information	1	0.01	0-9	1	1.00	0.00
												other	1	0.01	0-9	1	1.00	0.00
												acquire copyright material	1	0.01	0-9	1	1.00	0.00
									password/access token sharing	113	0.45	disclosure of information	113	1.00	0-9	89	0.79	0.04
															10-99	18	0.16	0.01
															100-999	4	0.04	0.00
															>1000	2	0.02	0.00
						human error	793	0.70	unattended asset/paper	235	0.30	records damaged	1	0.00	0-9	1	1.00	0.00
												disclosure of information	15	0.06	0-9	12	0.80	0.01
															10-99	2	0.13	0.00
															100-999	1	0.07	0.00
												expose to loss	2	0.01	10-99	2	1.00	0.00
												loss of data/asset	217	0.92	0-9	194	0.89	0.09
															10-99	11	0.05	0.01
															100-999	5	0.02	0.00
															1000-9999	7	0.03	0.00

threat	frequency	percentage	**location**	frequency	percentage	**method**	frequency	percentage	**weakness**	frequency	percentage	**event**	frequency	percentage	**Damage** (number of affected records)	frequency	percentage	Total %
									email entry errors	221	0.28	disclosure of information	221	1.00	0-9	208	0.94	0.10
															10-99	7	0.03	0.00
															100-999	4	0.02	0.00
															1000-9999	2	0.01	0.00
									email not protected	17	0.02	disclosure of information	17	1	0-9	17	1	0.01
									paper in post or internal mail	52	0.07	disclosure of information	52	1	0-9	52	1	0.02
									procedure not followed	128	0.16	disclosure of information	94	0.73	0-9	94	1	0.04
												expose to loss	34	0.27	0-9	34	1	0.02
									fax entry errors	39	0.05	disclosure of information	39	1.00	0-9	39	1	0.02
									informal conversation	1	0.00	disclosure of information	1	1.00	0-9	1	1	0.00
									telephone conversation	4	0.01	disclosure of information	4	1.00	0-9	4	1	0.00
									lack of training	37	0.05	disclosure of information	34	0.92	0-9	34	1	0.02
												delay process	1	0.03	0-9	1	1	0.00
												removal of information	1	0.03	0-9	1	1	0.00

threat	frequency	percentage	**location**	frequency	percentage	**method**	frequency	percentage	**weakness**	frequency	percentage	**event**	frequency	percentage	**Damage** (number of affected records)	frequency	percentage	Total %
												contaminated equipment	1	0.03	0-9	1	1	0.00
									user entry errors	44	0.06	misrepresent	14	0.32	0-9	14	1	0.01
												misplace of record	12	0.27	0-9	12	1	0.01
										44	0.06	disclosure of information	17	0.39	0-9	17	1	0.01
										44	0.06	loss of data/asset	1	0.02	0-9	1	1.00	0.00
									unknown	15	0.02	disclosure of information	13	0.87	0-9	5	0.38	0.00
															10-99	8	0.62	0.00
												unknown	1	0.07	0-9	1	1.00	0.00
												misrepresent	1	0.07	0-9	1	1.00	0.00
						employee manipulation and malfeasance	1	0.00	guards	1	1.00	take control of asset	1	1.00	0-9	1	1.00	0.00
						manual process	26	0.02	unattended asset/paper	1	0.04	disclosure of information	1	1.00	0-9	1	1.00	0.00
									organisational changes	1	0.04	disclosure of information	1	1.00	0-9	1	1.00	0.00
									improper disposal	24	0.92	disclosure of information	24	1.00	0-9	21	0.88	0.01
															10-99	3	0.13	0.00

threat	frequency	percentage	**location**	frequency	percentage	**method**	frequency	percentage	**weakness**	frequency	percentage	**event**	frequency	percentage	**Damage** (number of affected records)	frequency	percentage	Total %
						unknown	7	0.01	unknown	7	1.00	disclosure of information	7	1.00	0-9	4	0.57	0.00
															10-99	2	0.29	0.00
															100-999	1	0.14	0.00
						theft	1	0.00	unattended asset/paper	1	1.00	acquire data/asset	1	1.00	0-9	1	1.00	0.00
						it-enabled process	46	0.04	configuration	37	0.80	disclosure of information	34	0.92	0-9	30	0.88	0.01
															10-99	2	0.06	0.00
															100-999	1	0.03	0.00
															>1000	1	0.03	0.00
												contamination	1	0.03	>10.000	1	1.00	0.00
												network, other	1	0.03	0-9	1	1	0.00
												delay process	1	0.03	10-99	1	1	0.00
									organisational changes	1	0.02	delay process	1	1	0-9	1	1	0.00
									unknown	1	0.02	unknown	1	1	0-9	1	1	0.00
									changes	7	0.15	disclosure of information	1	0.14	100-999	1	1	0.00
												removal of information	5	0.71	0-9	4	0.8	0.00
															10-99	1	0.2	0.00
												record not available	1	0.14	0-9	1	1	0.00

threat	frequency	percentage	**location**	frequency	percentage	**method**	frequency	percentage	**weakness**	frequency	percentage	**event**	frequency	percentage	**Damage** (number of affected records)	frequency	percentage	Total %
												when needed						
						unauthorised access	1	0.00	doors	1	1.00	use of secure area	1	1.00	0-9	1	1	0.00
			staff home	11	0.01	it-enabled process	1	0.09	remote working environment	1	1.00	disclosure of information	1	1.00	0-9	1	1	0.00
						human error	8	0.73	fax entry errors	1	0.13	disclosure of information	1	1.00	0-9	1	1	0.00
									unattended asset/paper	6	0.75	loss of data/asset	5	0.83	0-9	5	1	0.00
												expose to loss	1	0.17	0-9	1	1	0.00
									paper in post or internal mail	1	0.13	disclosure of information	1	1.00	0-9	1	1	0.00
						manual process	1	0.09	privileges	1	1.00	use data for personal gain	1	1.00	0-9	1	1	0.00
						unauthorised accessing	1	0.09	privileges	1	1.00	disclosure of information	1	1.00	0-9	1	1	0.00
			patient home	14	0.01	human error	14	1.00	fax entry errors	1	0.07	disclosure of information	1	1.00	0-9	1	1	0.00
									paper in post or internal mail	4	0.29	disclosure of information	4	1.00	0-9	4	1	0.00
									procedure not followed	1	0.07	record not available when needed	1	1.00	0-9	1	1	0.00
									unattended asset/paper	5	0.36	loss of data/asset	5	1.00	0-9	5	1	0.00
									unknown	1	0.07	disclosure of information	1	1.00	0-9	1	1	0.00

threat	frequency	percentage	**location**	frequency	percentage	**method**	frequency	percentage	**weakness**	frequency	percentage	**event**	frequency	percentage	**Damage** (number of affected records)	frequency	percentage	Total %
									user entry errors	2	0.14	misrepresent	1	0.50	0-9	1	1	0.00
												disclosure of information	1	0.50	0-9	1	1	0.00
			unknown	175	0.11	unauthorised accessing	8	0.05	privileges	7	0.88	disclosure of information	7	1.00	0-9	6	0.86	0.00
									privileges	7	0.88	disclosure of information	7	1.00	10-99	1	0.14	0.00
									password/access token sharing	1	0.13	disclosure of information	1	1.00	0-9	1	1	0.00
						human error	165	0.94	procedure not followed	1	0.01	disclosure of information	1	1.00	0-9	1	1	0.00
									unattended asset/paper	128	0.78	disclosure of information	1	0.01	0-9	1	1	0.00
												loss of data/asset	127	0.99	0-9	124	0.98	0.06
															10-99	3	0.02	0.00
									fax entry errors	6	0.04	disclosure of information	6	1.00	0-9	4	0.67	0.00
															10-99	2	0.33	0.00
									email entry errors	30	0.18	disclosure of information	30	1.00	0-9	30	1	0.01
						manual process	2	0.01	improper disposal	2	1.00	disclosure of information	2	1.00	0-9	2	1	0.00
			other	242	0.15	it-enabled process	1	0.00	configuration	1	1.00	disclosure of information	1	1.00	0-9	1	1	0.00

threat	frequency	percentage	**location**	frequency	percentage	**method**	frequency	percentage	**weakness**	frequency	percentage	**event**	frequency	percentage	**Damage** (number of affected records)	frequency	percentage	Total %
						human error	233	0.96	unattended asset/paper	138	0.59	loss of data/asset	138	1.00	0-9	119	0.86	0.06
															10-99	14	0.10	0.01
															100-999	3	0.02	0.00
															>1000	1	0.01	0.00
															>10.000	1	0.01	0.00
									telephone conversation	1	0.00	disclosure of information	1	1.00	0-9	1	1.00	0.00
									paper in post or internal mail	31	0.13	disclosure of information	31	1.00	0-9	31	1	0.01
									procedure not followed	26	0.11	disclosure of information	26	1	0-9	26	1	0.01
									fax entry errors	17	0.07	disclosure of information	17	1	0-9	17	1	0.01
									email not protected	1	0.00	disclosure of information	1	1	0-9	1	1	0.00
									email entry errors	14	0.06	disclosure of information	14	1	0-9	12	0.86	0.01
															10-99	2	0.14	0.00
									user entry errors	5	0.02	disclosure of information	2	0.4	0-9	2	1.00	0.00
												misrepresent	3	0.6	0-9	3	1.00	0.00
						manual process	3	0.01	improper disposal	3	1.00	disclosure of	3	1	0-9	3	1.00	0.00

threat	frequency	percentage	**location**	frequency	percentage	**method**	frequency	percentage	**weakness**	frequency	percentage	**event**	frequency	percentage	**Damage** (number of affected records)	frequency	percentage	Total %
												information						
						unknown	3	0.01	unknown	3	1.00	disclosure of information	3	1	0-9	3	1.00	0.00
						physical damage	1	0.00	paper in post or internal mail	1	1.00	disclosure of information	1	1	0-9	1	1.00	0.00
						unauthorised accessing	1	0.00	password/access token sharing	1	1.00	disclosure of information	1	1	0-9	1	1.00	0.00
patient	13	0.01	on the premises	10	0.77	physical attack	2	0.20	other	2	1.00	disclosure of information	2	1	0-9	2	1.00	0.00
						eavesdropping	2	0.20	other	2	1.00	disclosure of information	2	1	0-9	2	1.00	0.00
						employee manipulation and malfeasance	1	0.10	other	1	1.00	disclosure of information	1	1	0-9	1	1.00	0.00
						manual process	1	0.10	procedure not followed	1	1.00	disclosure of information	1	1	0-9	1	1.00	0.00
						theft	1	0.10	unattended asset/paper	1	1.00	disclosure of information	1	1	0-9	1	1.00	0.00
						fraud	1	0.10	procedure not followed	1	1.00	misrepresentation of identity	1	1	0-9	1	1.00	0.00
						human error	1	0.10	unattended asset/paper	1	1.00	disclosure of information	1	1	0-9	1	1.00	0.00
						other	1	0.10	other	1	1.00	disclosure of information	1	1	0-9	1	1.00	0.00
			patient	3	0.23	eavesdropping	1	0.33	other	1	1.00	disclosure of	1	1	0-9	1	1.00	0.00

threat	frequency	percentage	**location**	frequency	percentage	**method**	frequency	percentage	**weakness**	frequency	percentage	**event**	frequency	percentage	**Damage** (number of affected records)	frequency	percentage	Total %
			home									information						
						manual process	1	0.33	other	1	1.00	copy information	1	1	0-9	1	1.00	0.00
						physical attack	1	0.33	other	1	1.00	disclosure of information	1	1	0-9	1	1.00	0.00
software	96	0.05	on the premises	90	0.94	script or program	11	0.12	configuration	11	1.00	contamination	11	1	0-9	10	0.91	0.00
						script or program	11	0.12	configuration	11	1.00	contamination	11	1	>1000	1	0.09	0.00
						system error	79	0.88	other	79	1.00	other	62	0.78	0-9	62	1.00	0.03
												record not available when needed	8	0.10	0-9	8	1	0.00
												destroy data	4	0.05	0-9	4	1	0.00
												delay process	2	0.03	0-9	2	1	0.00
												reorder data	2	0.03	0-9	2	1	0.00
												disclosure of information	1	0.01	0-9	1	1	0.00
			other	3	0.03	system error	3	1	other	3	1.00	disclosure of information	1	0.33	0-9	1	1	0.00
												other	2	0.67	0-9	1	0.5	0.00
															10-99	1	0.5	0.00
			staff home	3	0.03	system error	3	1	other	3	1.00	other	3	1.00	0-9	3	1	0.00

threat	frequency	percentage	**location**	frequency	percentage	**method**	frequency	percentage	**weakness**	frequency	percentage	**event**	frequency	percentage	**Damage** (number of affected records)	frequency	percentage	Total %
unknown	373	0.18	on the premises	155.000	0.42	human error	8	0.05	unknown	5	0.63	unknown	5	1	0-9	5	1	0.00
									unattended asset/paper	3	0.38	loss of data/asset	3	1	0-9	3	1	0.00
						script or program	1	0.01	website	1	1.00	contamination	1	1	10-99	1	1	0.00
						theft	145	0.94	unattended asset/paper	145	1.00	disclosure of information	145	1	0-9	130	0.90	0.06
															10-99	13	0.09	0.01
															100-999	1	0.01	0.00
															>10.000	1	0.01	0.00
						unknown	1	0.01	unknown	1	1.00	disclosure of information	1	1	0-9	1	1.00	0.00
			other	65	0.17	theft	63	0.97	unattended asset/paper	63	1.00	disclosure of information	63	1	0-9	58	0.92	0.03
															10-99	4	0.06	0.00
															100-999	1	0.02	0.00
						human error	2	0.03	procedure not followed	1	0.50	misrepresent	1	1	0-9	1	1.00	0.00
									unknown	1	0.50	loss of data/asset	1	1	0-9	1	1.00	0.00
			unknown	134	0.36	theft	56	0.42	unattended asset/paper	56	1.00	disclosure of information	56	1	0-9	56	1.00	0.03
						human error	1	0.01	unattended asset/paper	1	1.00	loss of data/asset	1	1	0-9	1	1.00	0.00
						unknown	77	0.57	unknown	77	1.00	disclosure of	77	1	0-9	71	0.92	0.03

threat	frequency	percentage	**location**	frequency	percentage	**method**	frequency	percentage	**weakness**	frequency	percentage	**event**	frequency	percentage	**Damage** (number of affected records)	frequency	percentage	Total %
												information						
															10-99	5	0.06	0.00
															>1000	1	0.01	0.00
			staff home	19	0.05	theft	19	1.00	unattended asset/paper	19	1.00	disclosure of information	19	1	10-99	2	0.11	0.00
															0-9	17	0.89	0.01
family member	1	0.00	on the premises	1	1.00	manual process	1	1.00	procedure not followed	1	1.00	disclosure of information	1	1	0-9	1	1	0.00
external human	3	0.00	on the premises	2	0.67	unauthorised access	1	0.50	privileges	1	1.00	misrepresent	1	1	0-9	1	1	0.00
						employee manipulation and malfeasance	1	0.50	telephone conversation	1	1.00	disclosure of information	1	1	0-9	1	1	0.00
			other	1	0.33	physical damage	1	1.00	paper in post or internal mail	1	1.00	disclosure of information	1	1	0-9	1	1	0.00

Appendix C: Delphi study questionnaires

Round 1

Which area(s) of expertise applies best to you?*
Expertise level
Information security ___
Healthcare/medical ___
Caldicott guardian/data protection ___
Risk management ___
IT Security ___
Information governance ___
Other ___

Scenarios based on incident registers

An analysis of 2108 information security incidents registered over 5 years in healthcare organisations in the UK delivered a top 5 of the most frequent incident scenarios and one scenario that affected the highest number of patient records.

These 6 scenarios are now presented to you. Please state your opinion about the expected frequency of these scenarios.

In your opinion, how frequent will this scenario occur?*
[ ] Very rarely: it will happen in less than 5 per 1,000 incidents.
[ ] Rarely: 5 to 10 times per 1,000 incidents
[ ] Sometimes: 10 to 50 times per 1,000 incidents
[ ] Frequently: 50 to 100 times per 1,000 incidents
[ ] Very frequently: more than 100 times per 1,000 incidents

Please try to estimate more specific how many out of 1,000 incidents will fit this scenario.
Please add your motivation or comments here:

Scenario 1. Email to wrong recipient.

100 out of 1,000 incidents (10% of past incidents)
involve an internal employee located on the premises who sends an email to the wrong addressee and consequently discloses the personal details of a few patients (less than 10 patients).

Scenario 2. Unattended asset goes missing.

90 out of 1,000 of the incidents (9% of past incidents)
involve an internal employee located on the premises leaving an asset unattended and consequently the asset goes missing. The asset contained personal information of a few patients (less than 10).

Scenario 3. Wrong privileges set.

60 out of 1,000 incidents (6% of past incidents)
involved an internal employee on the premises who unintentionally was given the wrong privileges or authorisations, causing disclosure of personal patient information to unauthorised persons.

Scenario 4. Password or access token sharing.

50 out of 1,000 incidents (5% of past incidents)
involve an internal employee sharing his password or access token leading to disclosure of patient information to unauthorised persons.

Scenario 5. Procedure not followed.

40 out of 1,000 incidents (4% of past incidents)
involve an internal employee located on the premises who does not follow the formal procedures leading to disclosure of patient information.

Scenario 6. More than 10,000 patient records affected.

1.5 out of 1,000 incidents (0.15% of past incidents)
involved the loss of a portable backup medium, affecting more than 10,000 patient records.

Create your scenario.
Please now create 2 information security incident scenarios in healthcare organisations for the near future. The scenarios should include only the human factors involved with information security risks.

The first scenario should be the one that you consider the most likely to happen. What is the risk scenario that healthcare organisations should be aware of? What kind of incident scenario do you think happens the most frequent?

The second scenario should be the one that you expect to affect the largest number of patient records. What will be a risk scenario that potentially has the most damaging effect?

In your opinion, what could be the most likely information security incident scenario in healthcare in the near future?

An initiator (human threat agent) such as:*
[ ] Medical staff
[ ] Financial administration staff
[ ] Other internal staff
[ ] Trainee
[ ] Personal assistant/secretary/admin support
[ ] Ex-employee

[ ] Employee in partner organisation or related healthcare provider
[ ] Employee in third party supplier or subcontractor
[ ] Patient
[ ] Family or carer/representative of patient
[ ] External group or activists
[ ] Other:
[ ] Unknown
Wanting (motive):*
[ ] No motive, unintentional action
[ ] Other
[ ] Justice
[ ] Satisfaction
[ ] Resignation
[ ] Knowledge
[ ] Financial gain
[ ] Emotional gain
[ ] Political gain
[ ] Covering up errors
[ ] Convenience
[ ] Thrill
[ ] Status
[ ] Challenge
[ ] Unknown
At the following location:*
[ ] On the premises of the organisation
[ ] At the patient's home
[ ] At the staff member's home
[ ] Public transport
[ ] On the premises of other healthcare provider or related organisation
[ ] In a public place (bar, restaurant, social club,.....)
[ ] Unknown
[ ] Other
Using the following method:*
[ ] Making a mistake
[ ] Stealing
[ ] Copying
[ ] Unauthorised accessing
[ ] Damaging/breaking
[ ] Manipulating
[ ] Abusing ICT facilities
[ ] Inserting a script/program
[ ] Physical attack
[ ] Overhearing/eavesdropping
[ ] Unknown
[ ] Other
And abusing the vulnerability or weakness:*
[ ] Unattended asset or record
[ ] Email recipient entry errors
[ ] Lack of internal control in procedure
[ ] Insufficient supervision
[ ] Lack of skills/training
[ ] Data entry errors
[ ] Procedure not followed

[ ] Informal conversation in public area
[ ] Telephone conversation in public area
[ ] Flaws in settings in authorisations/privileges
[ ] Sharing of password or access token
[ ] Paper record in internal post
[ ] Paper record in external post
[ ] Organisational changes, new procedures or routines
[ ] Transportation of storage medium
[ ] Security flaw in storage of data
[ ] Lack of security in email application
[ ] Fax to wrong recipient
[ ] Fax received in unsecured physical environment
[ ] Printer in unsecured environment
[ ] Hasty working
[ ] Unsecured remote working environment
[ ] Computer/network vulnerabilities
[ ] Physical security vulnerabilities
[ ] Unknown
[ ] Other
Leading to the event:*
[ ] Confidentiality breach: disclose personal data
[ ] Confidentiality breach: read/observe/hear personal data
[ ] Confidentiality breach: copy personal data
[ ] Confidentiality breach: acquire personal data
[ ] Confidentiality breach: locate personal data
[ ] Confidentiality breach: other
[ ] Availability breach: data lost or gone missing
[ ] Availability breach: destroy personal data
[ ] Availability breach: damage personal data or facilities
[ ] Availability breach: delay the process
[ ] Availability breach: other
[ ] Availability breach: data, notes or reports not available when needed
[ ] Integrity breach: insert false data, notes or reports
[ ] Integrity breach: modify notes, data or reports
[ ] Integrity breach: remove parts of data, notes or reports
[ ] Integrity breach: other
[ ] Unknown
[ ] Other
At the cost of:*
[ ] Repair costs
[ ] Mailing expenses
[ ] Replacement costs
[ ] Fines or penalties
[ ] Legal costs
[ ] Consultancy costs
[ ] Research or investigation costs
[ ] Call centre costs
[ ] Unknown
[ ] Other
Indirectly causing:*
[ ] Embarrassment to the organisation or medical staff
[ ] Affecting reputation of organisation or medical staff
[ ] Patients choosing for other healthcare providers

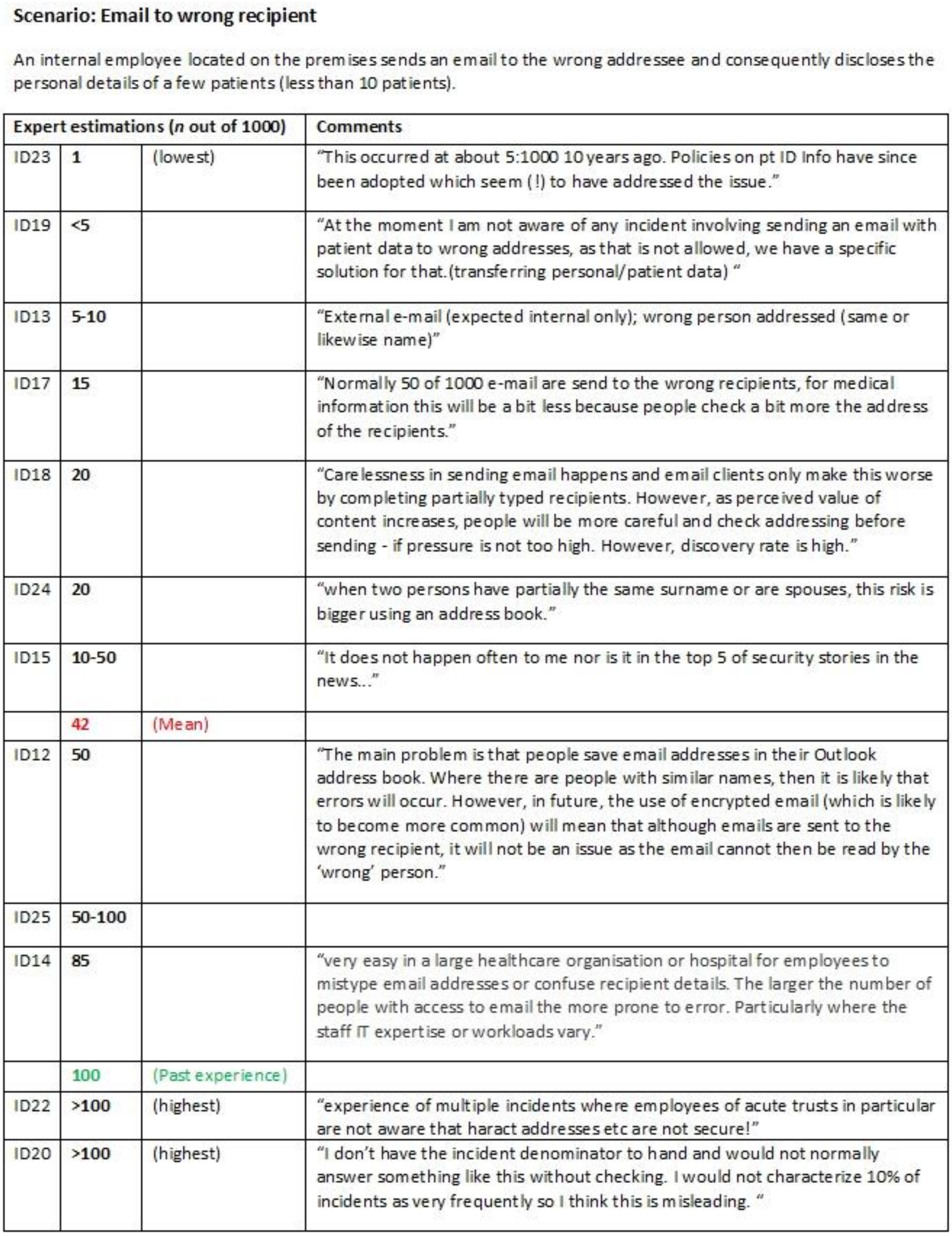
[ ] Loss of health or life of patient
[ ] Other
[ ] Discrimination
[ ] Quality of care affected
[ ] Compliance to regulation affected
[ ] Unknown
And affecting the following number of patient records:*
[ ] 0 - 9
[ ] 10 - 99
[ ] 100 - 999
[ ] 1,000 - 9,999
[ ] More than 10,000

Please add your motivation or comments here:

Delphi study questionnaire Round 2

For each scenario please answer these questions:

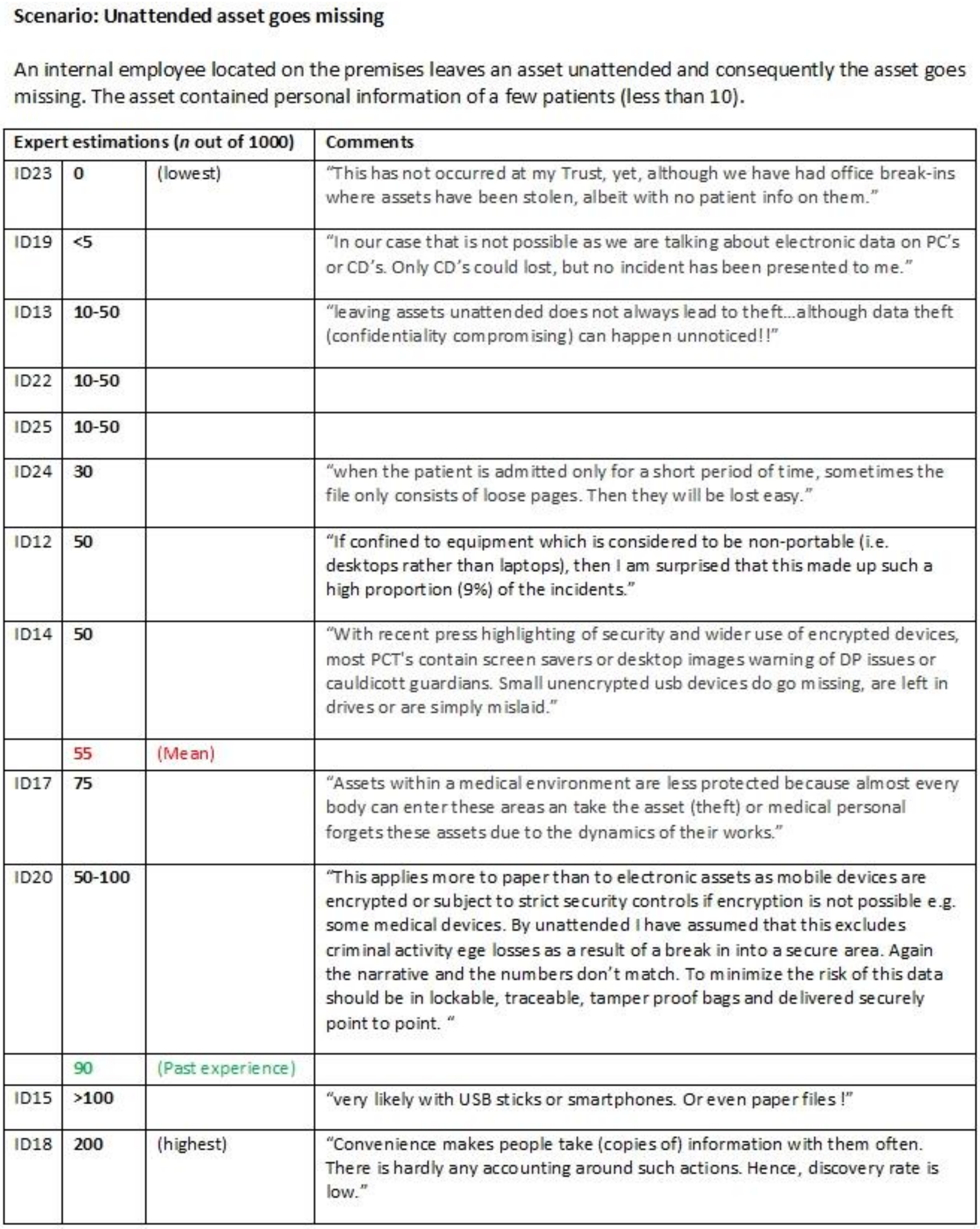
1) Please try to estimate (again) more specific how many out of 1,000 incidents will fit this scenario.
2) Please add your motivation or comments here:



Scenario: Email to wrong recipient

An internal employee located on the premises sends an email to the wrong addressee and consequently discloses the personal details of a few patients (less than 10 patients).

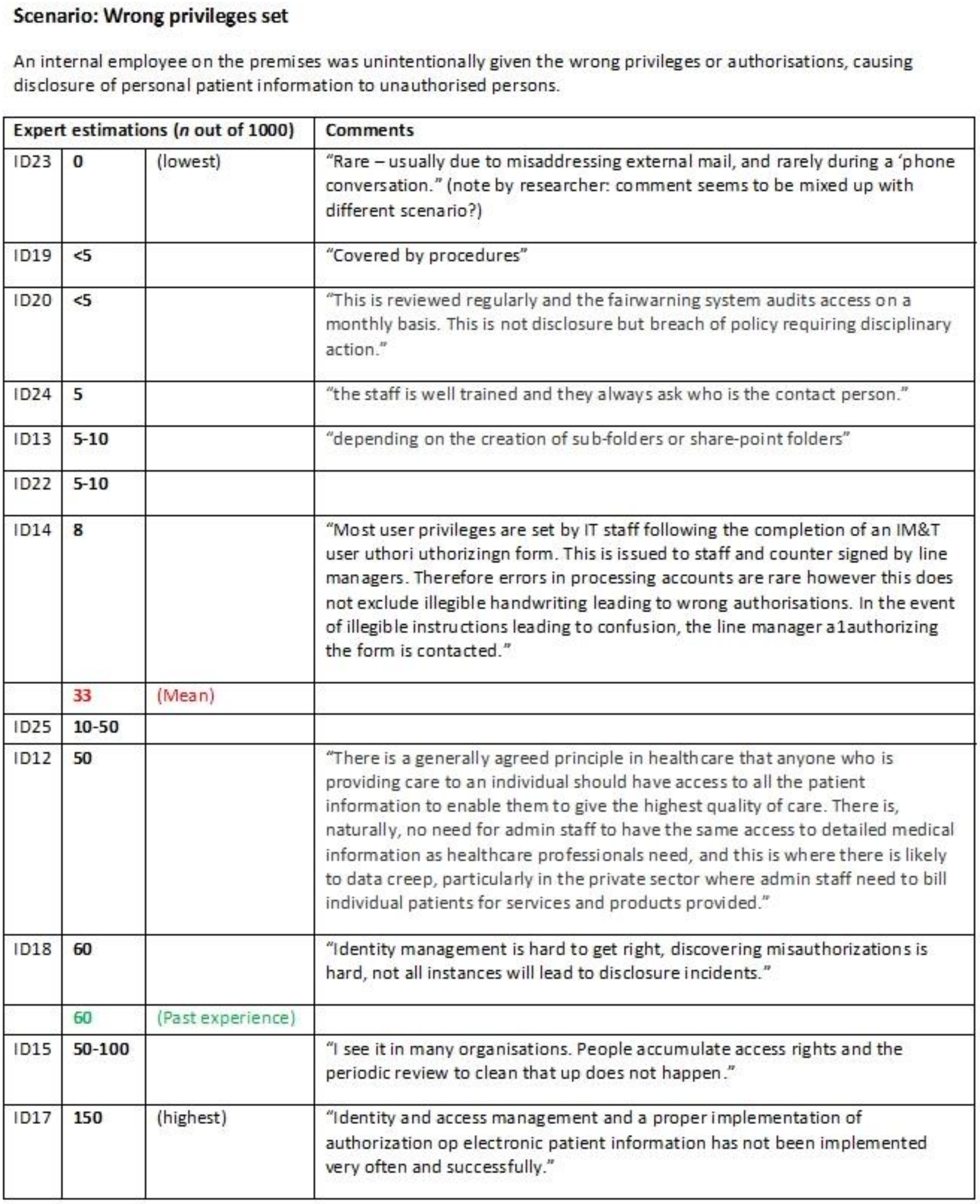
Expert estimations (*n* out of 1000)			Comments
ID23	**1**	(lowest)	"This occurred at about 5:1000 10 years ago. Policies on pt ID Info have since been adopted which seem (!) to have addressed the issue."
ID19	**<5**		"At the moment I am not aware of any incident involving sending an email with patient data to wrong addresses, as that is not allowed, we have a specific solution for that.(transferring personal/patient data) "
ID13	**5-10**		"External e-mail (expected internal only); wrong person addressed (same or likewise name)"
ID17	**15**		"Normally 50 of 1000 e-mail are send to the wrong recipients, for medical information this will be a bit less because people check a bit more the address of the recipients."
ID18	**20**		"Carelessness in sending email happens and email clients only make this worse by completing partially typed recipients. However, as perceived value of content increases, people will be more careful and check addressing before sending - if pressure is not too high. However, discovery rate is high."
ID24	**20**		"when two persons have partially the same surname or are spouses, this risk is bigger using an address book."
ID15	**10-50**		"It does not happen often to me nor is it in the top 5 of security stories in the news..."
	42	(Mean)	
ID12	**50**		"The main problem is that people save email addresses in their Outlook address book. Where there are people with similar names, then it is likely that errors will occur. However, in future, the use of encrypted email (which is likely to become more common) will mean that although emails are sent to the wrong recipient, it will not be an issue as the email cannot then be read by the 'wrong' person."
ID25	**50-100**		
ID14	**85**		"very easy in a large healthcare organisation or hospital for employees to mistype email addresses or confuse recipient details. The larger the number of people with access to email the more prone to error. Particularly where the staff IT expertise or workloads vary."
	100	(Past experience)	
ID22	**>100**	(highest)	"experience of multiple incidents where employees of acute trusts in particular are not aware that haract addresses etc are not secure!"
ID20	**>100**	(highest)	"I don't have the incident denominator to hand and would not normally answer something like this without checking. I would not characterize 10% of incidents as very frequently so I think this is misleading. "



Scenario: Unattended asset goes missing

An internal employee located on the premises leaves an asset unattended and consequently the asset goes missing. The asset contained personal information of a few patients (less than 10).

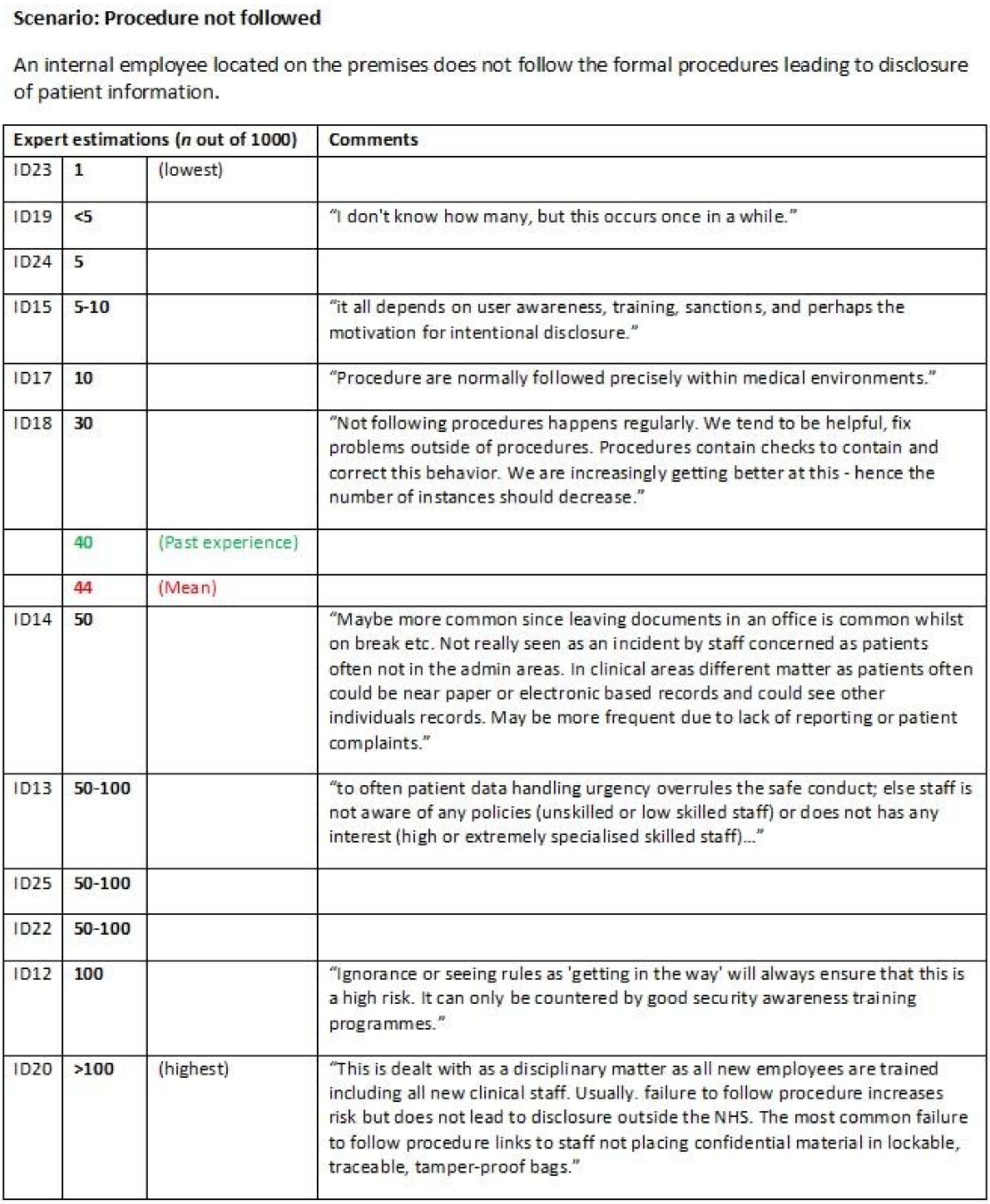
Expert estimations (*n* out of 1000)			Comments
ID23	**0**	(lowest)	"This has not occurred at my Trust, yet, although we have had office break-ins where assets have been stolen, albeit with no patient info on them."
ID19	**<5**		"In our case that is not possible as we are talking about electronic data on PC's or CD's. Only CD's could lost, but no incident has been presented to me."
ID13	**10-50**		"leaving assets unattended does not always lead to theft...although data theft (confidentiality compromising) can happen unnoticed!!"
ID22	**10-50**		
ID25	**10-50**		
ID24	**30**		"when the patient is admitted only for a short period of time, sometimes the file only consists of loose pages. Then they will be lost easy."
ID12	**50**		"If confined to equipment which is considered to be non-portable (i.e. desktops rather than laptops), then I am surprised that this made up such a high proportion (9%) of the incidents."
ID14	**50**		"With recent press highlighting of security and wider use of encrypted devices, most PCT's contain screen savers or desktop images warning of DP issues or cauldicott guardians. Small unencrypted usb devices do go missing, are left in drives or are simply mislaid."
	55	(Mean)	
ID17	**75**		"Assets within a medical environment are less protected because almost every body can enter these areas an take the asset (theft) or medical personal forgets these assets due to the dynamics of their works."
ID20	**50-100**		"This applies more to paper than to electronic assets as mobile devices are encrypted or subject to strict security controls if encryption is not possible e.g. some medical devices. By unattended I have assumed that this excludes criminal activity ege losses as a result of a break in into a secure area. Again the narrative and the numbers don't match. To minimize the risk of this data should be in lockable, traceable, tamper proof bags and delivered securely point to point. "
	90	(Past experience)	
ID15	**>100**		"very likely with USB sticks or smartphones. Or even paper files !"
ID18	**200**	(highest)	"Convenience makes people take (copies of) information with them often. There is hardly any accounting around such actions. Hence, discovery rate is low."



Scenario: Wrong privileges set

An internal employee on the premises was unintentionally given the wrong privileges or authorisations, causing disclosure of personal patient information to unauthorised persons.

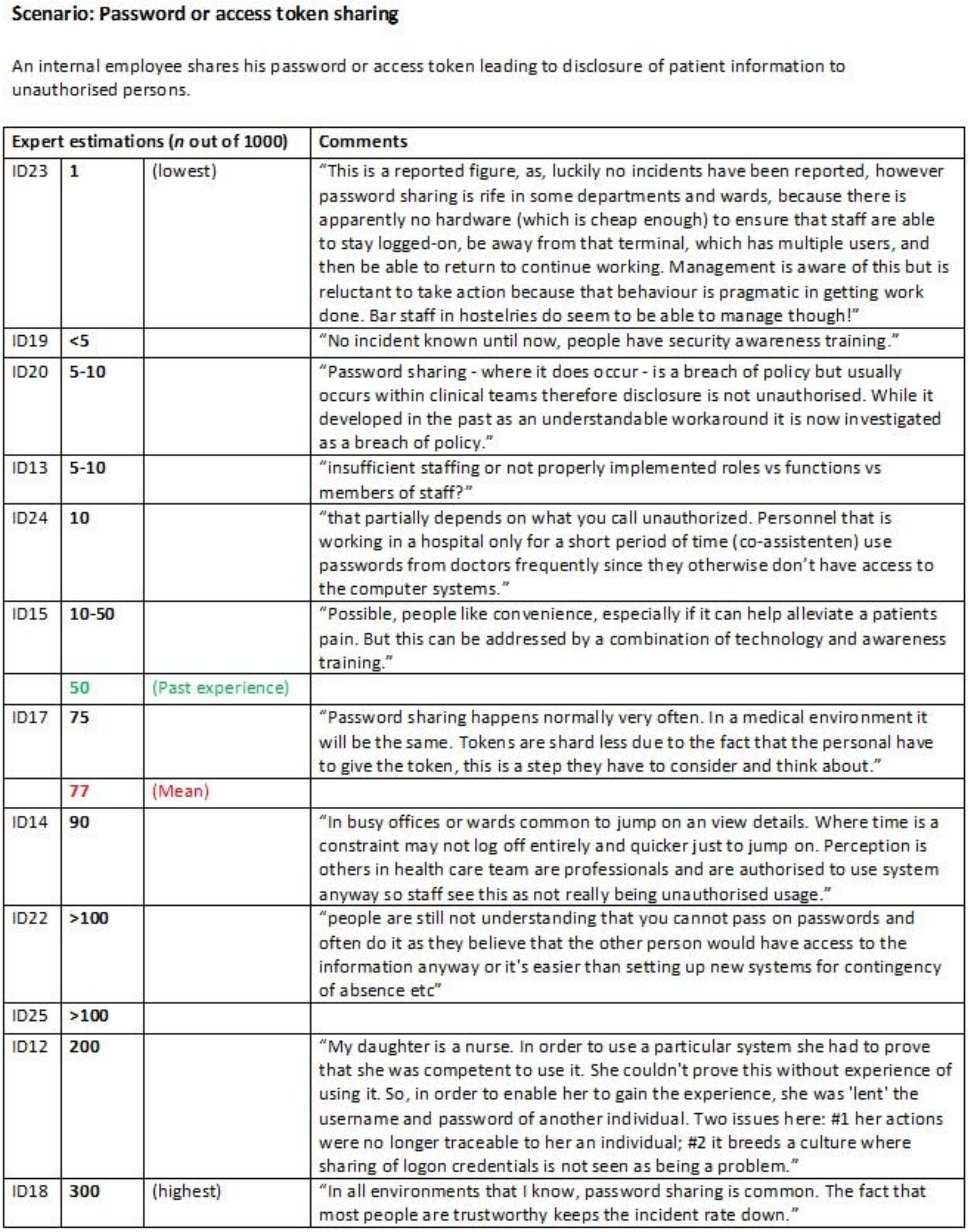
Expert estimations (*n* out of 1000)			Comments
ID23	**0**	(lowest)	"Rare – usually due to misaddressing external mail, and rarely during a 'phone conversation." (note by researcher: comment seems to be mixed up with different scenario?)
ID19	**<5**		"Covered by procedures"
ID20	**<5**		"This is reviewed regularly and the fairwarning system audits access on a monthly basis. This is not disclosure but breach of policy requiring disciplinary action."
ID24	**5**		"the staff is well trained and they always ask who is the contact person."
ID13	**5-10**		"depending on the creation of sub-folders or share-point folders"
ID22	**5-10**		
ID14	**8**		"Most user privileges are set by IT staff following the completion of an IM&T user uthori uthorizingn form. This is issued to staff and counter signed by line managers. Therefore errors in processing accounts are rare however this does not exclude illegible handwriting leading to wrong authorisations. In the event of illegible instructions leading to confusion, the line manager a1authorizing the form is contacted."
	33	(Mean)	
ID25	**10-50**		
ID12	**50**		"There is a generally agreed principle in healthcare that anyone who is providing care to an individual should have access to all the patient information to enable them to give the highest quality of care. There is, naturally, no need for admin staff to have the same access to detailed medical information as healthcare professionals need, and this is where there is likely to data creep, particularly in the private sector where admin staff need to bill individual patients for services and products provided."
ID18	**60**		"Identity management is hard to get right, discovering misauthorizations is hard, not all instances will lead to disclosure incidents."
	60	(Past experience)	
ID15	**50-100**		"I see it in many organisations. People accumulate access rights and the periodic review to clean that up does not happen."
ID17	**150**	(highest)	"Identity and access management and a proper implementation of authorization op electronic patient information has not been implemented very often and successfully."



Scenario: Procedure not followed

An internal employee located on the premises does not follow the formal procedures leading to disclosure of patient information.

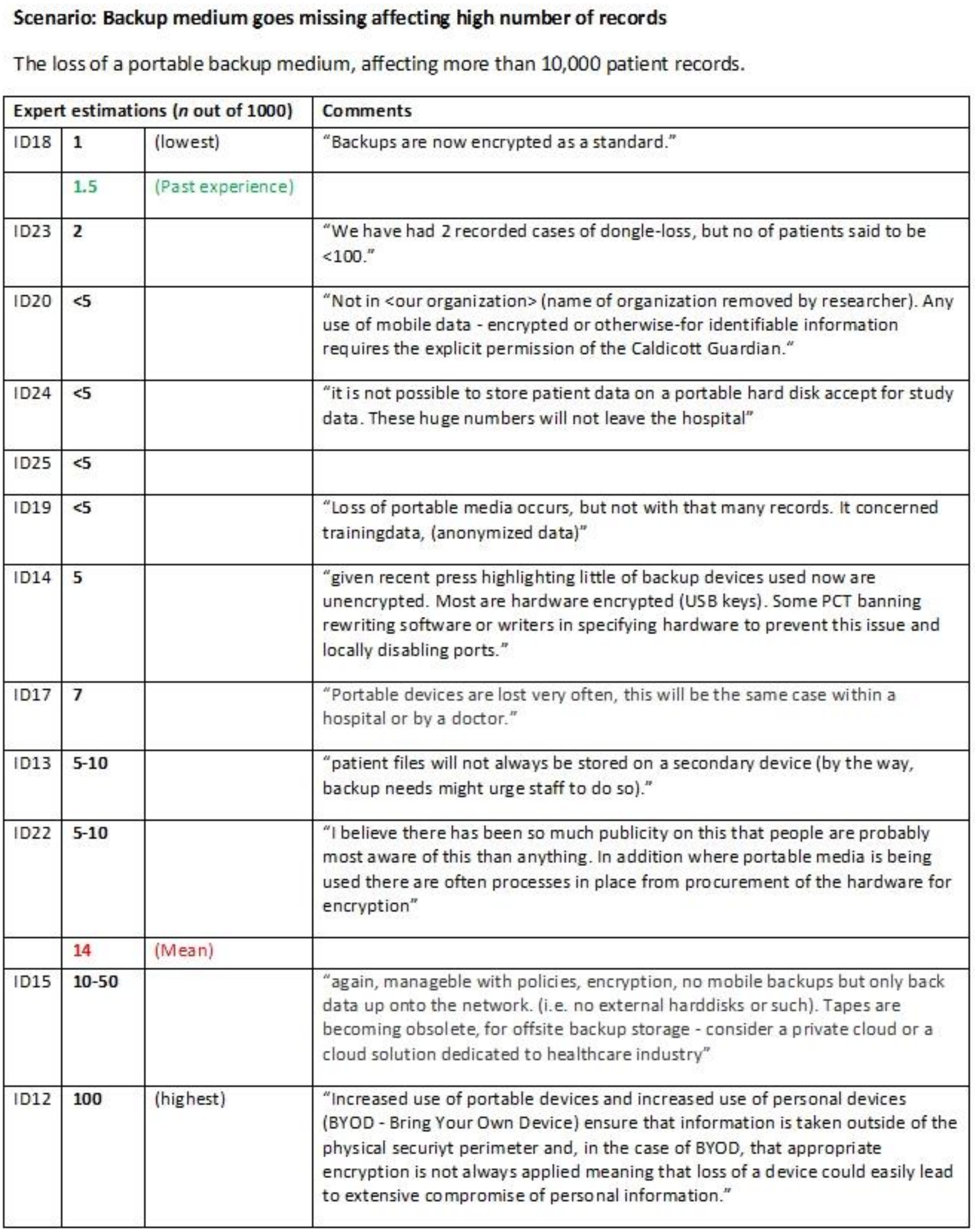
Expert estimations (*n* out of 1000)			Comments
ID23	**1**	(lowest)	
ID19	**<5**		"I don't know how many, but this occurs once in a while."
ID24	**5**		
ID15	**5-10**		"it all depends on user awareness, training, sanctions, and perhaps the motivation for intentional disclosure."
ID17	**10**		"Procedure are normally followed precisely within medical environments."
ID18	**30**		"Not following procedures happens regularly. We tend to be helpful, fix problems outside of procedures. Procedures contain checks to contain and correct this behavior. We are increasingly getting better at this - hence the number of instances should decrease."
	40	(Past experience)	
	44	(Mean)	
ID14	**50**		"Maybe more common since leaving documents in an office is common whilst on break etc. Not really seen as an incident by staff concerned as patients often not in the admin areas. In clinical areas different matter as patients often could be near paper or electronic based records and could see other individuals records. May be more frequent due to lack of reporting or patient complaints."
ID13	**50-100**		"to often patient data handling urgency overrules the safe conduct; else staff is not aware of any policies (unskilled or low skilled staff) or does not has any interest (high or extremely specialised skilled staff)..."
ID25	**50-100**		
ID22	**50-100**		
ID12	**100**		"Ignorance or seeing rules as 'getting in the way' will always ensure that this is a high risk. It can only be countered by good security awareness training programmes."
ID20	**>100**	(highest)	"This is dealt with as a disciplinary matter as all new employees are trained including all new clinical staff. Usually. failure to follow procedure increases risk but does not lead to disclosure outside the NHS. The most common failure to follow procedure links to staff not placing confidential material in lockable, traceable, tamper-proof bags."



Scenario: Password or access token sharing

An internal employee shares his password or access token leading to disclosure of patient information to unauthorised persons.

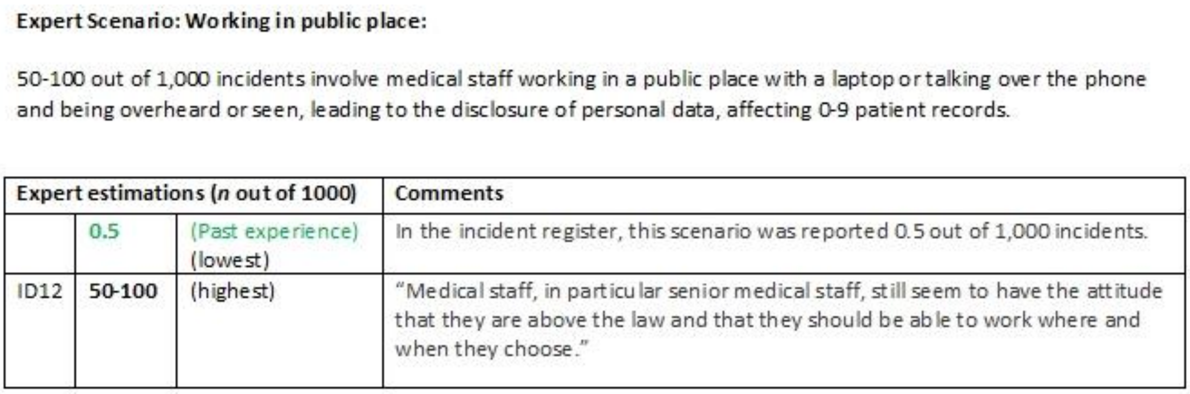
Expert estimations (*n* out of 1000)			Comments
ID23	**1**	(lowest)	"This is a reported figure, as, luckily no incidents have been reported, however password sharing is rife in some departments and wards, because there is apparently no hardware (which is cheap enough) to ensure that staff are able to stay logged-on, be away from that terminal, which has multiple users, and then be able to return to continue working. Management is aware of this but is reluctant to take action because that behaviour is pragmatic in getting work done. Bar staff in hostelries do seem to be able to manage though!"
ID19	**<5**		"No incident known until now, people have security awareness training."
ID20	**5-10**		"Password sharing - where it does occur - is a breach of policy but usually occurs within clinical teams therefore disclosure is not unauthorised. While it developed in the past as an understandable workaround it is now investigated as a breach of policy."
ID13	**5-10**		"insufficient staffing or not properly implemented roles vs functions vs members of staff?"
ID24	**10**		"that partially depends on what you call unauthorized. Personnel that is working in a hospital only for a short period of time (co-assistenten) use passwords from doctors frequently since they otherwise don't have access to the computer systems."
ID15	**10-50**		"Possible, people like convenience, especially if it can help alleviate a patients pain. But this can be addressed by a combination of technology and awareness training."
	50	(Past experience)	
ID17	**75**		"Password sharing happens normally very often. In a medical environment it will be the same. Tokens are shard less due to the fact that the personal have to give the token, this is a step they have to consider and think about."
	77	(Mean)	
ID14	**90**		"In busy offices or wards common to jump on an view details. Where time is a constraint may not log off entirely and quicker just to jump on. Perception is others in health care team are professionals and are authorised to use system anyway so staff see this as not really being unauthorised usage."
ID22	**>100**		"people are still not understanding that you cannot pass on passwords and often do it as they believe that the other person would have access to the information anyway or it's easier than setting up new systems for contingency of absence etc"
ID25	**>100**		
ID12	**200**		"My daughter is a nurse. In order to use a particular system she had to prove that she was competent to use it. She couldn't prove this without experience of using it. So, in order to enable her to gain the experience, she was 'lent' the username and password of another individual. Two issues here: #1 her actions were no longer traceable to her an individual; #2 it breeds a culture where sharing of logon credentials is not seen as being a problem."
ID18	**300**	(highest)	"In all environments that I know, password sharing is common. The fact that most people are trustworthy keeps the incident rate down."



Scenario: Backup medium goes missing affecting high number of records

The loss of a portable backup medium, affecting more than 10,000 patient records.

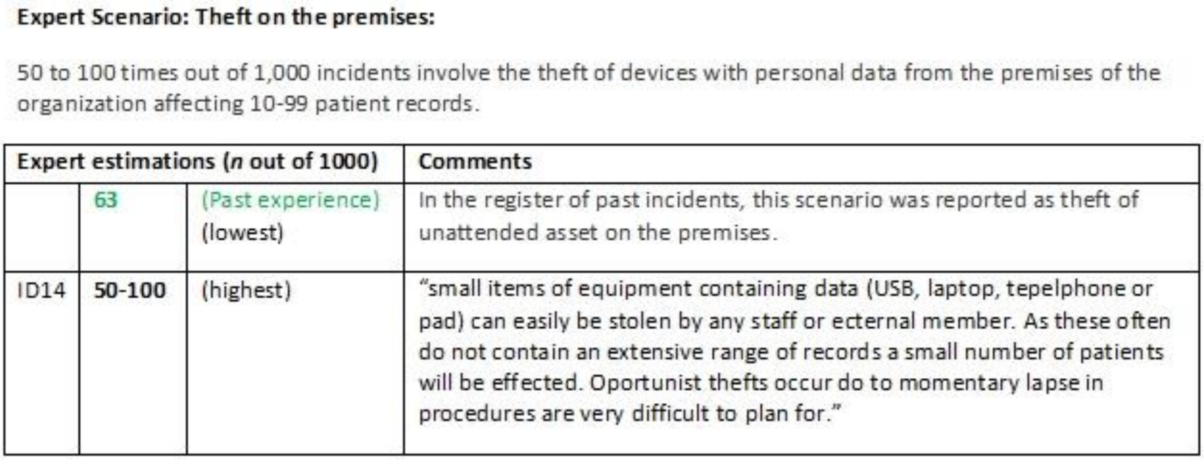
Expert estimations (*n* out of 1000)			Comments
ID18	**1**	(lowest)	"Backups are now encrypted as a standard."
	1.5	(Past experience)	
ID23	**2**		"We have had 2 recorded cases of dongle-loss, but no of patients said to be <100."
ID20	**<5**		"Not in <our organization> (name of organization removed by researcher). Any use of mobile data - encrypted or otherwise-for identifiable information requires the explicit permission of the Caldicott Guardian."
ID24	**<5**		"it is not possible to store patient data on a portable hard disk accept for study data. These huge numbers will not leave the hospital"
ID25	**<5**		
ID19	**<5**		"Loss of portable media occurs, but not with that many records. It concerned trainingdata, (anonymized data)"
ID14	**5**		"given recent press highlighting little of backup devices used now are unencrypted. Most are hardware encrypted (USB keys). Some PCT banning rewriting software or writers in specifying hardware to prevent this issue and locally disabling ports."
ID17	**7**		"Portable devices are lost very often, this will be the same case within a hospital or by a doctor."
ID13	**5-10**		"patient files will not always be stored on a secondary device (by the way, backup needs might urge staff to do so)."
ID22	**5-10**		"I believe there has been so much publicity on this that people are probably most aware of this than anything. In addition where portable media is being used there are often processes in place from procurement of the hardware for encryption"
	14	(Mean)	
ID15	**10-50**		"again, manageble with policies, encryption, no mobile backups but only back data up onto the network. (i.e. no external harddisks or such). Tapes are becoming obsolete, for offsite backup storage - consider a private cloud or a cloud solution dedicated to healthcare industry"
ID12	**100**	(highest)	"Increased use of portable devices and increased use of personal devices (BYOD - Bring Your Own Device) ensure that information is taken outside of the physical securiyt perimeter and, in the case of BYOD, that appropriate encryption is not always applied meaning that loss of a device could easily lead to extensive compromise of personal information."



Expert Scenario: Working in public place:

50-100 out of 1,000 incidents involve medical staff working in a public place with a laptop or talking over the phone and being overheard or seen, leading to the disclosure of personal data, affecting 0-9 patient records.

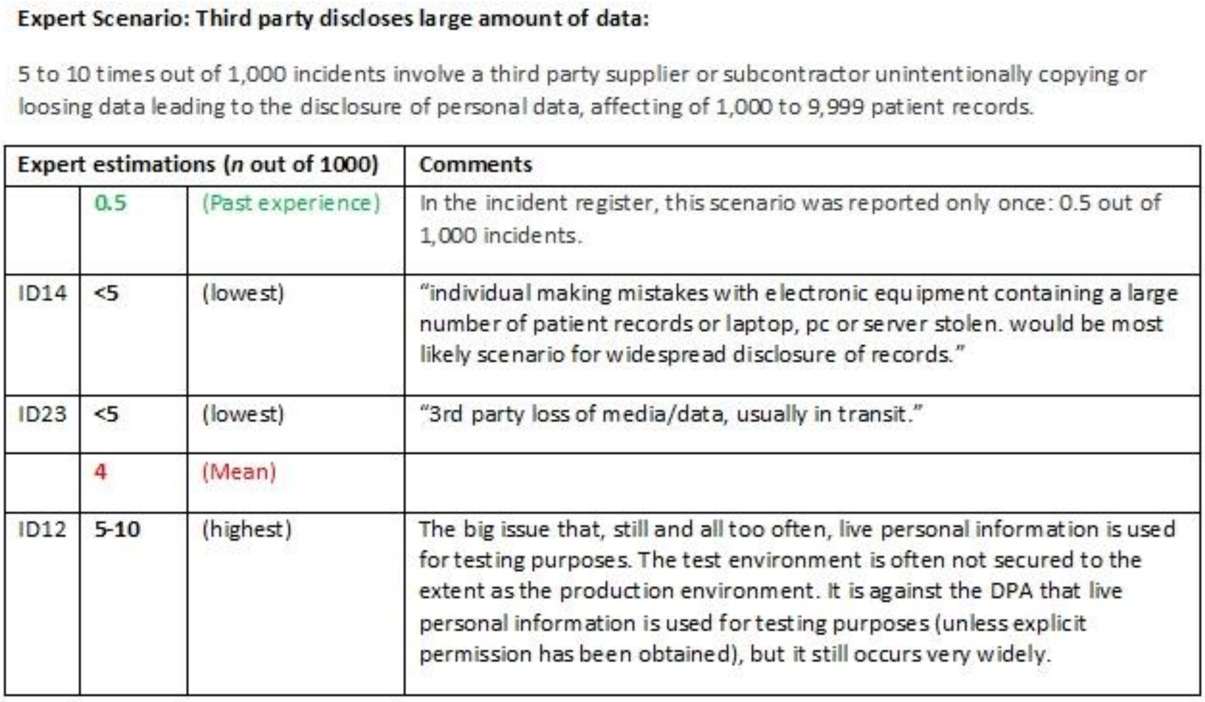
Expert estimations (*n* out of 1000)			Comments
	0.5	(Past experience) (lowest)	In the incident register, this scenario was reported 0.5 out of 1,000 incidents.
ID12	**50-100**	(highest)	"Medical staff, in particular senior medical staff, still seem to have the attitude that they are above the law and that they should be able to work where and when they choose."



Expert Scenario: Theft on the premises:

50 to 100 times out of 1,000 incidents involve the theft of devices with personal data from the premises of the organization affecting 10-99 patient records.

Expert estimations (*n* out of 1000)			Comments
	63	(Past experience) (lowest)	In the register of past incidents, this scenario was reported as theft of unattended asset on the premises.
ID14	**50-100**	(highest)	"small items of equipment containing data (USB, laptop, tepelphone or pad) can easily be stolen by any staff or ecternal member. As these often do not contain an extensive range of records a small number of patients will be effected. Oportunist thefts occur do to momentary lapse in procedures are very difficult to plan for."



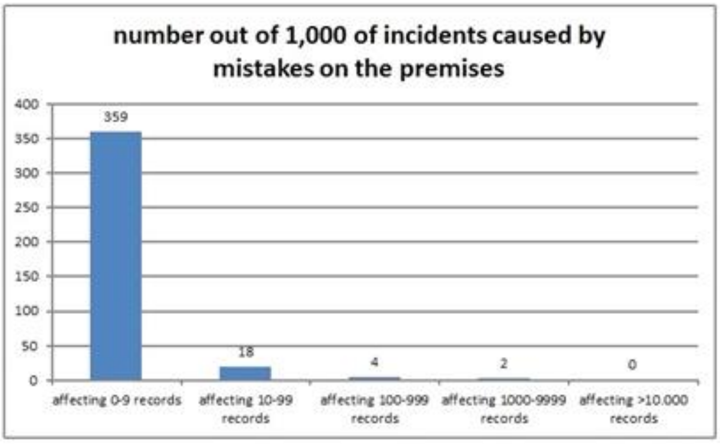
Expert Scenario: Third party discloses large amount of data:

5 to 10 times out of 1,000 incidents involve a third party supplier or subcontractor unintentionally copying or loosing data leading to the disclosure of personal data, affecting of 1,000 to 9,999 patient records.

Expert estimations (*n* out of 1000)			Comments
	0.5	(Past experience)	In the incident register, this scenario was reported only once: 0.5 out of 1,000 incidents.
ID14	<5	(lowest)	"individual making mistakes with electronic equipment containing a large number of patient records or laptop, pc or server stolen. would be most likely scenario for widespread disclosure of records."
ID23	<5	(lowest)	"3rd party loss of media/data, usually in transit."
	4	(Mean)	
ID12	**5-10**	(highest)	The big issue that, still and all too often, live personal information is used for testing purposes. The test environment is often not secured to the extent as the production environment. It is against the DPA that live personal information is used for testing purposes (unless explicit permission has been obtained), but it still occurs very widely.

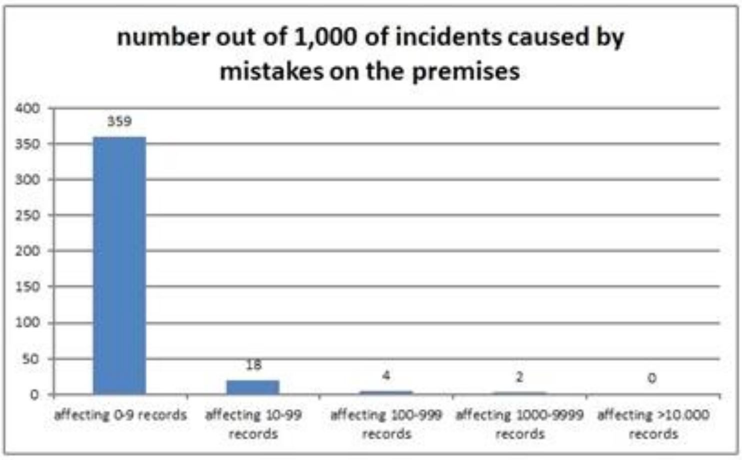
Expert Scenario: Mistakes impacting 1,000-9,999 records:

50 to 100 out of 1,000 incidents involve medical or other internal staff making a mistake affecting 1,000-9,999 patient records.

Expert estimations (*n* out of 1000)			Comments
	2	(Past experience) (lowest)	In the register of past incidents, this scenario occurred 2 times out of 1000 incidents. However, the combination of this scenario with a lower number of records affected (<10) showed a higher frequency: 359 out of 1,000 incidents.  number out of 1,000 of incidents caused by mistakes on the premises
ID25	**10-50**		
ID18	**50-100**	(highest)	Biggest risk is still internal mistakes, because of the high impact.

Expert Scenario: Mistakes impacting 10-99 records:

5 to 10 out of 1,000 incidents involve medical staff making a mistake affecting 10-99 patient records.

Expert estimations (*n* out of 1000)			Comments
ID23	**5-10**	(lowest)	"Transiently, the commonest problem in this trust. Usually junior medical staff losing handover lists, or similar documents."
	18	(Past experience) (highest)	In the register of past incidents, this scenario occurred 18 times out of 1000. 

Expert Scenario: External groups:

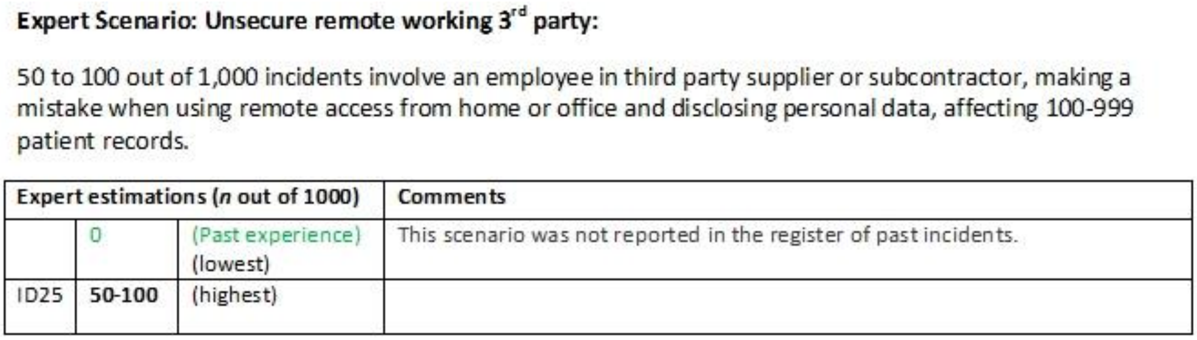
5 times out of 1,000 incidents involve external groups or activists wanting to steal, access, abuse or manipulate personal data.

Expert estimations (*n* out of 1000)			Comments
	0	(Past experience)	In the incident register, this scenario was not reported.
ID18	**<5**	(lowest)	The 'major hack' will happen, and when it happens it will affect a large number of patient records. It is hard to estimate how likely this is, hence I am reserved.
	5	(Mean)	
ID13	**5-10**	(highest)	"foreign countries or groups of activists (organised crime)"

Expert Scenario: Unsecure remote working:

5 to 10 out of 1,000 incidents involve an internal employee loosing data through an insecure remote working environment.

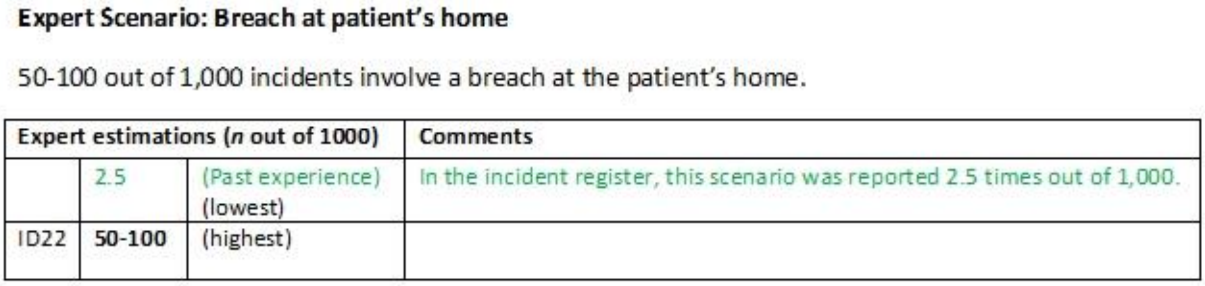
Expert estimations (*n* out of 1000)			Comments
	0.5	(Past experience) (lowest)	In the incident register, this scenario was reported in 0.5 cases out of 1,000.
ID19	**5-10**	(highest)	



Expert Scenario: Unsecure remote working 3rd party:

50 to 100 out of 1,000 incidents involve an employee in third party supplier or subcontractor, making a mistake when using remote access from home or office and disclosing personal data, affecting 100-999 patient records.

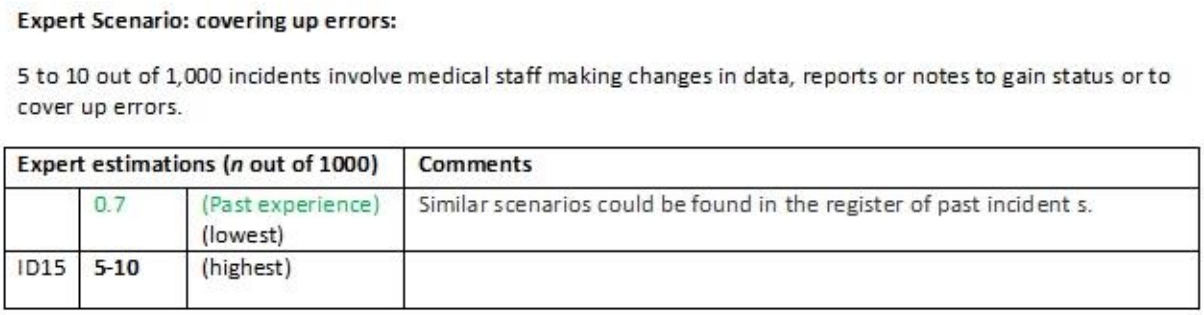
Expert estimations (*n* out of 1000)			Comments
	0	(Past experience) (lowest)	This scenario was not reported in the register of past incidents.
ID25	**50-100**	(highest)	



Expert Scenario: Breach at patient's home

50-100 out of 1,000 incidents involve a breach at the patient's home.

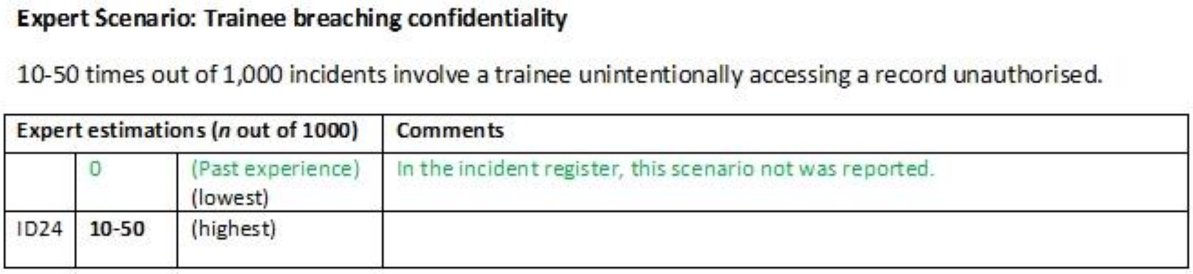
Expert estimations (*n* out of 1000)			Comments
	2.5	(Past experience) (lowest)	In the incident register, this scenario was reported 2.5 times out of 1,000.
ID22	**50-100**	(highest)	



Expert Scenario: covering up errors:

5 to 10 out of 1,000 incidents involve medical staff making changes in data, reports or notes to gain status or to cover up errors.

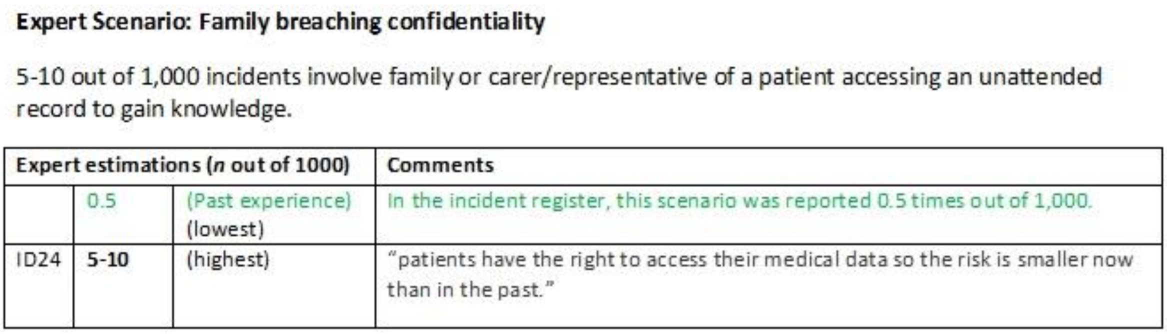
Expert estimations (*n* out of 1000)			Comments
	0.7	(Past experience) (lowest)	Similar scenarios could be found in the register of past incident s.
ID15	**5-10**	(highest)	



Expert Scenario: Trainee breaching confidentiality

10-50 times out of 1,000 incidents involve a trainee unintentionally accessing a record unauthorised.

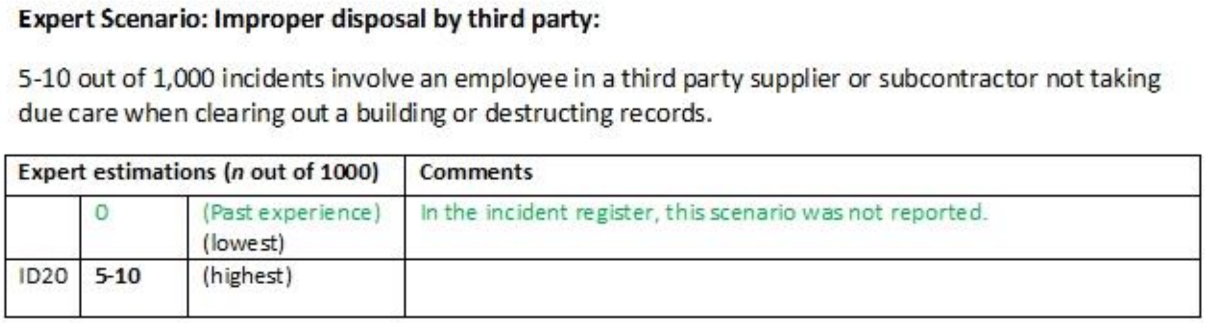
Expert estimations (*n* out of 1000)			Comments
	0	(Past experience) (lowest)	In the incident register, this scenario not was reported.
ID24	**10-50**	(highest)	



Expert Scenario: Family breaching confidentiality

5-10 out of 1,000 incidents involve family or carer/representative of a patient accessing an unattended record to gain knowledge.

Expert estimations (*n* out of 1000)			Comments
	0.5	(Past experience) (lowest)	In the incident register, this scenario was reported 0.5 times out of 1,000.
ID24	**5-10**	(highest)	"patients have the right to access their medical data so the risk is smaller now than in the past."



Expert Scenario: Improper disposal by third party:

5-10 out of 1,000 incidents involve an employee in a third party supplier or subcontractor not taking due care when clearing out a building or destructing records.

Expert estimations (*n* out of 1000)			Comments
	0	(Past experience) (lowest)	In the incident register, this scenario was not reported.
ID20	**5-10**	(highest)	

Delphi study questionnaire Round 3

For each scenario:
Please give your final estimation how many times out of 1,000 incidents this scenario will occur in the near future. After 2 survey rounds, the combined estimation of all experts is 88.5 times per 1,000 incidents.*

Password or access token sharing
In this scenario, an employee shares a password or access token with someone and as a consequence patient information is disclosed to an unauthorised person. 66% of the expert panel agreed in Round 2 that this scenario is likely to occur more frequently than the incident registers had shown. The panel estimates that the frequency will be between 50 and 100 times out of a 1,000 incidents (past experience showed 50 times out of 1,000). The comment from the expert who estimated the lowest frequency, suggests that 'there is no evidence that this happens'. The experts rating the frequency the highest suggest that 'it is not possible for staff to work without sharing passwords'.
Read all details from Round 2 (statistics, all comments, all estimated frequencies) in this document: Password-access token sharing (link opens PDF).

Theft on the premises
This was a scenario created by an expert in Round 1. The scenario involves the theft of devices with personal data stored on it from the premises of the organisation. The scenario was also reported frequently in the incident registers although the experts together estimate the frequency a little lower (the combined experts estimation is 50 times per 1,000 incidents), and the past experience frequency is 63 times).

56% of the experts agree that this scenario happens sometimes. One expert suggests that this scenario could be combined with lost assets, as it is often not clear whether an item was lost or stolen. Another expert estimates the frequency of this scenario as very low, suggesting that ‘people are becoming more aware’.
Read all details from Round 2 (statistics, all comments, all estimated frequencies) in this document: Theft on the premises (link opens PFD).

Procedure not followed
Not following the formal procedures could lead to the disclosure of patient information. The experts estimated the possible frequency of occurrence of this scenario as similar to the frequency of past incidents (40 times out of 1,000 incidents).
Half of the experts in the panel estimate the frequency to be between 10 and 50 times per 1,000 incidents. Round 2 showed outliers with higher estimations and lower estimations. Most of the comments made by the experts refer to staff often breaching policy and procedures but ‘this is not always reported as an incident’.
Read all details from Round 2 (statistics, all comments, all estimated frequencies) in this document: Procedure not followed (link opens PDF).

Mistakes
A little less than 400 out of 1,000 scenarios in the register of past incidents were due to mistakes made by internal staff. Most frequently, these mistakes affected less than 10 patient records per incident. Incidents that affected more than 1,000 records occured rarely (2 times out of 1,000).
In contrast, mistakes affecting a low number of records occurred 371 times out of 1,000 in the past, and there are many possible sub-scenarios within these 371. Some of these sub-scenarios involve the leaving of assets or paper records unattended or sending emails to the wrong recipient. These sub-scenarios are described below.
Mistakes affecting more than 1,000 records
Only a few incidents affected more than 1,000 patient records (2 times out of 1,000 in contrast to the more frequent (371.5) mistakes affecting less than 10 records). The experts appear to agree that the mistakes impacting a high number of records occur more frequently than 2 times out of 1,000 (35 times).
Read all details from Round 2 (statistics, all comments, all estimated frequencies) in this document: Mistakes affecting high number of records (link opens PDF).

Email to wrong recipient
This scenario was reported the most frequent in the registers of past incidents. It involves emails containing personal data of patients being sent to either the wrong recipients and/or to persons not authorised to receive that information. The experts did not estimate the possible frequency of occurrence to be as high as it occured in the registers, although the estimations in Round 1 varied within a range of 99. The range of answers declined in Round 2. The consensus rate went up from 42% to 70%.
70% of the experts expect the frequency of occurrence of this scenario to be between 10 and 50 times per 1,000 incidents (this scenario will happen sometimes), in contrast to past experience which was 100. Round 2 showed only outliers on the lower side. From the comments made by one of these experts, this lower estimation could be explained by the different solution that the expert's organisation uses instead of email.
Read all details from Round 2 (statistics, all comments, all estimated frequencies) in this document: Email to wrong recipient (link opens PDF).

Unattended asset goes missing

This scenario was reported as the second most frequent in the registers of past incidents (90 times out of 1,000 incidents). The experts estimate the possible frequency of occurrence lower (45), although there seems to some disagreement. Reading through the comments, the diversity could be explained by lower estimations from experts working in organisations where there is no storage of patient data possible on smaller devices such as memory sticks and portable devices, where the comments from experts who are rating the frequency higher refer to the use of sticks, phones and other small devices to store data. However, this scenario refers to paper records as well as electronic assets.

Read all details from Round 2 (statistics, all comments, all estimated frequencies) in this document: Unattended asset goes missing (link opens PDF).

Business partner, supplier or contractor discloses patient data

The scenario where a third party causes a data breach was mentioned by 3 experts in Round 1 and their scenarios were combined into one. After Round 2, all experts agree that the frequency of occurrence is less than 10 times out of 1,000 incidents with a combined estimated frequency of 5. With a range of answers of 7, and a small standard deviation, this is the scenario with the best consensus.

However, this scenario is at a high abstraction level and many sub-scenarios can be identified within this scenario.

One of them is a more specific scenario that was suggested by one of the experts in Round 1 of the survey, where the third party causes a breach through an unsecure remote working environment. There were no reports of this kind of incidents in the register of incidents that was used for this study but in Round 2 of the survey some experts estimated the frequency of this scenario higher than the 5 that was given for the more general scenario above.

A second possible sub-scenario is the improper disposal of paper records by a third party. This scenario was suggested by an expert in Round 1 and in Round 2 all experts estimated the frequency of this scenario as less than 10 times out 1,000 incidents. Comments made in Round 2 indicate that it could happen rather often when buildings are cleared or when old paper files are archived before disposal by third parties.

The register of past incidents showed that the most frequent reported type of incidents caused by third parties was the loss of paper records or reports with personal data through the post and the second most frequent was unsecured emailing. The frequencies of these incidents were very low so they were not included as scenarios in the Delphi study.

Read all details from Round 2 (statistics, all comments, all estimated frequencies) in this document: Business partner discloses data (link opens PDF).

Wrong privileges or authorisations set

This scenario describes how confidentiality breaches are caused by flaws in the settings of authorisations and privileges, causing unauthorised access to patient data. The experts estimate the possible frequency of occurrence lower than the frequency of past incidents showed (60 times per 1,000 incidents). The range of expert estimations decreased in Round 2 and 60% now estimate that this scenario will occur 10 to 50 times out of 1,000 incidents. Round 2 showed a few outlying answers. From the comments made by the experts who estimate the frequency of occurrence as high, it seems that, according to their opinion, ‘identity and access management are not often implemented successfully in organisations’. The profiles of these experts (ID14, ID15, and ID17 in Round 1) show that these are the panel members with the highest expertise level in IT security. On the contrary, the experts who rated the frequency the lowest, refer in their comments' to be confident that the procedures should cover this risk and to have confidence in the IT staff'.

Read all details from Round 2 (statistics, all comments, all estimated frequencies) in this document: Wrong privileges set (link opens PDF).

Working in a public place

This was a scenario created by an expert in Round 1. It suggests that medical staff can be overheard when they discuss a patient over the phone in a public place, or that it can be seen by others what they are working on when they work on a laptop, leading to a confidentiality breach. In Round 2, the respondents estimated the frequency for this scenario quite differently. In most of comments that were made, it is suggested that this scenario is likely to be related to awareness and attitude of medical staff and the environment that they work in.

Read all details from Round 2 (statistics, all comments, all estimated frequencies) in this document: Working in a public place (link opens PDF).

Backup goes missing scenario

Backup medium goes missing

This is the 'disaster' scenario, the one that caused the highest number of patient records exposed in the register of past incidents. It happened 1.5 times out of 1,000 incidents and the experts seem to rate the frequency of this kind of scenario slightly higher. The scenario refers to the main system backups with the full database of patient records and not to portable 'convenience' backup devices which a smaller number of patient data. The comments in Round 2 made by experts who used the correct interpretation referred to encryption and cloud computing as emerging standard practice that will prevent this incident from happening in the future. After Round 2, the expert's estimations are still very diverse, possibly caused by the misinterpretation of this scenario.

Read all details from Round 2 (statistics, all comments, all estimated frequencies) in this document: Backup goes missing (link opens PDF).

Copy data to portable storage medium

This scenario occurs when a person copies personal data on a portable storage medium for convenience and transports it anywhere. The breach is the act of copying the data, which could affect personal details of 100 to 999 patients. The scenario was created in Round 1 and there were only a few comments on this scenario, varying from 'we are not aware of this happening' to 'it is happening'.

Read all details from Round 2 (statistics, all comments, all estimated frequencies) in this document: Copy data to storage medium (link opens PDF).

Family of patient accesses patient's record

This scenario occurs when a family member, a representative or carer of the patient accesses the unattended record. This rare scenario (0.5 times out of 1,000 incidents in the register of past incidents) was suggested by an expert in Round 1 and most experts agree that the frequency of occurrence will be fewer than 10 out of 1,000 incidents. One of the comments shows a different interpretation of this scenario, where the family member discloses information about the patient to a third person. However, this point of view is a different scenario and not the one meant here.

Read all details from Round 2 (statistics, all comments, all estimated frequencies) in this document: Family accesses record (link opens PDF).

Unsecured remote working
This scenario was proposed as an emerging risk as remote working for hospital employees is growing. The scenario not only applies to the digital connection to the organisation's network, but also to the paper based data and memory sticks that are being taken to the external location and could get lost or gone missing. The expert's estimations varied in Round 2 but most seem to estimate this scenario as a very rare one.
Read all details from Round 2 (statistics, all comments, all estimated frequencies) in this document: Unsecured remote working (link opens PDF).

Trainee breaching confidentiality
This scenario was proposed by one expert in Round 1 and it involves a trainee accessing a patient record without authorisation. Possible causes could be telling about their new job to friends or looking up a celebrity's status. It could also be unintentional when a name is mistyped and another data set is accessed. Most experts expect that this scenario happens less than 5 times out of 1,000 incidents.
Read all details from Round 2 (statistics, all comments, all estimated frequencies) in this document: Trainee breaching confidentiality (link opens PDF).

External groups
This scenario was proposed by 2 experts in Round 1. It involves external groups or activists abusing several vulnerabilities to gain access to data to destroy it, change it or otherwise abuse, publish or damage it. In Round 2 this was mostly evaluated as a very rare scenario. The comments vary from the opinion that it will happen for sure to that it is very unlikely to happen at all in healthcare.
Read all details from Round 2 (statistics, all comments, all estimated frequencies) in this document: External groups (link opens PDF).

Covering up errors
A scenario where medical staff making changes in data, reports or notes to gain status or to cover up errors occurred in register of past incidents, although very rarely (0.7 times out of 1,000 incidents). In Round 2, the combined estimation by the experts is 2.5. The comments that were made by experts in Round 2 varied from 'this is not applicable' to 'this happens more often than perceived'.
Read all details from Round 2 (statistics, all comments, all estimated frequencies) in this document: Covering up errors (link opens PDF)

Breach at a patient's home
This scenario was suggested in Round 1 by one expert, who estimated the frequency of this scenario to be about 75 times out of 1,000 incidents. Breaches of confidentiality at a patient's home were reported in the register of past incidents with a frequency of 2.5 times out of 1,000 incidents.

In Round 2, the comments about this scenario are very diverse but all expected frequencies are lower than 51. It has been suggested that since the impact is low, it is not a very important scenario. Another comment states that data is being updated by staff at the patient’s home and the informal environment influences security awareness and records are not always marked as confidential.
Read all details from Round 2 (statistics, all comments, all estimated frequencies) in this document: Breach at a patient's home (link opens PFD).

Appendix D: Interview questions

IT Security Manager

Introduction (5 minutes)

Introduce self.
Describe research and goals.
Explain consent form and sign.
Interview will be semi structured. The questions below are representative of what I will ask, but I expect other questions to emerge during the course of the interviews.

General (10 minutes)

How are information security related responsibilities (IT security, Caldicott Guardian, Data Protection, Freedom of information, Records management, risk management, and quality management) organised?
How do these roles link into each other and to the Scottish Information Governance Board?
Are the NHS Scotland Information Governance Standards (September 2007) leading in the way GGC has organised information governance?
How does your organisation position Information Security (is it mainly an ICT 'thing' or does it have a wider scope)?
Which developments in society or politics will influence the NHS's approach to information security in the future?

Information security risk assessment approach in the organisation (30 minutes)

Which method and techniques for Information Security Risk Assessment are used in the organisation?

a. How often are information security risk assessments performed?
b. How long does one assessment take to complete (average)?
c. Which tools are used?
d. Who participates? (List of names & job title, these persons will be asked to complete a survey).
e. Do business partners, subcontractors or other organisations participate?
f. What is the scope/are the scopes of individual risk assessments (system, department, process, location, paper-based records/electronic records)?
g. How do you define the boundaries of the scope (where does a 'system' end?)?
h. How are results documented?
i. Who receives a copy of the risk register/report?

How does the risk register influence decision making?
How is the quality of the results evaluated?
How do you know that your risk forecasts are correct?
How is staff encouraged to report a risk when they perceive one during their daily routines?
If you have ever compared the results with the information security incident register, what was the conclusion?
If you have ever compared the results with other organisations, how did you do that and did it add value to you?

If you have ever evaluated the usability and quality of the method with the participants, what were the opinions?
What do you think could be improved on your method?
How do you think information security risks will be monitored in 2023?
What do you generally see as the biggest risks to information security today and in the future?

Incident reporting (10 minutes)

Apart from the existing procedures for incident reporting, how are employees encouraged to report an incident or near miss?
How often do you get such information?
Have you ever compared the incident register with other organisations (benchmarking)?
If yes: how, how often, did it add value to you?
If not: why not and would you want to?

Close interview (5 minutes)

Thank for participation.
The report of this interview will be emailed shortly.
Discuss next step (survey & document review of risk and incident registers).

Information Governance

Introduction (5 minutes)

Introduce self.
Describe research and goals.
Explain consent form and sign.
Interview will be semi structured. The questions below are representative of what I will ask, but I expect other questions to emerge during the course of the interviews.

General (10 minutes)

How is Information governance organised within your department and how is that related to other responsibilities (IT security, Caldicott Guardian, Data Protection, Freedom of information, Records management, risk management, and quality management)?
Which developments in society or politics will influence the NHS's approach to information governance in the future?
How does your organisation position Information Security (is it mainly an ICT 'thing' or does it have a wider scope)?

Information security risk assessment approach in the organisation (20 minutes)

How are risks to the security of personal and other important information identified within the department?
How often do you participate in information security risk assessments organised by or organised together with other departments?
How does the risk register/report influence decision making?
How do you know that your risk forecasts are correct?
How is staff encouraged to report any risks they may suspect?

How is staff trained/educated in information security risk awareness?
What do you generally see as the biggest risks to information security today and in the future?
How do you think information security risks will be monitored in 2023?

Information security incident reporting (10 minutes)

How can staff report an incident?
What is your risk and incident reporting culture like? (are employees encouraged to report?)
How often do you receive such information?
Have you ever compared your incident register with other departments? (benchmarking)?
If yes: how, how often, did it add value to you?
If not: why not and would you want to?
Risk model (10 minutes)
Look at the classification of risk factors from the HI-risk model (will be provided during interview), are there any factor that could be added? Special attention to organisational and individual vulnerabilities.
Please comment on the top 10 of risk scenarios that were created in the HI-risk model (will be shown in separate document).

Close interview (5 minutes)

Thank for participation.
The report of this interview will be emailed shortly.
Discuss next step (observations).

Appendix E: Case study survey questions

1. Please indicate how much you agree with the following statements.

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Our organisation assesses information security risks with a practical approach.					
Our approach delivers reliable results.					
Our approach is the best possible way to assess risks.					
Our management is aware of the most important information security risks.					
The scope of our risk assessments is wide enough.					
The frequency of our risk assessment is enough.					
Our approach contributes positively to risk awareness in the organisation.					
The results give me what I need to mitigate risks in my daily work.					
The risk reports are used to make management decisions.					
Our risks are similar to those in any other NHS organisation.					
Our risks are similar to any other organisation in different industries.					

2. In your opinion, what could potentially be improved in the current approach that is used in your organisation?

3. Which of the following characteristics would you be interested in adding to the information risk assessment approach?

	Interested	Neutral	Not interested	Not sure
A comparison against risks identified by other organisations.				
A comparison of each risk register against the actual suffered incidents.				
A comparison against the opinions of security experts and trend watchers.				
A special list of human and organisation-related risks.				
A healthcare sector wide risk overview.				

1. An analysis performed in healthcare organisations resulted in a list of expected risk scenarios for the future. Below is a list of 5 possible risk scenarios (presented here in random order). Please rank them in order of the highest expected frequency of

occurrence in the near future (this year). The scenario that you would expect to occur the most often goes on top.

Drag items from the left-hand list into the right-hand list to order them.

- Assets (equipment, records, mobile phones and so on) go missing from the premises.
- Staff using each other's user account and password.
- Staff making mistakes with e-mail recipients or using private e-mail accounts to send patient information.
- Staff causes a security breach by not following the formal procedures.
- Staff gains access to data they should not have access to, caused by wrongly set or out-dated authorisations and privileges in the system.

5. Please describe which other significant risk(s) to the security of information you see occurring in your organisation?
6. What do you expect to become the biggest risk(s) to information security in healthcare in the next years?
7. How do you expect that information risks will be monitored 10 years from now?
8. How do you expect cybercrime to affect the healthcare infrastructure in the future?
9. How do you expect government policy to influence information security in the healthcare sector?