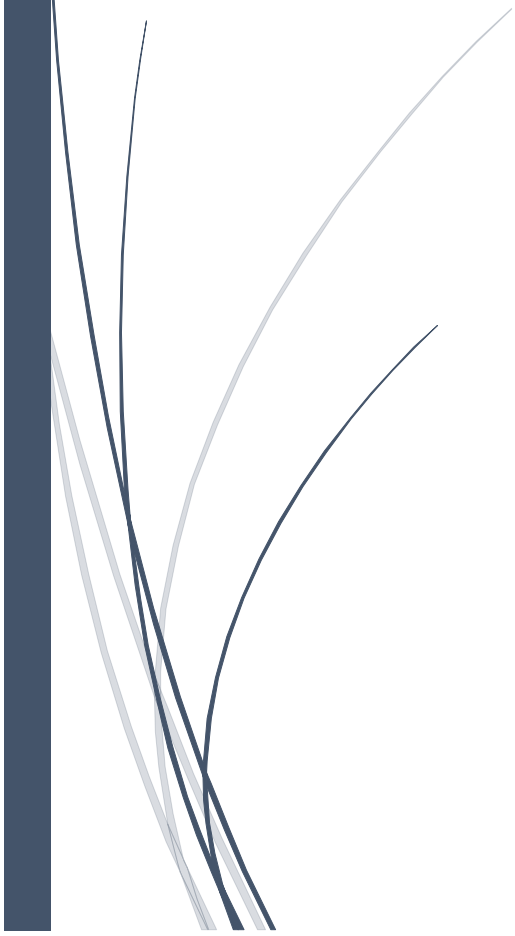
A Risk-Driven Investment Model for Analysing Human Factors in Information Security



Reza Alavi

UNIVERSITY OF EAST LONDON

A Risk-Driven Investment Model for Analysing Human Factors in Information Security

Reza Alavi

A thesis submitted for the degree of Doctor of Philosophy

The University of East London

School of Architecture, Computing and Engineering (ACE)

Director of Study: Doctor Shareeful Islam

Supervisor: Doctor Win See Lee

2016

Acknowledgements

Conducting PhD research is quite challenging. This becomes even more demanding if you are in full-time employment whilst having other commitments such as family and even a second part-time job.

I am very grateful to the University of East London for giving me an opportunity to conduct my PhD study. I would like to thank Dr. Shareeful Islam for assisting me during my studies in a challenging and competitive environment and supporting me in all aspects during the course of the research. This research could not have achieved its objectives without his precious and analytical insight and comments.

I also want to thank Dr. Sin Wee Lee for co-supervising this thesis, Professor Haralambos Mouratidis for his support throughout the work on my dissertation and my colleagues David, Rob, Neil, Sean, Salma, Peter and Trevor for their support throughout my research. During my research work, I collaborated with colleagues and friends in various universities and financial organisations to whom I wish to express my sincere gratitude.

Above all, I want to thank my wife and my son for supporting me in every step of my research and for giving me the greatest joy of my life. Finally, I would also like to thank all the staff at the University of East London, especially my ADI colleagues and the library for the wonderful times and support they gave me. I also would like to thank the admin team in the School of Computing and Graduate School for the fruitful help and advice they provided during the course of my research.

Copyright

Signed..... Date.....

Abstract

Information systems are of high importance in organisations because of the revolutionary industrial transformation undergone by digital and electronic platforms. A wide range of factors and issues forming the current business environments have created an unprecedented level of uncertainty and exposure to risks in all areas of strategic and operational activities in organisations including IT management and information security. Subsequently, securing these systems, which keep assets safe, serves organisational objectives. The Information Security System (ISS) is a process that organisations can adopt to achieve information security goals. It has gained the attention of academics, businesses, governments, security and IT professionals in recent years. Like any other system, the ISS is highly dependent on human factors as people are the primary concern of such systems and their roles should be taken into consideration. However, identifying reasoning and analysing human factors is a complex task. This is due to the fact that human factors are hugely subjective in nature and depend greatly on the specific organisational context. Every ISS development has unique demands both in terms of human factor specifications and organisational expectations. Developing an ISS often involves a notable proportion of risk due to the nature of technology and business demands; therefore, responding to these demands and technological challenges is critical. Furthermore, every business decision has inherent risk, and it is crucial to understand and make decisions based on the cost and potential value of that risk. Most research is solely concentrated upon the role of human factors in information security without addressing interrelated issues such as risk, cost and return of investment in security.

The central focus and novelty of this research is to develop a risk-driven investment model within the security system framework. This model will support the analysis and reasoning of human factors in the information system development process. It contemplates risk, cost and the return of investment on security controls. The model will consider concepts from Requirements Engineering (RE), Security Tropos and organisational context. This model draws from the following theories and techniques: Socio-technical theory, Requirements Engineering (RE), SWOT analysis, Delphi Expert Panel technique and Force Field Analysis (FFA). The findings underline that the roles of human factors in ISSs are not being fully recognised or embedded in organisations and there is a lack of formalisation of main human factors in information security risk management processes. The study results should confirm that a diverse level of understanding of human factors impacts security systems. Security policies and guidelines do not reflect this reality. Moreover, information security has been perceived as being solely the domain of IT departments and not a collective responsibility, with the importance of the support of senior management ignored. A further key finding is the validation of all components of the Security Risk-Driven Model (RIDIM). Model components were found to be iterative and interdependent. The RIDIM model provides a significant opportunity to identify, assess and address these elements.

Some elements of ISSs offered in this research can be used to evaluate the role of human factors in enterprise information security; therefore, the research presents some aspects of computer science and information system features to introduce a solution for a business-oriented problem. The question of how to address the psychological dimensions of human factors related to information security would, however, be a rich topic of research on its own. The risk-driven investment model provides tangible methods and values of relevant variables that define the human factors, risk and return on investment that contribute to organisations' information security systems. Such values and measures need to be interpreted in the context of organisational culture and the risk management model. Further research into the implementation of these measurements and evaluations for improving organisational risk management is required.

Contents

Abbreviations

ISS	Information Security System
IS	Information Security
RE	Requirements Engineering
SWOT	Strengths, Weaknesses, Opportunities, Threats
FFA	Force Field Analysis
ISA	Information Security Awareness
SEA	Social Engineering Attack
ROI	Return on Investment
ROISI	Return on Information Security Investment
SI	Security Incident
NPV	Net Present Value
IRR	Internal Rate of Return
KSPIs	Key Security Performance Indicators
RIDIM	Risk-Driven Investment Model
BIA	Business Impact Analysis
OAV	Objective Absolute Values
BCA	Cost-Benefit Analysis
AICCA	Availability, Integrity, Confidentiality, Accountability, Auditability
BCP	Business Continuity Plan
DRP	Disaster Recovery Plan
BID	Business Intelligence Dashboard
IRT	Incident Response Team
RAT	Remote Access Trojan
IDS	Intrusion Detection System
BASE	Basic Analysis and Security Engine

LIST OF PUBLICATIONS

1. Alavi, R., Islam, S., Jahankhani, H. & Al-Nemrat, A. 2013. Analyzing Human Factors for an Effective Information Security Management System. International Journal of Secure Software Engineering (IJSSE), 4**,** 50-74.

2. Online: Weblog publication: Human Factors in ISMS: Goal Driven Risk Management. October 2013. http://www.tripwire.com/state-of-security/security-data-protection/2-human-factors-isms-background-knowledge/

3. Online: Weblog publication: Analyzing Human Factors for an Effective Information Security Management System. October 2013. http://www.tripwire.com/state-of-security/security-data-protection/human-factors-effective-information-security-management-systems/

4. Alavi, R., Islam, S. and Mouratidis, H., 2014, June. A Conceptual Framework to Analyze Human Factors of Information Security Management System (ISMS) in Organizations. In HCI (24) (pp. 297-305).

5. Alavi, R., Islam, S. and Mouratidis, H., 2015. Human Factors of Social Engineering Attacks (SEAs) in Hybrid Cloud Environment: Threats and Risks. In Global Security, Safety and Sustainability: Tomorrow's Challenges of Cyber Security (pp. 50-56). Springer International Publishing.

6. Alavi, R., Islam, S. and Mouratidis, H., 2015. Managing Social Engineering Attacks- Considering Human Factors and Security Investment. Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015). Plymouth, University of Plymouth.

7. Reza Alavi , Shareeful Islam , Haralambos Mouratidis , (2016) "An information security risk-driven investment model for analysing human factors", Information & Computer Security, Vol. 24 Iss: 2, pp.205 – 227

8. Agile Changes of Security Landscape: A Human Factors and Security Investment View. International Symposium on Human Aspects of Information Security & Assurance (HAISA 2016). pp112-124. https://www.cscan.org/default.asp?page=openaccess&eid=17&id=303.

9. Online: Weblog publication: Identifying Cyber Risks: The Important Role of Senior Management. August 2016. http://www.tripwire.com/state-of-security/risk-based-security-for-executives/risk-management/identifying-cyber-risks-the-important-role-of-senior-management/.

CHAPTER 1

Introduction

Contents

1.1. Overview

It is quite unusual to admit that nowadays organisations get along without having an astute and decisive information system. Information systems support organisations to achieve strategic competitive advantages over other organisations and assist senior management in the decision-making process. In addition, they help organisations in timely implementation of projects and effective risk management. A reliable and coherent information system requires a solid security framework that ensures Confidentiality, Integrity, Availability, Authenticity and Auditability of the critical information assets; therefore, managing security is essential for organisations doing business in a globally networked and competitive environment whilst seeking to achieve their objectives and goals and ensuring the continuity of business. Information Security Systems exist to setup a solid security framework and regulate the systematic way in which information technology can use relevant resources. They address all issues that relate to the initiation, implementation, maintenance and evaluation of a secure information system [1]. There have been several studies in the domain of human factors and information management systems, though very little research has addressed the role of main human factors in the ISS context and lifecycle or considered risks and security investment.

Inadequate implementation of security seriously impacts upon organisations' productivity and reputation [2] [3]. According to the Technical Report of Information Security Breaches (2015) by the UK Department for Business, Information & Skills, large organisations have faced a 75% increase in security incidents related to human factors [4]. Even using the latest security techniques and protocols, most systems still frequently encounter security breaches. Technological solutions dealing with issues arising from information security are very similar globally, including anti-virus software, firewalls and intrusion detection systems [5].

Numerous technical advancements do not always produce a more secure environment [6] because security breaches do not always originate with technical problems; rather, they also depend on the humans who use the systems and behave within the system environment; therefore, human factors perform an important role in information security systems. The role of people has not only been highlighted by numerous academic studies but also by IS professionals and various IS regulations and standards. For example, a section of ISO27001, the main security standard, describes the role of people, including the importance of responsible management, commitment, training, awareness and competence and skills [7]. The main question is why all manner of regulations, standards and technical competencies have not addressed the issues related to human factors. An understanding of human factors requires the development of an effective information security management system.

This research intends to analyse main characteristics of human factors within the context of ISSs in organisations and address them within a unique risk-driven investment model. The uniqueness of this model derives from the organisational benefits gained by linking the risks due to incidental and human factors with the investment to ensure the economical allocation to address the most pressing risks factors. This approach is uniquely proposed for the consideration of human factors, risk and concerns of investment.

1.2. Research Motivation and Novelty

For many years, the study of human factors, a term that is used in this research prevalently, has been evolving as a unique and independent discipline. It focuses on the nature and characteristics of human interactions, viewed from the unified perspective of the science, engineering, design, technology and management of human compatible systems. It includes a variety of natural and artificial products, processes and living environments [8]; therefore, both human factors and the relationship between those factors and technology, information security systems in particular, are not a new phenomenon. Many studies on human factors and computer science, technology, information systems and information security have been published, though no research has been done to specifically address the role of human factors in ISSs in an organisational context, considering their unique specifications [9] [1]. The advancement of the implementation of Information Security System (ISS) procedures in organisations has not provided effective security. Inadequate ISSs seriously impact upon organisations' productivity and reputation [2] [3] [10]. It is also argued that there is no universal, top-model framework to fulfil ISS goals [11]. However, the real challenges are from non-technical issues such as human and organisational factors, which need more attention to ensure the effectiveness of an ISS. Effectively and progressively, information systems are shifting from the technical realm to a socio-technical ecosystem, where human factors play a more important role. Deloitte, in its 2006 global security report, argues that many security breaches are the result of human errors or negligence because of weak

operational practices [12]. It is also highlighted that human factors present the greatest single issue of concern in ISSs [13]; thus, there is a need for an adequate model and a comprehensive understanding of human factors and their impact on the effective implementation of information security systems. This task is challenging, because the domain is highly subjective by nature and it is difficult to quantify all the human factors into a measuring scale. For instance, it would be extremely difficult to judge and evaluate people's attitudes towards information security. Consequently, the motivation of this research lies with the lack of adequate and appropriate models and methodologies in the current literature to support the analysis and reasoning of main characteristics of human factors within the context of ISSs in organisations, considering risks and security investment.

The contribution of this research is a novel risk-driven investment model to support the analysis of human factors in the ISS development process. The model utilises concepts from goal-oriented requirements engineering, conceptual modelling, Secure Tropos language modelling and organisational context. The focus of the model is on non-technical elements that include direct and indirect human factors. Literature has illustrated that requirements engineering approaches are appropriate for the analysis and reasoning of non-technical issues related to information systems and therefore are appropriate for an analysis of human factors related to security. The researcher believes that having considered all available and current methodologies presented in the literature to support such an analysis effectively and sufficiently, this research has adopted the right approach and techniques.

1.3. Problem Domain

Information Security falls back on a range of different disciplines: computer science, communication technology, criminology, law, business, mathematics, amongst others; therefore, like most things in life, success in all of these areas is achieved through understanding and managing the human factors.

What is meant by ***"human factor"***?

Human factor refers to the environmental, organisational, job factors and human and individual characteristics that influence human behaviour. However, it is widely defined as referring to the science of ergonomic design [14]. Ergonomics (or human factors) is the scientific field interested with the understanding of interactions amongst individuals and other elements of a system, and the declaration that applies theory, principles and methods to design in order to optimise human wellbeing and performance and general system functions.

In information security, the human factors context defines the impact of people and the unforeseeable forces that cause many of best planned

technological systems to collapse. This can be as a result of carelessness, stress, apathy, error, lack of sufficient communication or inadequate support of management. In addition, human factors hinder information systems' capabilities for securing information assets. Technology is key to security, increasingly so as businesses learn how to apply its influence to handle growing business and security needs. However, technology is designed, implemented, operated and evaluated by people and, therefore, human factors greatly determine whether information systems are used or misused. As we evolve from a predominantly process-driven business model to a more cursive and coherent information-driven model, the impact of human factors has become greater. Information security incidents are rising despite the use of technological advancements and the provision of training and awareness programs for users [12] [15]. Persistent security incidents indicate a lack of understanding of some of the issues concerning information security. Much existing research investigating these concerns exists, yet information security incidents are increasing [16]. Organisations seem attached to a general mind-set that technical aspects of information security have greater impacts on successful projects than non-technical factors. This is in spite of abundant research identifying non-technical factors as the main cause of information security incidents [17] [18]. Information security scholars have identified many non-technical factors, such as human factors, as responsible for security breaches and incidents [3] [17] [18] [19] [20]. Although current practices in ISSs have received approval from governments, corporations, standard bodies and regulators, the human factor domain still lacks maturity. Most studies have, however, concentrated on information systems rather than ISS. Although human factors are identified as key parameters in a successful ISS, a detailed analysis is required for an understanding of their impact.

Human factors and influence create great challenges for information security systems. Because of human nature, people often make inconsistent, subjective and myopic decisions and assessments that pose a great risk to information assets. All kinds of human factors can deeply affect the way information security is managed. Though human factors need to be analysed and measured, their high subjectivity makes this extremely difficult; therefore, a detailed analysis of the main human factors and their unique specifications and requirements in ISSs is a critical concern. This research thus intends to analyse the main human factors involved in an ISS from an organisational perspective to provide a model to address risk and security investment. Information security incidents due to human factors have been shown to be a major issue within the ISS domain, hindering the business management agenda, and they will remain there until the consequences of human failure are addressed. This major issue in the domain of ISSs will become increasingly important with the ever growing social networking, use of mobile devices and cloud computing, with its potential for even greater security breaches, and ultimately cause more risk and damage to organisations [21]. An adequate model to address this concern will be presented in this research.

1.4. Research Contributions

This research contributes to current knowledge of information security by demonstrating the importance and critical role of human factors in the development of information security system processes. The main contribution will be the advancement of the theoretical and practical basis for ISSs in proposing an objective framework for developing, assessing and modelling a risk-investment security approach. Furthermore, it improves understanding of risk-investment constructs in the security incident stages in relation to maximising return on security investments. This research examines the role of human factors in ISS processes on the basis of risk and investment. The findings will emphasise the importance of human factors in today's information security context and provide guidance on addressing risk to and return on security investments. This could perhaps serve to improve the financial performance and competitiveness of organisations and increase the effectiveness of their security policies and guidelines. It is expected that the outcomes of this research will have a positive impact on the ISS guidelines in organisations and therefore increase the effectiveness of security systems' design and implementation. The outcomes of the research can be applicable in all organisations and assist in the decision-making process by providing new control measures in regard to security investment.

It is expected that the main outcome of the study, the Information Security Risk-Driven Investment Model (RIDIM), will be used by organisations to:

- help them better articulate security policy processes, considering critical human factors and the consequences of their risks
- provide adequate and appropriate training and awareness programs to address risks related to critical human factors
- calculate the ROISI to obtain accurate risk identification and therefore an adequate investment for the introduction of new controls and mitigation processes.

The specific benefit to organisations will be a bespoke formulation of the RIDIM Security Investment and Risk-based Model and risk-investment metrics.

1.5. Research Questions

The main research goal is to develop a risk-driven security investment model to support the analysis and reasoning of the main characteristics of human factors within the context of ISSs in organisations. With this goal in mind, the thesis attempts to address the following questions:

1) ***What are the main characteristics of human factors within the ISS context?***

2) ***How can we provide an analysis and reasoning of human factors, risks and security investment in the development process of an ISS?***

3) ***How can a Security Risk-Driven Model support the analysis of the effect of human factors in the ISS development process?***

This research uses a number of theories and methods to achieve the research objectives and evaluates their applicability.

1.6. Research Objectives

The main objective of this research is to address critical human factors in ISS projects and their relation to risk and investment issues in such projects. The following goals are thus proposed to achieve the main objective:

1. To evaluate and identify the main direct and indirect human factors in ISSs.
2. To prioritise critical human factors.
3. To determine the relationship between critical human factors, risk and security investment.
4. To develop a model of risk-investment, considering critical human factors, risks and security investment, for use in the development of ISSs.

1.7. Research Methodology

Both a positivistic and interpretivist research philosophy shapes the overall research design of the mixed methods approach. A detailed qualitative of the research objectives are presented that are formed by an interpretivist view. However, the research lies predominantly in the positivistic field, where the empirical data converged and therefore both qualitative and quantitative methods were used. The semi-structured interviews, structured questionnaire, detailed interviews and Delphi expert panel and use of real life security incidents were used as case studies to ensure the reliability and validity of the results. The research methodology also used a literature review, identification of suitable methods and case study approach.

1.8. Research Outlines

The first chapter delivers the inspiration for and the novelty of this research by outlining the research domain, problem relevance and research contribution. Following Chapter 1, the thesis is categorised into the following chapters:

Chapter 2: Related Work and Related Theories: A review of the literature, related work, relevant theories and current status of security practices related to ISSs in organisations is presented. The chapter begins

by outlining the basics of information security attributes. It then continues by reviewing existing practices and current research into the role of human factors in ISSs. The chapter the defines and reviews Social Engineering Attacks (SEAs), the main source of incidents related to human factors. It then defines Information Security Risks and Return On Information Security Investment (ROISI). A definition of Information Security Dashboard, which provides a method by which businesses can address information security issues and concepts, is provided. It the continues with the relevant theories and methods, including Socio-technical theory, SWOT, Delphi Expert Panel and Force Field methodologies, as well as Requirements Engineering (RE) and Secure-Tropos methodology. The researcher performed a literature review to understand human factors and their impact on information security management systems [22]. The literature search process focused on the studies that considered human-related issues and linked them with information security, focusing on an organisational context. In particular, the human factors that directly and indirectly impact an organisation were emphasised. The research identifies relevant literature from major research databases such as IEEE Xplore, SpringerLink, ScienceDirect, Elesevier, ACM Digital Library and Google scholar. The study considered only peer reviewed papers and counted the citations of individual papers to assess their quality. The extracted data were combined and analysed based on a security incident. Finally, the chapter summarises the existing state of the art of ISSs and outlines the main thesis contribution by revisiting research questions.

Chapter 3: Research Methodology: The research methodology and research methodology process is outlined. The research used a mixed method, combining both quantitative and qualitative techniques. It was constructed on unstructured but detailed interviews and a structured survey study, using Delphi expert panel method. The methodology of the research comprises four stages: Investigation, Prioritisation, Gap Analysis, and Control and Evaluation (IPGACE). This is followed by an outline of the research goals and a discussion.

Chapter 4: Overview of Human Factors: Critical human factors are identified using the research methodology techniques introduced in Chapter 3. Consequently, this chapter uses current literature, unstructured interviews, SWOT analysis and a survey study to identify main human factors, which it then characterises into two main categories; direct and indirect human factors. The direct human factors are exactly related to people and their characters and feelings. The indirect factors take into account the organisational contexts and forces that affect people. Two real incidents were used as case studies to analyse and prioritise these factors.

Chapter 5: Risk-Driven Investment Model (RIDIM): The Risk-Driven Investment Model (RIDIM) is introduced, the main

contribution of this research. The first part of the chapter offers a detailed explanation of the basic concepts of the model, considering the actors, goals, risks, security incidents, vulnerabilities, security investment, plan and protect mechanism and configuration of the meta-model. Then it outlines the process model in a real world scenario in three activities and tasks associated in RIDIM. The chapter continues to incorporate the outcome of the activities with the outcome of ROISI to integrate the principles of RIDIM into requirements engineering at an abstract level.

Chapter 6: Evaluations: The proposed security investment and risk-based model is evaluated. The research considers SEAs as security incidents and describes how RIDIM can assist in controlling such incidents. The case study implements RIDIM in a real world example and takes into account the security budget of a large organisation. Finally, the chapter concludes by suggesting adequate budget requirements for a protection mechanism against SEAs.

Chapter 7: Conclusions and Discussions: Conclusions on the overall thesis contribution are presented. The research results are summarised. In addition, this section includes a discussion of the limitations of the RIDIM as well as some suggestions for the direction of future work.

CHAPTER 2

Related Works and Relevant Theories

Contents

2.1 Introduction

This chapter offers background information and reviews related works which are relevant for this research. It introduces the concepts of information security, human factors, business and organisational oriented issues such as the information security dashboard and return on investment, which is one concept used for modelling human factors. This chapter also discusses the theories and existing state-of-the-art works around Requirements Engineering (RE), Socio-technical theory, SWOT analysis methodology, Force Field Analysis (FFA), the Delphi Expert Panel Survey method and Social Engineering Attacks (SEAs), all relevant for this research as shown in Figure 2.1. A literature review is a method of identifying, interpreting and evaluating all available research sources relevant for a specific research question or topic area [23] [24]. We follow a list of keywords, including *Information Security, Information Security Management System, Human Factors, Return of Security Investment, Risks and Requirements Engineering* for this review through widely familiar database sources such as *ACM, IEEEXplore, and Google Scholar.*

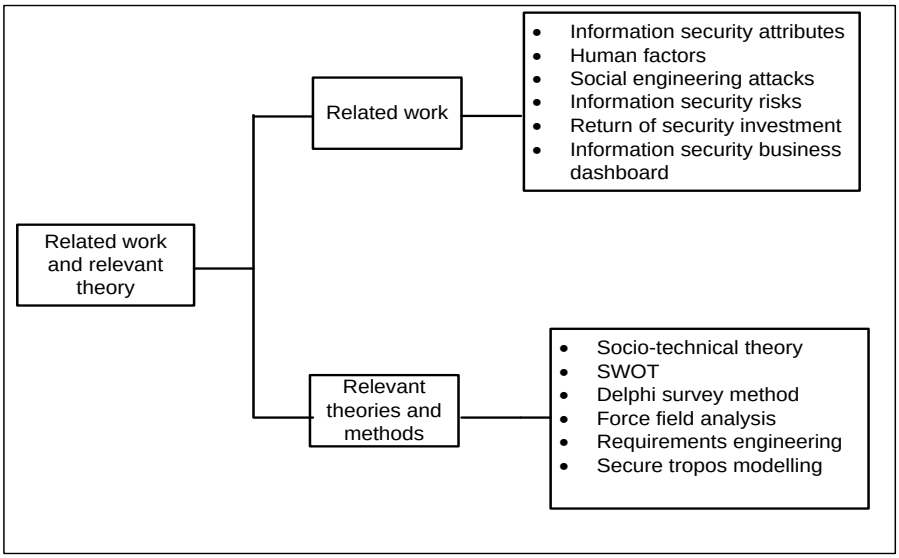


Figure 2.1 Overview of related works and relevant theories

2.2 Basics about Information Security Attributes

Information security attributes provide a foundation for information security and are designed for modelling policies within this field [25]. They are: Availability, Integrity, Confidentiality, Accountability, and Auditability (AICAA). Although they are considered essential to information security systems, they are in fact largely dependent on the specific requirements of the organisation's security goals in the context of the business's nature and certain threats to particular information assets. An overview of these attributes is given below.

2.2.1 Availability

Availability refers to the timely and uninterrupted access to information systems and services given to authorised actors. Availability in a security mechanism provides extensive assurance of the accessibility of resources and data to authorised users. For example, availability offers effective and constant access to data in the case of Distribution Denial-of-Service (DDoS) attacks. In addition, availability entails supporting infrastructure such as network services and access control mechanisms, which enables authorised users to acquire authorised access [26]. Having a control mechanism established maintains availability, safeguarding authorised access and ensuring an adequate level of performance and conformity to deal with unforeseen interruptions and deliver redundancy, prevent data destruction and loss and maintain a reliable backup. Threats to availability include failure and errors in software and electrical equipment, spillages of chemicals and liquids as well as natural factors such as high temperature, air system faults, flooding and so on. Some forms of attack focus on disrupting availability, including DDoS attacks, data destruction and communication interruptions. Human factors present another threat to availability such as through the unauthorised alteration of sensitive information as a result of error, oversight, tiredness, incompetency, stress and so on. Availability

breaches can arise because of the actions of users, an inaccuracy in security policy or an incorrect implementation of security control.

2.2.2 Integrity

Integrity is the second principle of the AICAA. Upholding integrity, entities must preserve their authenticity and be intentionally modified only by authorised subjects. Security mechanisms provide integrity by offering strong assurance that all resources and data are unaltered from their original form whilst they are stored, transferred or processed. This ensures that information systems and their components are not compromised and their integrity maintained [27]. The following actions are required to achieve integrity; authorised modifications, the consistency of internal and external data to ensure its correctness and validation in a verifiable manner and in an interoperable format. Viruses, SEAs, APTs, phishing, logic bombs, unauthorised access, errors in coding and applications, malicious modification, intentional replacement and system back doors are just some examples of the many types of breach that can violate integrity. As with confidentiality, integrity incidents are not limited to deliberate attacks. Many instances of unauthorised alteration of sensitive information are because of human factors such as error, lack of communication, inadequate training, oversight, ineptitude and stress. Several countermeasures can safeguard integrity against possible threats. These include strict access control, rigorous authentication procedures such as multi-authentication methods, intrusion detection systems, encryption, hash total verifications, interface restrictions and extensive and adequate awareness training. Integrity is reliant on confidentiality and without confidentiality integrity cannot be preserved.

2.2.3 Confidentiality

The third component of AICAA is confidentiality. Security mechanisms offer confidentiality to both soft and hard assets and provide them with a high level of assurance, because such mechanisms are limited to authorised access. Unapproved disclosure of assets might occur under presence of threats to violate the confidentiality rule [28]. Data must be protected from unauthorised access, use or disclosure in storage, during processing and in transit in order for confidentiality to be maintained. For this purpose, a detailed and distinctive security mechanism is required for each single official set of data resources. Attacks such as capturing network traffic, stealing password files, port scanning, shoulder surfing, eavesdropping and sniffing are used to violate confidentiality, though SEA incidents are the most common and successful types of attacks. SEAs, discussed later, take advantage of human weakness and ineptitude to breach confidentiality. Incidents that lead to confidentiality breaches can also be due to inadequate encryption of a transmission, failing to fully authenticate a remote system before relocating data, leaving access points unsecured and accessing malicious code that opens a back door. These violations of confidentiality can stem from actions of an end user or a system administrator, inaccuracy in a security policy or a misconfigured security control. Encryption, strict

access control, thorough authentication processes, data classification, extensive training and awareness programs and network traffic padding can be used as countermeasures to safeguard confidentiality against possible threats. It is important to mention that without integrity, confidentiality cannot be upheld as they depend on each other extensively. Sensitivity, discretion, criticality, disguise, secrecy, privacy, solitude and isolation are other perceptions, conditions and characteristics of confidentiality. However, as organisations must act pragmatically towards security and assurance, the preservation of confidentiality must adhere to business requirements, need, goals and objectives. Confidentiality should enable the achievement of business objectives. Confidentiality itself is not the objective.

2.2.4 Accountability

Accountability is an indispensable part of information security. Accountability requires that each individual working with an information system have precise responsibilities for information assurance. In practice, the person who is in charge of information assurance is responsible for the overall information security plan and the measurement of it. Prohibiting employees from installing unauthorised software on an information system owned by an organisation would be an example of this. Each individual must be held responsible for the information assets that they own. The practice will improve overall security and trustworthiness in organisations. In order for accountability to be measured, there must be a process in which the accountability properties in various stakeholders and entities are defined whilst clear metrics are introduced by the Chief Information Security Officer (CISO). The ISO27001 standards state that clear rules for information security, involving a process for assigning and accepting accountability for the appropriate safeguarding of information assets, must be adhered to [1]. This provides an ability to hold individuals, entities and stakeholders responsible for their actions in user transactions and for their use of information.

2.2.5 Auditability

Auditability is a crucial part of information security and assurance. Various level of controls and auditability in organisations are required to deal with the concerns of regulation and compliance [29]. In information security, compliance and regulatory requirements are complex and enable greater security control and auditability. Data security's characteristic attribute is that it guarantees the completeness, accuracy and consistency of information. The data auditability goal requires the authentication of information for reporting and adequate evidence. The trustability of information systems works alongside the auditability of such systems, concerning various stakeholders in enterprise security systems that include human factors. As information systems' activities move ever closure to cloud computing, cloud virtualisation management becomes even more critical for organisations. Consequently, attestation and clarification have

become integral components in the security management of virtualisation and cloud-based information systems. As a result, it is crucial that auditability, which relies heavily relies on attestation and clarification, is followed. The following concepts, which are part of the business domain, are discussed in order to understand the risk-driven investment model.

2.3 Human factors

Conventional patterns of how ISSs are run are rapidly evolving. Evolving computing technology provides many benefits, such as accessibility and the availability of resources for organisations [1]. But the economic advantage and cost impacts are far more attractive to organisations than anything else. This convenience and attractiveness, however, comes with new security challenges and risks that require investment to be managed and mitigated. Human factors further complicate these challenges and the way they are addressed. Social Engineering Attacks (SEAs) are very commonly used by attackers to access classified data. Human factors in information security certainly are an important concern for an organisation's critical business operations. Therefore, it is imperative for organisations to address all concerns, including risks and investment in security. Information Security Systems can be used to address issues related to the establishment, evaluation and maintenance of a secure information system. Inadequate implementation of security causes serious impacts on organisations' productivity and reputation [18]. According to the Verizon Report of Data Breach Investigation Report (2016), human factors are responsible for most successful attacks. Even using the latest security techniques and protocols, most information systems still face numerous security breaches; therefore, conventional and solely technical approaches cannot address this very pressing issue.

Human factors can prove difficult to contain whilst interrelating and working in an IT environment and must be considered to protect the security of such an environment [32]. Human factors have various dimensions which are uniquely intertwined with organisational culture and individual perceptions and characteristics. Consequently, providing a global solution to information security is a big challenge in the organisational context; therefore, this research recognises human factors, which directly and indirectly affect information security, as one of the major components responsible for inadequate information security and risk to organisational assets. As human factors are at the heart of the vast majority of security breaches, resulting from issues such as error, inadequate skills or apathy, a consistent effort is required to address them. This research aims to provide a model to address such issues.

2.4 Social Engineering Attacks

A Social Engineering Attack (SEA) is the act of manipulating a person to take an action that may or may not be in the target's best interest, with the

perpetrator obtaining information, gaining access or getting the target to take a certain action [36]. Responding to the threats of SEAs using technological resources and tools would not be enough to deal with the associated risks because people are at the centre of such attacks and they play a vital role in it. Organisations may use various tools to detect and minimise attacks. For example, they may use the Basic Analysis and Security Engine, known as BASE, which is a PHP-based analysis mechanism, in order to examine and process a database of security events generated by different Intrusion Detection Systems (IDSs), firewalls and network monitoring instruments. It is quite powerful and contains features such as a query-builder and search interface for alerting the user when certain patterns are detected, a packet decoder and charts and statistics based on time, sensor, signature, protocol, IP address, and others. BASE, however, has difficulty preventing and responding to human actions and behaviour in socially engineered incidences. This is because SEAs result mainly in the exploitation of human factors, and people are at the centre of such incidents. There are specific factors, identified in a previous study, that play important roles in such attacks [18]. These include a lack of awareness, inadequate communication skills, a lack of supervision and insufficient involvement of management.

2.4.1 Reasons behind Social Engineering Attacks

Human factors remain essential to any SEAs because no matter how many training programs or control mechanisms are deployed, people are the weakest link in a security system [37]. SEAs can cause a great deal of disruption to everyday business activities and create financial, social and technical mayhem, the impacts of which can extend beyond geographical borders and organisational boundaries; therefore, dealing with SEAs would be in the best interest of any organisation. According to the Verizon Enterprise Solutions report [38], human factors are the main sources of SEAs, confirmed by a number of academic sources [8] [39]. People can be easily socially engineered, which leads to the compromise of information systems in organisations. Even when attackers use complex and sophisticated technical hacking methods, they invariably use people as a main tool in delivering their malicious software. For example, they use e-mail attachments, which can easily mislead people and deliver the payload of a malicious program, in order to gain access to a system. This type of attack is just one example out of hundreds and has been successful with big organisations and central governments. Janczewski and Fu identified five main causes of SEAs: people, lack of security awareness, psychological weaknesses, technology and defence and attack methods [40].

2.4.2 Social Engineering Attack Taxonomy

Providing a strong security posture is crucial for business continuity. With the current major threats of cyber-attacks and virtual terrorism, security must be given adequate consideration. If it is not, everyday organisational activities will be grounded with real possibilities of loss, punitive financial fines and damaged reputations. SEAs undermine organisations' efforts to

deal with security in an effective way. There are several malicious practices such as the Advanced Persistent Attack that create security breaches in organisations [41]. Janczewski and Fu (2010) further categorised SEAs into "Human-Based" and "Technology-Based" attacks [40]. The role of people and certain human factors contribute greatly to SEAs. The attackers crack the security of an information system by exploiting human weaknesses. SEAs increase the risk of incurring financial loss, legal fees and reputational loss for organisations. SEAs pose a challenging task for organisations to deal with because they are human-oriented activities and human factors are difficult to deal with. There is a clear link between the main human factors and SEAs (Figure 2.2).

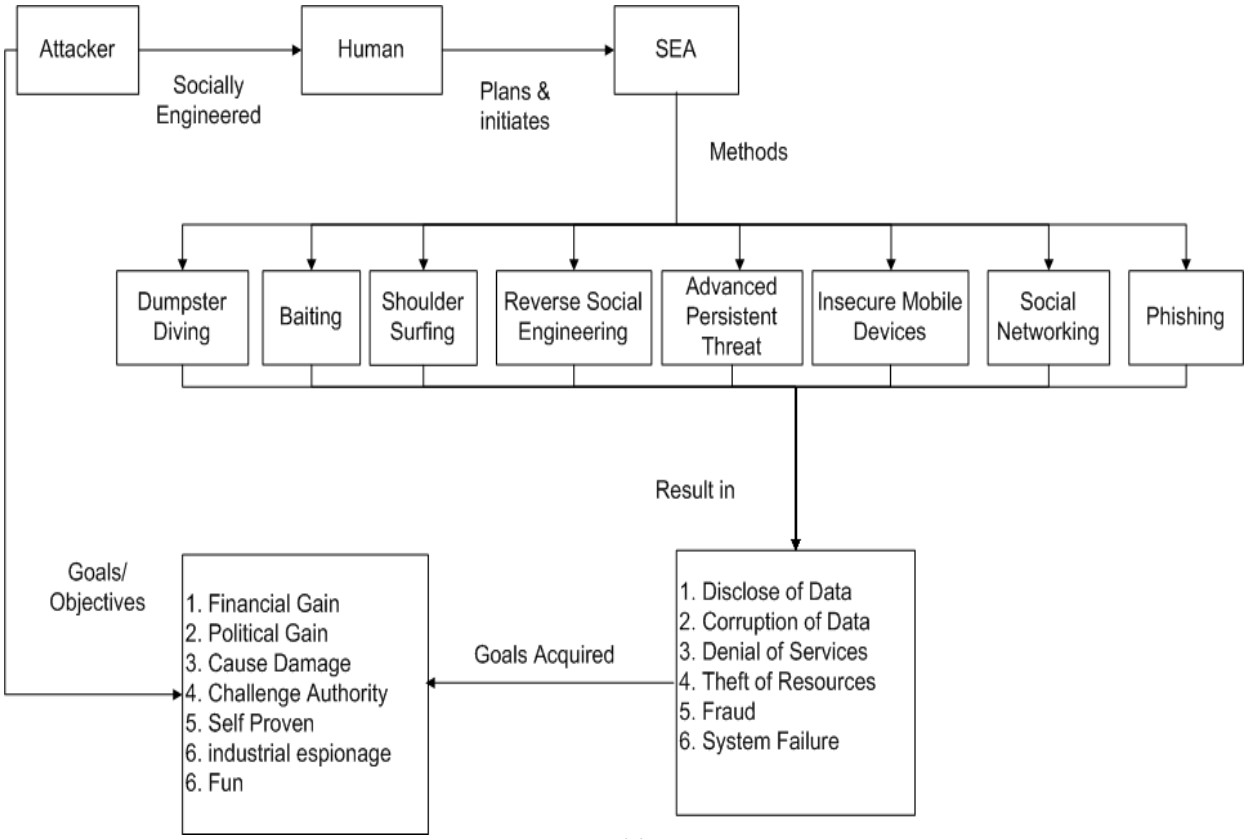


Figure 2.2: Social Engineering Attack Taxonomy

Figure 2.2 depicts the taxonomy of SEAs, in which an attacker socially engineers people inside an organisation with adequate and effective planning and chooses a malicious attack type that suits the person and the organisation. The figure shows various SEA techniques, each impacting in various ways upon organisations, such as through disclosure or corruption of data. This fulfils the attacker's goals and objectives, which range from financial gain to challenging authority.

There have been a number of works that focus on analysing SEA attacks. Janczewski & Fu (2010) provided a conceptual model in order to understand the impact of SEAs on individuals and businesses and present a defensive approach to mitigate these risks [40]. The study focused on IT

departments and took a more abstract view of SEAs without considering concepts related to critical human factors and their relationships with security investment. Greitzer et al. (2014) looked at the insider threat that derives from SEAs [42]. The study considered some related human factors but concentrated mainly on unintentional insider threats whilst observing psychological and social characteristics of people. Karpati et al. (2012) used a comparison study between Mal-Activity diagram and Misuse Cases and presented two modelling techniques [43]. This study attempted to provide a conceptual comparison in order to determine the advantages and efficiency of each approach. Although the work concentrated on SEAs and provided a concrete discussion on the validity of the study, it did not embrace security investment and actors such as humans and security systems. Each approach has its unique advantages and efficiencies. Whilst Misuse Cases are used mainly for threat modelling and security requirements elicitation, the Mal-Activity diagrams can be used to complement Misuse Cases which includes adverse events together with authentic and rightful activities in the ISSs. Some other studies concentrate on specific attacks such as phishing, Jagatic [44] or advanced persistent attacks [45].

All the aforementioned works contribute towards investigating SEA-related security incidents. However, none of these works explicitly focus on critical human factors, which are one of the main reasons for SEAs. In particular, SEAs require a systematic approach to analyse the complex human factors and address any issues relating to them. Security markets are saturated with technical solutions promising much in the way of security efficiency whilst brushing aside human elements, despite overwhelming evidence to the contrary; therefore, it is important to analyse human factors whilst considering security investment so that an organisation can make the right decision on its information security.

2.5 Information Security Risks

Information security risk refers to an element or effect that has a potentially damaging consequence on the availability, integrity, confidentiality, accountability and auditability (AICAA) of a critical organisation asset. Generally, risk is defined as combination of the probability of an event and the severity of its consequence. The event can be certain or uncertain and can be influenced by a single occurrence or a series of occurrences. Security risk management is a process that integrates methods and artefacts for identifying, analysing, controlling and continuously monitoring risks in order protect the asset from any potential vulnerabilities and threats. Risk management is considered an integral part of all organisational processes, including strategic planning and all project and change management processes. It does not only support security experts in the handling of security vulnerabilities, but it also provides a framework that allows for an evaluation of the return on a security investment. There are standards such as ISO 31000:2009 that provide a process, framework and a number of principles for effective risk management practice [46].

There are several works in the literature that emphasise early risk management practice in information system development. For instance, the Information System Security Risk Management (ISSRM) reference model includes three different concepts relating to the assessment and management of risk [47]. Asset-related concepts describe what assets are important to protect and what criteria guarantee asset security. Risk-related concepts present how the risk itself is defined and what major principles should be taken into account when defining the possible risks. Risk treatment-related concepts describe what decisions, requirements and controls should be defined and implemented in order to mitigate possible risks. ISSRM integrates with the misuse case model in [47] to enhance the analysis of security risks using both textual and graphical presentation. Another technique is OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation), which is a free methodology developed by the Carnegie Mellon University SEI (Software Engineering Institute) [132] and is used and implemented by some organisations. Organisations aim to create an information security risk mitigation plan that is strategically bound to organisation-wide risk treatment. This is in line with the recommendations of Phase 3 of the OCTAVE process, "Developing Security Strategy", which recommends employing a common evaluation basis. OCTAVE risk assessment techniques seek to establish a defence strategy for the critical assets of the entire auditee organisation without consideration of critical human factors and cost; therefore, the OCTAVE process, specifically Phase 2, "Identify Infrastructure Vulnerabilities", does not perform any further than automated vulnerability scanning with no consideration of risk, human factors and investment.

Considering the research objectives with regard to critical human factors and the return of the investment in security, the analysis of security risks should embrace these two factors. This is important because from a financial perspective information security is related to reducing loss, rather than generating profit. However, the loss related to the intangible assets, and critical human factors are difficult to quantify. Therefore, information security risk assessments are a practical way of improving information security whilst evaluating likelihoods and potential impacts of all security incidents, whether they are active or passive. Human and organisational factors have always formed the position of information security risk assessment activities.

There are a number of international standards related to IS and its concepts, but two in particular are highly relevant to this research. Table 2.1 provides a comparison between concepts used in this research and two main related international standards, ISO31000 and ISO27001.

Concepts	ISO31000	ISO27001	Thesis
Human Factors	✓	✓	✓
Risk	✓	✓	✓
Investment	✖	✖	✓
Cost-Benefit	✓	✖	✓
Main Human Factors	**Partly**	**Partly**	✓
Critical Human Factors	✖	✖	✓
Security Incidents	**Partly**	**Partly**	✓

Table 2.1: Comparison between concepts in standards in this thesis

2.6 Return on Information Security Investment (ROISI)

The process of securing information has become more critical than ever. When security is mission-critical and tied to revenue chains and compliance, then it has significant bottom-line impact. Security cannot tolerate any performance delays in protection mechanisms and requires extra attention to ensure its success and at the lowest possible cost. Cost and urgency in organisations' procurement processes thus become a priority, especially dealing with security requirements. Nevertheless, the way security is designed and implemented varies from one organisation to another and depends upon the nature of the business, organisational culture and how the business risk management approach is adopted. Understanding the value of information assets is a principle challenge in organisational contexts. The value of an information asset is a measure of the extent to which it drives business value. Considering risk assessment objectively, there are four ways to address risks to information assets in an organisation; risk can be accepted, managed, transferred or avoided. Losing a customer database would be an organisational catastrophe, which inspires consideration of risk management and investment in security. The value placed on information can be understood and be seen to be based upon several perspectives, including revenue generation, risk and privacy.

Providing an appropriate evaluation of different security solutions and assessing costs and benefits of technological tools without having tangible data is thus a concern for organisations. The benefits of different information security solutions vary, depending on the possibility of attack. Risk evaluation and analysis deals with the likelihood of an attack occurring and the efficacy of a given security solution in mitigating the damage caused by the attack. Most researchers have concentrated on the success of security systems without consideration of the cost, which impacts upon the overall Return on Information Security Investment (ROISI). However, both the security concepts within ISS processes and the cost concepts in the ROISI process have the same goal: the protection of information assets to prevent extra cost as a result of financial and reputational loss. Adopting a combined framework would enable us to address both security and investment concepts. This work is novel in that it combines concepts from

security, risk and investment fields to provide evidence for the optimal defence mechanism against threats from security incidents and their resultant risks and to assist in the calculation of the return on security investments, considering human factors. Available tools and methods allow organisations to calculate and analyse the financial impact of a specific security control, which cannot be used to analyse the cost-benefits of other factors such as human factors. Information security management systems are now increasingly based on economic principles such as cost-benefit analysis [48]. This is part of the 'information security financial metrics approach' that has been developed mainly in the last 10 years or so. Balancing information security costs and benefits is essential for organisations. However, organisations will invest in information security to a greater extent if the cost of investment is less than the cost of potential risk [49]. There are important variables in this measurement that are required to be as precise as possible. Accurate information on the likelihood of IS incidents and their impacts must be acquired in order to assist in the quantification of ROISI. It is, however, important to remember that there is a significant difference between quantifying and measuring ROI on ISS and new machinery systems and controls [50].

2.7 Information Security Business Dashboard

Information security management and business decision-making are intimately interconnected with risk management. Executive boards require an understanding and monitoring of the risks that have the potential to obstruct their organisation's ability to achieve its goals. These risks are characterised by Key Risk Indicators (KIRs), which stem directly from the organisation's long-term strategy [25]. The Business Intelligence Dashboard (BID) guides organisations towards a suitable information security posture whilst providing answers to key questions often raised by executives. Providing a meaningful BID for organisations and their senior executives helps them to receive some extended analytical insights on security metrics and Key Security Performance Indicators (KSPIs), a non-technical method that can be grasped by non-technical senior executives. BID offers the following benefits for information security in organisations:

- Improved business decisions through the use of images and graphs.
- Comparative analysis of the strengths and weaknesses of an information security system.
- Clear and easily understood by non-technical senior management viewers, providing different users with different views.
- Enables users to access available information as required.
- Accumulates and analyses data from across the information security and business ecosystem to achieve new insights from dimensions, metrics and business contexts that were previously absent.
- Presents implications of such security metrics.

The above benefits help organisations to more accurately determine the amount of investment required for their information security and, more

importantly, assist them in balancing the actual investment with the return on that investment.

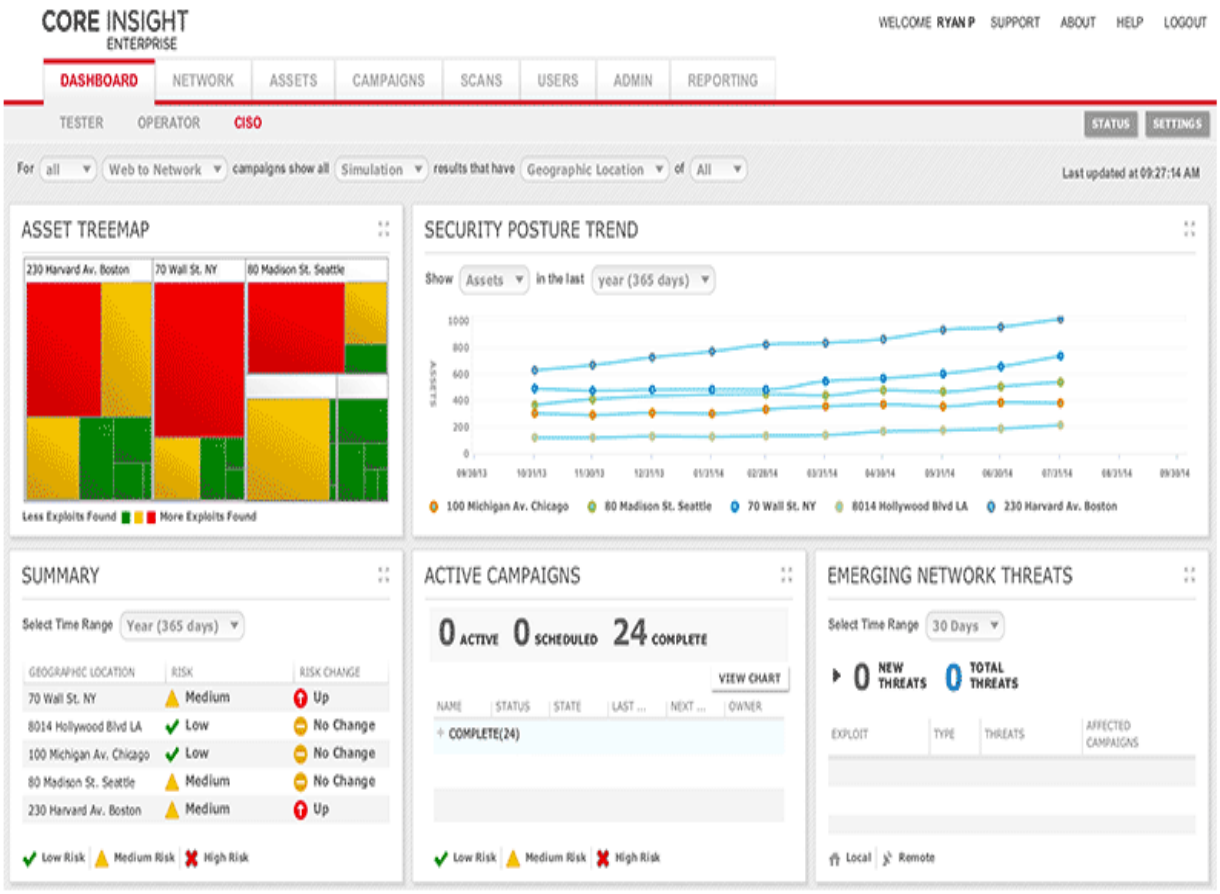


Figure 2.3. BID Sample: http://www.coresecurity.com/core-insight-dashboards

Figure 2.3 illustrates a BID sample within the CoreSecurity. Business Intelligence Dashboard (BID), one of the business domain concepts used in this research to provide some practical and meaningful insights into information security. BIDs are of particular interest in this research as they involve several core concepts of information security that are relevant to measures and metrics for core organisational goals. These areas are:

- Risks
- Security Incidents
- Critical human factors such as awareness
- Threat levels
- Key information security projects such as Cost and ROISI
- Compliance, conformance and performance

BIDs are based upon and defined by the type of security incidents they aim to defend against, although examining BIDs alone does not provide a comprehensive picture of all issues related to SIs, particularly insight into

critical human factors and their relation to risk and investment concepts; although extremely useful, BIDs are thus unable to respond effectively to all SI challenges.

2.8 Relevant Theories and Methods

This section presents the relevant theories and methods that have been used in this research. In particular, socio-technical theory has been employed to deal with human factors and the SWOT, Delphi survey and force field methods to analyse security incidents. This research also draws from requirements engineering concepts to develop a risk-driven investment model that considers human factors.

2.8.1 Socio-Technical Theory

A socio-technical system is founded and defined upon two categories: the technical and the social. Both groups are considered to be equally important to information security [51]. The risk-investment approach towards an ISS is viewed as a socio-technical one because both technological and social considerations are essential to its success. A number of studies have found that organisations experience information security incidents or cyber security risks predominantly due to human factors [52] [53]. These studies have provided various approaches and models, responding to the ever-increasing demand for an understanding of human factors [54]. They have drawn from variety of theories across various fields such as psychology, including occupational psychology [55], sociology, including socio-technical theory [56], and criminology, particularly deterrence theory [57] [58], amongst others. Each has attempted to provide an explanation of the role of human factors in information security risks and incidents. All of these techniques are beneficial to the identification and modelling of human factors, though few have presented a model in which, explaining how people roles resulted from forces behind direct and indirect human factors and how organisations could effectively address the driving and resisting forces to change undesired situation to an ideal situation.

This integration and co-ordination of an ISS has both social and technical views, creating a socio-technical nature in those forces involved [59]. This is a challenge due to the fact that human factors are a subjective matter and require socio-technical systems theory and practice to be dealt with comprehensively. However, it is evident that ISSs comprise a blend of people who work within a technological process [60]. This marriage of people and process is quite similar to that presented by the Tavistock Institute for the British coal mining industry, where new machines were supposed be to run by people who were required to learn new technical skills [61]. This combination of technology and humans is complex and delicate. The complexity arises from the number of systems and skills involved and the delicacy from the dynamic relationship among these systems within the organisation [62]. Many researchers therefore believe that an ISS serves a deep and interdependent socio-technical function [60]

[63] [64], although they have different views on the more influential factors. Denning (1999) believes technological solutions weigh more than social and human elements when it comes to information security, whilst Desman (2002) states that information security is mainly a social matter, not a technological issue [63] [64], despite his acceptance of the presence of technological deterrents and solutions. Having examined much of the research carried out in the field of information security, it can be concluded that the social and technical factors must work synergistically to fulfil security objectives. The key concern is how to design, implement and evaluate an ISS that works well for all stakeholders and that the two sections, technical and social, yield constructive outcomes for a joint security optimisation. The socio-technical view of information security is also reflected in other areas of security such as trust modelling. Pavlidis et al. (2011) consider the trust relationship between the user and the socio-technical system in the design of security software, indicating recognition and consideration of information security as a socio-technical problem [65]. Bulgurcu et al. (2009) present a socio-technical vision of information security, which is recognised as one of the top priorities of managers, but argue that technological-based solutions alone are not sufficient to deal with ever changing security risks and threats [66], though they do concede that technological solutions are nevertheless important [66]. They further argue that insider threats are real and important and present them as having a socio-technical dimension. Consequently, socio-organisational solutions are offered along with technology-based solutions that can efficiently reduce the risks. Some researchers have gone even further, arguing that extreme threats such as SEAs have absolutely no technological solutions [67].

2.8.2 SWOT Methodology

SWOT helps us to understand strengths, weaknesses, opportunities and threats in an organisational context with respect to human factors. It is generally used to generate alternative strategic plans by identifying the strengths and weaknesses of an organisation with respect to the opportunities and threats that exist within the environment [68]. The outcome of a SWOT approach assists in confirming whether a system has achieved or failed its objectives. Although the SWOT framework has been used only in planning, it is also a powerful precision tool that presents an in-depth analysis of the situation [69]. Due to technological advancements, organisations are required to continuously reconfigure their IS controls: human factors may also require appropriate adjustment. SWOT provides an enhanced evaluation when assessing organisations who are required to deal with security reconfiguration and, ultimately, helps to clarify what is required of personnel in order to achieve best practice. SWOT supports identifying an approach to maximise the efficiency of ISSs in relation to human factors. This approach would thoroughly analyse the complex issues around human roles in an ISS and is in line with the goal of this research. Figure 2.4 depicts a brief overview of SWOT. Here weaknesses can be converted to strengths and create opportunities. Reducing threats to a system or organisation and creating new opportunities is essential in

achieving the objectives of a system. If threats emerge, then a system's vulnerability can rise and weaknesses can be exploited.

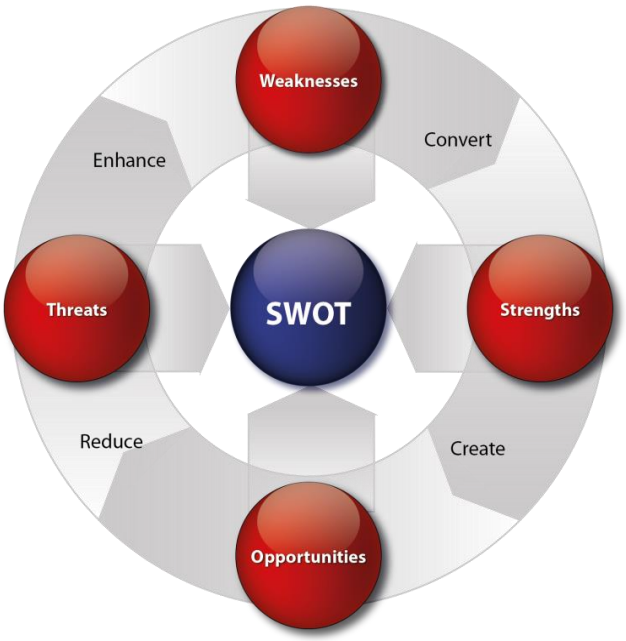


Figure 2.4 SWOT Overview

2.8.3 Delphi Survey Method

The Delphi Expert Panel Technique (survey study) is seen as a popular and established tool in the field of information security [70] [71] [72]. The Delphi method was developed in 1950's with the purpose of creating a stable and consistent method for attaining the consensus of a group of experts [70]. This research chose to use the Delphi technique because it helps to clarify the variables under investigation [73]. It is also noted that the Delphi method can facilitate multi-phase constant surveys whilst providing organised feedback loops [31]. The phases were incorporated in three stages:

1. Brainstorming sessions to identify human factors.
2. Narrowing down main human factors.
3. Prioritising and ranking human factors.

The Delphi technique is not without its weaknesses. Certain limitations and problems around the reliability, validity and credibility of the Delphi method have been highlighted [133], and these restraints have socio-technical and ethical impacts. A consensus approach may lead to a weak form of the best opinion, with the result representing the smallest common factor [134]. Also, because of the constant and comparative nature of the technique, the Delphi method is time-consuming. In addition, there are problems with the methodology arising from the panel size and sampling techniques that may lead to participants shifting from their original ideas during the study period.

2.8.4 Force Field Analysis

Conflicts must be minimised in any process of system change within organisations. Adequate communication within the organisation to convey dialogue between all stakeholders enhances the effectiveness and efficiency of the proposed changes in system. The Force Field Analysis (FFA) technique, whose principles can be found in Physics, was introduced by Kurt Lewin [74] [75]. It can be utilised as a tool, assisting organisational change by reducing tension and strengthening communication. FFA employs the idea that the equilibrium state of a system is maintained by two sets of conflicting forces. Building on Lewin's Force Field Analysis (FFA), there are two forces in organisations that work against each other. One group of forces pushes for stability and to maintain the status quo, resisting against any changes. The other group drives and pushes the system towards change. When these forces are equally balanced, a 'quasi-stationary equilibrium' arises that maintains the status quo [76]. In order that organisations go ahead with changes they require, they must reinforce driving forces and diminish resisting forces. The steadiness of human behaviour, based on "quasi-stationary equilibrium", is also perpetuated by the battle between driving and resisting forces [76]. For any changes to occur, either with humans or in organisations, the alteration of this force field is necessary. This is a very complex psychological process because there is always an instantaneous resisting force against any driving force for change, which preserves equilibrium [76].

FFA has been widely used for management changes in organisations [77]. Lewin's analysis model assesses the impact of all elements and forces that influence change. Driving forces are forces that coerce for and elevate change. Senior management support is a key example of driving forces [18]. In contrast, restraining forces are forces that serve to hold back the driving forces and prevent a change from happening by creating obstacles and risks. Concerns over individual errors could be an obstacle to the implementation of improved ISSs. Strengthening driving forces whilst eliminating restraining forces ensures the success of ISS goals, i.e. preventing risks. Driving forces usually exist in the system but restraining forces are harder to identify and establish because they are commonly personal psychological vindications that are rooted in organisations.

2.8.5 Requirements Engineering (RE)

The current reasoning in the field of RE is that requirements demand to be articulated in the framework of real-world knowledge [78]. Research in this area focuses on conceptual techniques and tools for distinctively capturing and representing in a structured way domain knowledge, which can eventually be used to drive the system development phases. The literature shows that security regulations and standards cannot facilitate a comprehensive information security solution in the organisational context [79]. However, the information security requirements engineering approach

can provide a comprehensive and structured elicitation and understanding of information security requirements [79]. This would enable an analysis and elicitation of risk, investment and return on investment concepts in the development of the RIDIM model. This approach explicitly models the relations between goals and the risk factors that obstruct these goals. Risks are then assessed and suitable control actions are selected to mitigate them so that the project can attain its goals. Further, the mitigation mechanism then enables organisations to invest adequately in security whilst the return of that investment can be calculated in a clearer and simpler way and be understood by senior managers and non-technical executives. Goals are the objectives, expectations and constraints of a specific system context and its surrounding environment as prescriptive statements of intent whose satisfaction contributes to the overall project success. The model supports different levels of abstraction from goal to obstacle and finally to treatment. A goal model of requirements engineering includes the following steps:

- Defining the relationships between an ISS and human factors in an organisational context (environment) based upon what the system is supposed to do and why. The understanding of this relationship provides reasons to justify the necessity of the ISS in the organisational context as the nature and requirements of organisations and businesses are rapidly changing.

- Elucidating ISS requirements that include the goal specifications to explain why and how the ISS can achieve its goals.

- Using sub-goals to obtain more clarification on and analyse ISS goals.

- Managing conflicts between various stakeholders of an ISS, including human factors, by identifying and assisting in the reconciliation of the trade-offs between cost, flexibility and the goals of the effective ISS. This is because the main goal can be in conflict with overall organisational objectives, such as cost reduction, that play an important role in businesses.

- Quantifying the fluffiness of ISS requirements by ensuring that they achieve ISS goals in the proposed model.

Risks associated with human factors in the process of developing an ISS should be considered at all stages within the RE phases. This is simply because human factors are the main cause of information security breaches, which obstruct the goals of the system and impacts upon its effectiveness. Fulfilling the elicitation and analysis of information security requirements can be started at the stage where stakeholders (human factors and organisational forces) are identified. A consideration of system requirements and their specifications such as risk and investment can then be analysed. This would assist the model in identifying the functional security goals that have been refined into security requirements.

Stakeholders also concern about the security incidents and their types such as Social Engineering Attacks (SEAs) which in this research are being considered.

2.8.6 Secure-Tropos Modelling

Secure-Tropos modelling is an extension of the Tropos methodology that deals with relationships among the actors within social and organisational settings [80] [81]. It introduces security-related concepts (e.g. security constraints, secure dependency, secure goals) within the Tropos methodology to enable developers to consider security issues throughout the development lifecycle. A security constraint is defined in the Secure-Tropos framework as a restriction related to security issues, such as privacy or integrity, that influences the analysis and design of the software system under development by restricting the system or by refining some of the system's objectives. These constraints represent the initial high level security requirements reported and elicited from a number of sources including the stakeholders and users of the system as well as domain and security experts. In the actor model, Secure-Tropos introduces secure dependencies whereby actors must fulfil the constraints to attain their goals. Secure-Tropos uses the term 'secure entity' to describe any goals, tasks and resources related to the security of the system.

2.9 Conclusion

This chapter discussed and summarised the investigation into the related works and relevant methodologies applicable to this research. Analysing human factors is a challenging task because human factors are a subjective matter demanding the use of socio-technical systems theory and practice to tackle; therefore, we use socio-technical theory to analyse human factors. Existing works in information security do not comprehensively focus on human factors and their impact on potential risks and the mitigation of such risks. Furthermore, these works also do not consider the return on security investment that is rooted in human factors. This research intends to develop a model that can explain how human factors and a risk-investment approach can be shaped to better respond to information security incidents and risks. Risk-driven investment modelling in requirements engineering contributes to the identification and analysis of the human factors and other organisational issues relevant to the design and implementation of ISSs. This model maps direct human factors to risk-investment issues and consequently enables one to draw a conclusion about how security threats can be mitigated or avoided altogether , using security incidents and SEAs. This research also employs the SWOT and force field theories to evaluate the proposed approach.

CHAPTER 3

Research Methodology

Contents

3.1 Introduction

A research methodology is a structured approach to solving a problem [82]. It involves examining how research is to be conducted and the process of describing, explaining and predicting hypotheses. Considering this definition, this research follows a number of theories and methods, outlined in Chapter 2, to achieve its goals. The theoretical approach of this research is based upon socio-technical theory and Requirements Engineering (RE), where human factors, security requirements elicitation and analysis are considered. Concepts from risk management, return on security investment, goal modelling and security incidents are used in developing our model. We also follow the SWOT and Force field analysis theories for evaluating the proposed approach and information security incidents. Finally, the Delphi survey method will help gain an understanding of the critical human factors with more reliability and expert consideration. Each of these theories and methods are explained in each phase of this research in various components (Figure 3.1). This figure illustrates an overview of the research methodology components adopted by this research.

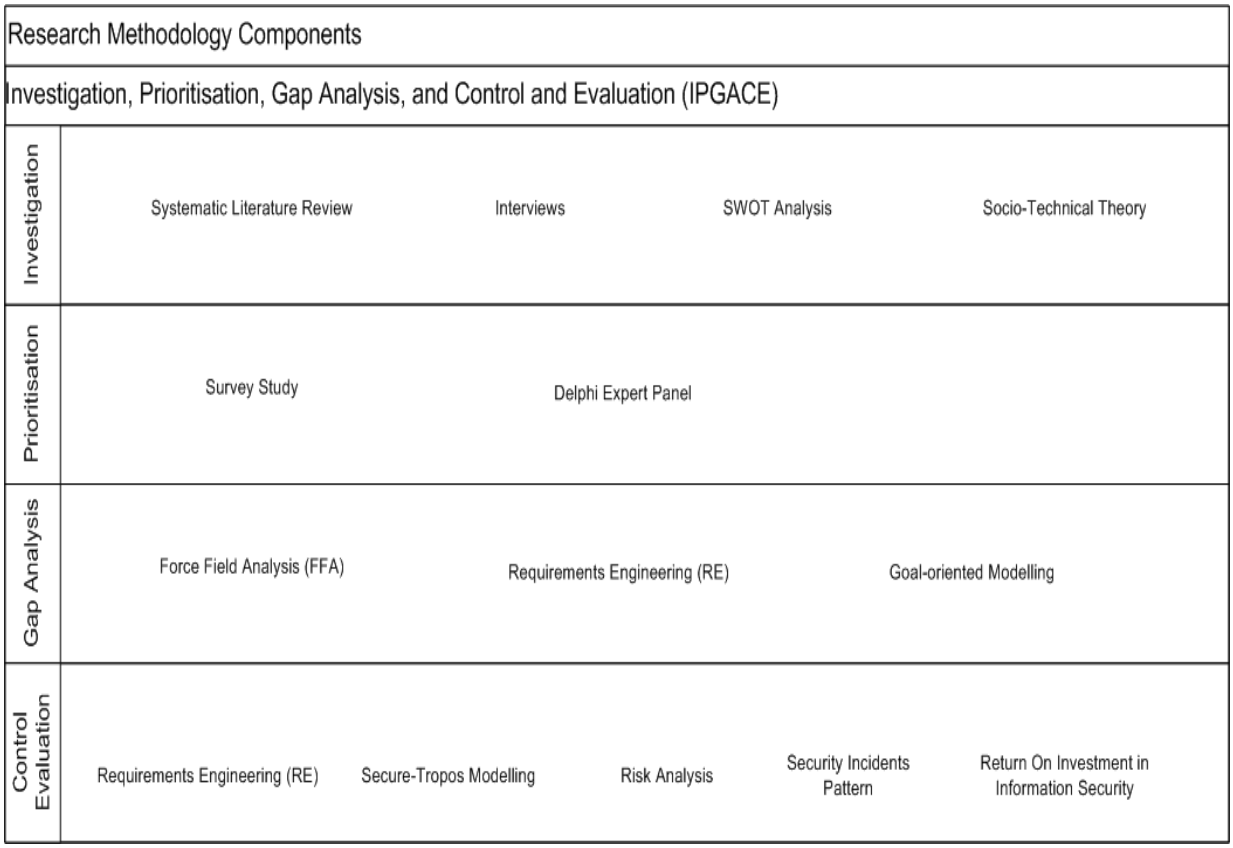


Figure 3.1: Research Methodology Components

The figure shows the four phases of the research methodology:

- Investigation
- Prioritisation
- Gap Analysis
- Control & Evaluation

The figure explains how each phase uses certain tools and techniques to fulfil its objectives.

3.2 Research Methodology Process

In order to present a comprehensive research methodology that considers all aspects of the research concepts, a systematic analysis process that consists of four sequential phases has been adopted. These phases enable us to clearly identify the problem and aims of the research and apply relevant quantitative and qualitative research methods and techniques. By utilising a mixture of both quantitative and qualitative approaches, a more enhanced understanding of the research problems can be obtained than from a single approach alone [82].

The research methodology process consists of the following phases:

- **Phase 1: Investigation** phase *to identify human factors* using a literature review, interviews, socio-technical theory and SWOT analysis. The investigation extends the problem domain relating to human factors, the organisational context of information security risk, risk analysis and security investment and reviews the existing state-of-the-art ISSs through an exhaustive literature search. This allows the research to peer into the characteristics of main human factors in great detail with a consideration of organisational culture and its effect on security culture and the contexts. Consideration of organisational context and institutional forces side-by-side with human factors, information security risks and investment provides a rich understanding of the impacts of main human factors in the process of ISS design, implementation and evaluation. Human factors in an organisational context play an important role in creating an effective security system through collaboration and teamwork, and the investigation phase allows a concrete and adequate understanding of all concepts in this process.

- **Phase 2: Prioritisation** phase *to prioritise main human factors* using a survey study, specifically the Delphi expert panel technique. This phase uses the empirical investigation for the purpose of prioritisation. There are three stages in the Delphi process that will be explained later in Chapter 6. The Delphi technique provides a group decision to ensure that each member gives an honest opinion of what they think the importance of a particular human factor will be; therefore, the process avoids pressurising people to go along with others' thoughts and allows them to join in the process in an objective, impartial and anonymous way. This method is used to obtain an agreement on ranking the main human factors without people having to agree verbally.

- **Phase 3: Gap analysis** phase *to understand the current and ideal situation* of an ISS concerning human factors using Force Field Analysis and Requirements Engineering. Gap analysis combines the strengths of both FFA and RE. Gap analysis considers the available and current controls against the root causes of incidents to fill the security control gap and, in a sense, works as an auditing process. Gap analysis also provides an accurate, objective and complete picture of what is missing in the process of securing a system. In addition, gap analysis enables the study to determine how the current controls shape the security system architecture with regard to human factors, risk and security investment. Human factors and investment affect risk in an organisation, and gap analysis can bring a significant understanding of the way an information security system is designed and implemented. In addition, gap analysis helps in finding a solution by forming a model, which this research intends to introduce. Understanding the current situation and an ideal situation builds a clear view of what the model should look like to fill the gap between current and ideal security systems and

address the main concerns of the study.

Phase 4: Control and evaluation phase *to develop a novel risk-investment model to support the analysis and reasoning of human factors in the information system development process* using Requirements Engineering, Secure-Tropos modelling, risk analysis, security incident patterns and Return On Information Security Investment (ROISI). This study chose an empirical method to evaluate the main contribution of the research. The use of a case study helped the evaluation process of the RIDIM model. Information security systems are multidimensional and vary from one organisation to another, being greatly impacted by human factors; therefore, the nature of risk is diverse and validating a specific method from a complex set of activities is challenging. Consequently, there are challenges involved in conducting an empirical study in the information security field. Information security projects, like many other projects embarked upon within organisations, have their own constraints and limitations, such as human resources, time, budgets and quality control. It is not always possible to address such concerns with a comprehensive model. Adding to this, each organisation has its own culture and approach to project management, whether it be an IS project or any other. The control and evaluation of such projects thus becomes even more challenging. However, using a combination of methods does help to satisfy control and evaluation requirements to an acceptable level. For the purpose of this research, ISS projects come with a substantial amount of risk from various dimensions and addressing all of them is very hard. The nature of risks originating from human factors are subjective and providing a quantitative value proved difficult. This becomes even more challenging when investment and return on security investments are tangled with human factors.

These phases lead to four steps, as follows:

Step 1: Establishing the problem domain in which the main human factors and their characteristics are being identified. This step comprises a literature review, interviews and SWOT analysis on the theoretical basis of socio-technical theory. In order to address risk and investment issues in ISSs in relation to human factors, it is imperative that main human factors and their chrematistics be recognised: this is the fundamental problem which this research aims to address. It is extremely problematic, given the subjective nature of human factors, to determine whether an effective level of risk and investment identification and analysis in an organisational context promotes the discovery of main human factors. Understanding and identifying human factors, however, requires a holistic approach that considers all socio-technical aspects. Human factors are not just simple issues, e.g. insider threats or end users. A detailed examination of the roles and responsibilities of end users, middle and senior managers in the organisational context is required. In addition, the culture and the nature of the business play an important role in this process.

- **Step 2: Ranking human factors**, whereby the critical human factors and their characteristics are established. This step involves the Delphi expert panel and survey study. The main human factors are prioritised to ensure that only the critical factors are determined. The main human factors in themselves are very difficult to analyse and quantify on the basis of risk and investment in ISSs; therefore, they need to be prioritised and ranked for the identification of the critical human factors. The prioritisation assists us in the modelling and evaluation process, making it more concise and effective. This can be achieved by identifying which factors will have the most substantial impact, which are the most important and which are the most relevant. The impact, importance and relevance of an ISS must be considered to ensure that the outcome model is the most suitable one for addressing human factors.

- **Step 3: Understanding the situation**, in which the various concepts involved in the process are defined. This step includes the Force Field Analysis (FFA) and Requirements Engineering process. This step is absolutely necessary for the gap analysis. Without a clear understanding of the current situation and where organisations are in an ISS, providing a solution that can be tested against it would make no sense. This step allows the gap analysis to find the deficiencies in ISSs created by critical human factors and address them. Understanding the current situation will enhance the maturity of the proposed model. In the security industry, an understanding of the current situation is used in gap analysis to compare and weigh with information security standards such as ISO27001. However, as we have argued previously, such standards cannot provide a detailed, optimal solution for dealing with critical human factors in a risk and investment-based environment, and ultimately the proposed solution will lack maturity. This level of maturity is required to address very subjective and critical human factors in the ISS process.

- **Step 4: Modelling human factors**, whereby the various activities defining a number of concepts lead to the formation of the RIDIM model to allow the modelling of critical human factors, risks and security investment. For research to reach to this point, the key concepts of the study focused on defining and exploring critical human factors and risk and security investment concepts based on a holistic theoretical framework composed of key parts of ISSs. The central foundation of this step is to model how critical human factors impact upon each area of information security risk management, security investment and ROISI. Critical human factors within the RIDIM model pose the central risk to security investment and entire ISS.

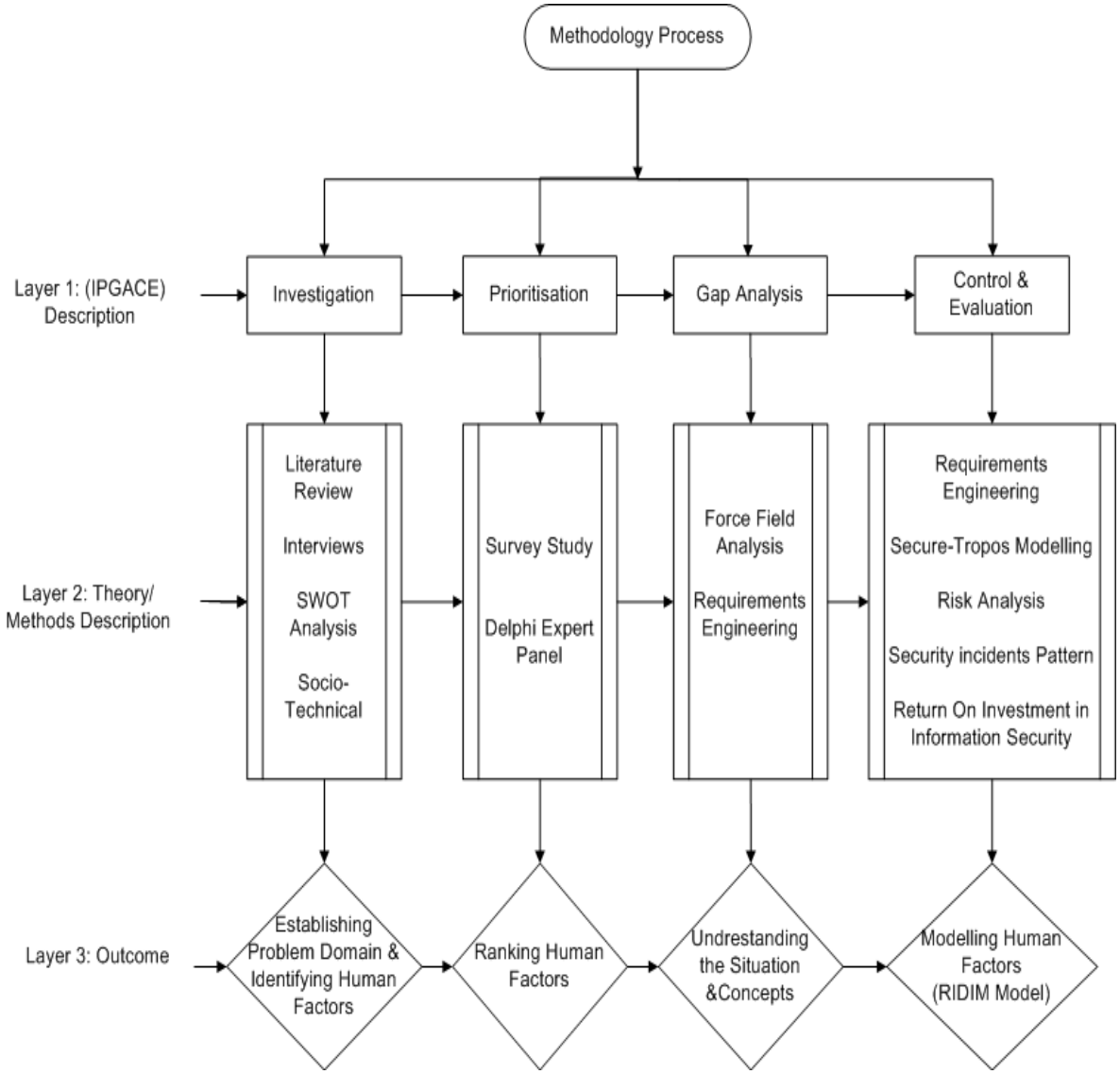


Figure 3.2: Overview of research methodology.

Figure 3.2 shows the underlying methodology process, which consists of three different layers. Layer 1 includes the 4 phases of Investigation, Prioritisation, Gap Analysis and Control & Evaluation, named IPGACE and described above. Layer 2 describes the theories, methods, tools and resources used during the course of this research. They include a literature review, interviews, the SWOT analysis tool, socio-technical theory, a survey study, the Delphi expert panel, Force Field Analysis, Requirements Engineering, Secure-Tropos modelling, risk analysis tools, security incident patterns and return on investment in information security. Layer 3 examines the efficacy of the tools and techniques employed by this research.

3.3 Data Analysis

In this research, qualitative and quantitative data analysis techniques were applied together. In order to understand, organise and contextualise,

interpretations of qualitative data derived from interviews and surveys was used in the content analysis. For the purpose of analysing data from the surveys, inferential and descriptive statistical methods were employed. The research used the Statistical Package for the Social Sciences (SPSS) software package to analyse the data. Despite the fact that SPSS does not support structural equation modelling and does not allow simultaneous estimation of regression parameters and the mapping of associations between independent variables, it is nonetheless very useful for thoroughly exploring data [24]. The results of the SPSS technique strengthened the analysis of main and critical human factors.

3.4 Sampling

Quantitative and qualitative data from large financial organisations, including insurance companies, retail and investment banks, has been collected based on predefined criteria to serve the purpose of the research goals and objectives. This approach provided a sound judgement for an inform sampling from the case study organisations. The research objectives required a flexible approach for gathering the samples, which was made possible by the use of a case study and multiple data collection methods. In order to conduct a Delphi study with greater reliability, the number of participants was increased significantly to ensure that their number was sufficient.

3.5 Validity, Reliability, Repeatability

The validity of the research findings is related to the extent to which the data can be generalised and how relevant and applicable it is in other frameworks [24]. The more objectively and consistently data analysis is carried out, the greater the validity expected. This relies clearly on the choice of the methodology, which handles greater reliability when retained systematically and accurately. In addition, it is crucial that the data analysis and research findings are logical and distinct, and that they are presented accurately with a rational relationship to all concepts. This quality of the outcome of data analysis ensures not only reliability but also repeatability [135]. In other words, given a similar setting with homogenous team members, the outcome and research findings would be expected to be quite alike. This research believes that using a mixed methodology has secured validity, reliability, objectivity and credibility whilst also ensuring repeatability.

3.6 Ethical Considerations

In any research project, the ethical requirements and principles must be considered and dealt with sensitively. They are fundamental for safeguarding both participants and researchers and have been designed to ensure the wellbeing of both, in addition to protecting their privacy [24]. Furthermore, there are many regulations and legal requirements that research bodies must follow. This study was conducted with thorough deliberation on how the research findings may impact participants and their

respective organisations, whilst at the same time bringing many advantages to similar organisations. The analysis and understanding of the role of human factors and their impacts in the organisational context within a risk-based and security investment approach provides a significant contribution to knowledge about the safety and protection of organisational assets from human-activity-related risks. One of the primary and most important underlying ethical principles is privacy and confidentially which, during the process of this research, was considered and complied with [135].

This research was carried out in adherence with the ethical research policies of the University of East London. A letter of consent and researcher's introductory letter was provided to the participants with an explanation of how data will be used and treated in this research. Participants were assured that their personal and organisational identities and any data they provided would be safeguarded during the research with regard to privacy, particularly whilst being transferred or kept in storage. All data was encrypted using AES 256 encryption methods. The participants were also assured that all data would be erased at the end of the research.

3.7 Conclusion

This chapter provides an overview of the research methodology used in this research. There are various uncertainties throughout the development of an ISS project. These ambiguities include a diverse range of non-technical factors, such as people, organisational context and investment requirements; all introduce risk, which requires attention and mitigation. For this purpose, the study presents a vigorous research plan whereby several different techniques to collect both quantitative and qualitative data are utilised with a view to answering the research questions. The research follows several techniques, including a literature review, SWOT, force field analysis and an empirical investigation, for this purpose. Furthermore, the research also follows concepts from existing well-known methods such as Secure-Tropos. The validity, credibility and reliability of the research findings were reinforced by the introduction and employment of these mixed methods.

CHAPTER 4

An Overview of Human Factors

Contents

4.1 Introduction

Technical advancements do not always produce a more secure environment. All kinds of human factors can deeply affect the management of security in an organisational context; therefore, security is not solely a technical problem; rather, we need to understand human factors to achieve effective information security system practice. For this purpose, the study identifies critical direct and indirect human factors that impact upon ISSs. These factors were analysed through the study of two security incidents in UK financial organisations using the SWOT (Strength, Weaknesses, Opportunities, and Threats) technique discussed in the preceding chapter.

Typically, human work within an organisation falls into four categories: individual, team, management and customer/interested party [83] [31]. Human factors within these categories can become uncontrollable forces. Because people have different perceptions of security, their reactions to information security procedures are diverse. Each individual has concerns, values, culture, skills, knowledge, attitudes and behaviour of his or her own. These factors are highly subjective and extremely hard to measure and calculate in ISS processes. These human forces interact with technological elements in an interconnected world of so-called "secure information systems" [32]. People have their own unique culture, attitudes, skills, knowledge, understandings, behaviour and interests that depend upon the role that they play within the organisation. Individuals' interaction with computers and decisions made with regard to information security are certainly very dynamic and complex issues. Human factors are the greatest single issue of concern in IS [33]. We therefore need a comprehensive understanding of human factors and their impacts for an effective implementation of ISSs. This task is challenging, as the domain is highly subjective by nature and it is difficult to quantify all the factors into a measuring scale. There are many areas in which judgement becomes extremely difficult and hugely subjective because the study is about people and their reactions to IS and, therefore, it is highly personal. For instance, it would be extremely difficult to judge and evaluate people's apathy and their attitudes towards ISSs.
This research categorises the critical human factors as direct and indirect. The direct factors are greatly dependent upon an individual's perception,

behaviour and knowledge of IS, whereas the indirect factors are affected by an individual's understanding, predominantly by forces beyond their power such as organisational culture, guidelines and policies. The identified factors have been analysed using two real security incidents in UK financial organisations. This study used the SWOT (Strength, Weaknesses, Opportunities, and Threats) analysis tool for this purpose. The study's observation is that technology is not responsible for these security incidents: humans are. This research discovered certain elements that were involved in these incidents, such as errors, inadequate awareness of programmers and lack of communication between senior management and employees. This study concludes that individual security awareness, communication with the security team and adequate and sufficient budget planning are essential accompaniments to technical solutions in effective information security practice. As mentioned above, it would, for the purposes of this study, be highly arduous to quantify the result. However, using a business tool would assist in acquiring a trade-off balance between human and technology factors. People are at the centre of any technological design and use of a product. An ISS, like any technologically designed system, requires consideration of a user-cantered design approach [84] to avert the risk of individuals behaving irrationally with these system designs. The role of humans has never been disputed. People (users) can be an asset or a threat.

Organisations must therefore address human elements in order to deal with IS incidents, as highlighted by researchers in the aftermath of a number of human-related security incidents [34] [18]. Organisation policies, standards, procedures and codes of conduct are designed for people to follow. People are the executers of policies; this involvement of people has a significant impact on any proposed ISS. The human factor is one of the major forces behind the effective success or failure of a security system [8] [31] [32]. Sarker stated in "Assessing insider threats to information security using technical, behavioural and organisational measures" that technical solutions alone do not suffice because insider threats are fundamentally a people issue [35]. The evidence clearly shows that the human factors in ISSs have been undermined and underdeveloped.

4.2 Direct and Indirect Human Factors

Figure 4.1 depicts two main categories of human factors: the direct and indirect factors and their sub-factors. These factors have been identified through systematic literature review, survey study and interview sessions from samples taken in five organisations. In this study, direct factors are those that mostly depend on certain individual characteristics and have a significant impact on ISSs. Indirect factors greatly depend on external factors such as organisational issues (i.e., inadequate budgets or budget management and security policy enforcement). They also influence direct factors and ultimately the ISS. This section provides a brief overview of each of these factors.

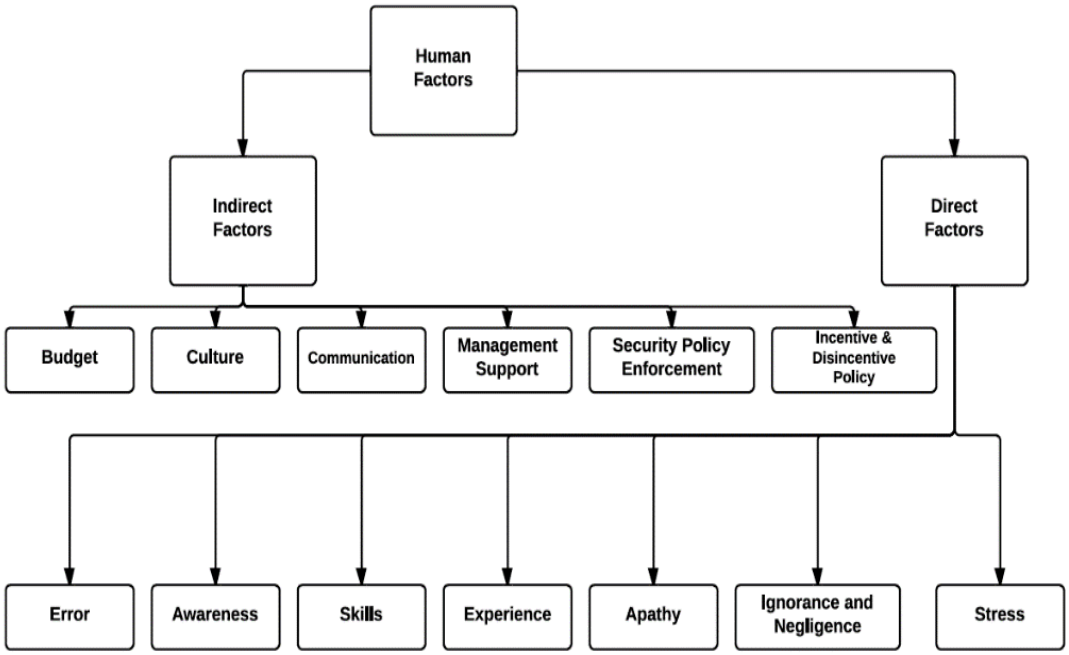


Figure 4.1. Human factors in information security systems.

4.2.1 Direct Factors

Direct factors are based on individuals who have a direct impact on the overall ISS within an organisation. These individuals are involved in the organisation's efforts to meet its goals and objectives. For instance, error, apathy, stress, awareness and experience have a direct relationship with character and personality. They are also social entities within the ISS and cannot be measured using a technical approach. A socio-technical approach enables these entities to be defined in an ISS and is constructed upon social and technical sub-systems alike [51]. As stated previously, these factors impact the ISS by affecting individuals directly. Direct factors are mostly dependent on individuals' characteristics. Indirect forces, such as security policy enforcement and management support, mainly exist in the organisational context and therefore do not have any effect on people's actions.

Errors

Error can be defined as a divergence in a system that works accurately [85]. IS incidents often happen when a security measure has been used that is adequate but blind to human behaviour [14] [86]. For example, password validation policies commission people to choose a complex password. Such a password would likely be a combination of letters with at least one letter capitalised and digits that some users may find difficult to remember. As a result, people write down their passwords in unsecure places such as their notebooks, which can be seen by others. Personal roles in IS policies should thus be given great attention. Human errors can be deliberate or careless. However, some authors such as Kraemer and Carayon believe that human

errors are careless accidental incidents exacerbated by poor ISSs [14]. Their investigation concludes that indirect forces, such as communication and security culture, are the sources of human error. Consequently, ISSs with an extremely high technical backbone can be stumped by human error. In other words, many technical measures can be defeated by errors made by people. Security policies are designed to restrain behaviour in order to eliminate errors. However, behaviour is significantly hard to define, measure and control in any organisation.

Information Security Awareness

Awareness programs ensure that people in organisations understand their responsibilities and are a focal point in ISSs. For instance, users should report any suspicious email they receive. Information Security Awareness (ISA) terminology concerns people's understanding and consciousness of an ISS through security policy. The security policy can be misinterpreted and misunderstood and, therefore, the awareness program is as important as any other IS procedure. The NIST report concluded that the importance of factors such as a clear definition of roles and responsibilities has been ignored, and these factors are required to be perceived by employees in addition to awareness programs [87]. It has been widely accepted that awareness programs have a positive impact on the effectiveness of ISSs [14] [37]. Organisations are extremely apprehensive about their employees' ability to follow and implement information security rules and regulations, such as in a security policy [39] [88]. However, a number of studies have criticised current IS awareness approaches for the absence of solid guidelines and adequate theoretical reasoning [39] [89] [90]; therefore, it is clear that there is a gap in the research on developing more effective and adequate ISA programs.

Skills

Skills facilitate the function of a role and play an important part in effective human performance. Education and training are crucial in developing skills and demonstrating a commitment to preserve professionalism and competency. Skills are one of the main forces in dealing with IS issues such as incident response [91]. The absence of adequate and appropriately skilled staff contributes to a weak performance of IS policy [14]. In dealing with all aspects of an ISS, skill competency plays a major role [34]. Employees are required to possess adequate skills to deal with the requirements of information security policy. For instance, if people do not know how to deal with suspicious emails, they might open them. It is also important that people's skills are not overestimated or underestimated [32]. Organisations must not focus solely on people with complete technological competency. Training programs, which equip employees with adequate skills to confront IS challenges and meet organisational objectives, should be selected from mixed and varied factors of business [92]. This becomes more important when business behaviour is changing rapidly due to new technological advances [93]. Organisations are required to be flexible enough to absorb rapid change in the business environment.

Experience

Subjective experience contributes to human knowledge [94]. Scholars have different views on the factor of experience with respect to the ISS concept. Some argue that people's understanding of IS concepts and procedures relies upon a few human factors, including their experiences [32] [95], whilst some go further and claim that a successful implementation of an ISS depends greatly on people's knowledge and experience [32]. These scholars believe that experience is necessary for an information security team. They argue that inexperienced employees and a lack of training is a threat to information assets. However, adequate security behaviour is more related to people, management and social skills than security experience [92]. Although there is disagreement on the level of influence the factor of experience has, both sides would not deny its important role. For example, a new access control applies a limitation on shared information in order to preserve corporate secrets. Employees may find this requirement extremely challenging and contradictory to old practices; therefore, their experience of the free movement of information is undermined by the new policy.

Apathy

Apathy in an organisational context can be seen as the unwillingness of employees to contribute to the achievement of the organisation's goals and objectives in situations where they should demonstrate pro-social behaviour [96]. Apathy creates significant issues in organisations due to a lack of willingness to implement organisational procedures. Apathy towards ISS procedures and rules drives uncertainty in the security policies because people are not willing to follow them. It creates an environment in which employees believe they have no responsibilities [97]. Whereas a positive attitude, motivation and optimal working conditions contribute to better performance, apathy and unresponsiveness produce undesirable functions [98]. Siponen argues that positive attitude serves the effectiveness of a security system; however, it is extremely difficult to measure attitude and motivation [89]. Thomson argues that miscommunication between employees and senior management contributes to misunderstanding that leads to employee apathy [96]. This report also notes that in organisations where a coercive environment exists, employees feel frustrated and dissatisfied [5] [99]. A coercive environment has been defined as an organisation where everything is dictated and no consultation with employees is made with regard to corporate goals and objectives [99]. In such an environment, people are not motivated to work toward organisational objectives, such as ISS goals. For example, if senior management changes backup procedures without consideration of human and organisational limitations, a coercive environment will form in which employees will lack enthusiasm for following security policy; ultimately, the performance of the team suffers and the effectiveness of any proposed ISS will be undermined.

Incentive and Disincentive Policy

Incentive and disincentive policies in organisations reward good behaviour and punish bad attitude. There are certain connections between people's

attitudes and incentive and disincentive policies; even a little persuasion invariably increases motivation. Kabay argued that even a simple comment on IS policy made by an employee should be considered seriously, considering how it can ultimately affect the entire ISS in an organisation [97]. Incentives and disincentives are important factors in an organisation, but they have not been considered in previous studies of ISSs. These factors have an impact on people's motivation to go along with IS policies [96]. Organisations sometimes focus on punishment when instead they should divert their attention towards training and reward policy. For example, organisations should reward employees who report IS incidents or suspicious behaviour and provide training instead of punishing people who open up their personal emails at work. Incentives promote a positive attitude and encourage employees to act in a pro-social manner, whilst punishments alienate people. Employees may then still follow the IS policy even if they do not approve of it, because they have been rewarded for demonstrating the desired behaviour [5] [99].

Ignorance and Negligence

Employees in organisations, sometimes unintentionally, do not pay enough attention to security policy. One example of user negligence and ignorance is when software piracy occurs because employees have little knowledge of software installation for various reasons such as a lack of training. The number of IS accidents attributed to people is high: accidental breaches form the majority of incidents [100]. The impact on an ISS as a result of ignorance or negligence requires decisive action and must be addressed by IS professionals. Organisations pay far more attention to reinforcing technical facilities to overcome this issue, but ignorance and negligence are human issues and must therefore be confronted differently. It is also very difficult to audit people's behaviour. Some authors addressed this problem by proposing the use of deterrence theory, in which the threat of sanction is recommended [6] [101] [102] [103]. Vance argues, however, that employee negligence and/or ignorance of IS policies is not always corrected by fear or threat [11].

Stress

Individuals' stress in corporations can be caused by heavy workloads and tight project deadlines. People react maladaptively to stress and work overload despite any training programs they may receive. Stress leads to human error. Those under stress may have a tendency to bypass IS policies. Stress and fatigue have a direct relationship to IS vulnerabilities [77]. Unbalanced and excessive workloads create stress and extra pressure for employees; such a load greatly undermines people's morale and organisational ethics [97]. Assigning heavy workloads creates extra and unwanted pressure on people and can lead to a downturn in an organisation's moral behaviour. This moral and ethical breakdown prompts IS incidents because people do not feel valued [97]. Organisations must ensure that their employees are protected from both internal and external pressures.

4.2.2 Indirect Factors

Indirect factors have a certain influence on direct factors, as well as impacting upon ISSs. However, these factors affect people through elements that are largely controlled by organisations and which individuals have no jurisdictional power over; therefore, these factors are collective matters managed by organisations. We consider five indirect factors: budget, culture, communication, security policy enforcement and management support.

Budget

Running an organisation costs money; therefore, the existence of an organisations depends on adequate budget planning. Information security experts widely believe that budgets have a significant impact on the efficiency of ISSs [76] [104]. To ensure that an ISS fulfils its objectives effectively, organisations must have an effective cost strategy, which should be adopted for addressing the technical and personal requirements of the ISS. For instance, organisations will not be able to deal with ISS goals sufficiently if an access control mechanism has not been implemented or if employees have not been receiving adequate training. Although organisations are required to invest in IS, they may not be able to maintain a sufficient level of investment; thus, the areas that are most vulnerable and at risk, such as back-up and disaster recovery planning, should be an organisation's main concern [104] [105]. The importance of training emerges when the element of cost effectiveness is highlighted. Some measures to reduce cost, such as automated user access provisioning, require training programs that are less costly. This demonstrates the relationship between budget planning and direct human factors.

Culture

Organisational culture consists of the values, beliefs, practices, attitudes, behaviour, reputation and ethics of an organisation and its employees. Dhillon believes that information security culture (ISC) provides a behavioural model in which organisations facilitate the protection of information assets [106]. On the other hand, some authors argue that ISC is a management problem and cannot be fully determined [107]. To demonstrate the ISC in organisations, the example of security policy can be used: Employees follow an embedded security policy as part of the ISC within the wider organisation culture. The support of management is necessary to ensure ISC is promoted to enhance the effectiveness of the implementation of security policy [108]. This can be achieved by increasing awareness, training and education programs. There are certain limitations to the study of ISC, however, due to the complexity and sensitive nature of its concepts.

Communication

Communication in an organisational context is the exchange of messages and ideas between people inside and outside of the organisation. Communication enables people to convey a message to an appropriate destination or person. The development of information and

communication technology has played an important role in computer security [106]. There are many forms of communication, but the most common are face-to-face and written, both electronically and by hand. Communication can be used to enhance IS awareness and motivate employees to comply with security policy. At the same time, if communication goes wrong or is misused, the outcome could damage the ISS. Management is required to communicate effectively with employees to ensure that they are aware of IS policy and understand the reasons for its effective implementation. The subsequent effective communication involves reaching all employees in an organisation at all levels of its hierarchy [109]. Examples of communication include security awareness workshops as well as email, phone and face-to-face meetings. In email exchanges between employees in an organisation and people in other organisations, for example, confidentiality plays an important role. Employees must be informed about the sort of information that can be sent to third parties without violating confidentiality.

Security Policy Enforcement

A security policy is an organisational document in which the information security procedures and rules are outlined. Employees at all levels of the organisation must understand the security policy and participate in its implementation according to their position [1]. Enforcing a security policy is a major issue for an ISS and its successful implementation should be supported by management [1] [110] [111]. Network security, access control, IT personnel job descriptions and password policy are examples of factors that are required to be covered by security policy. IS policy violations are under-researched, and there are clear gaps in this area [112].

Management Support

To enforce policies relating to the ISS in organisations, management must support it from the design stage through all evaluation stages. The role of management in an ISS is not only to advocate but also to deliver a clear message of IS policy to the rest of the organisation. An obvious example of management endorsement of an ISS in organisations is the allocation of an adequate budget, which is entirely under the control of senior management. The general perception of senior management is that an ISS is entirely the responsibility of an IT department, who should ensure the installation of appropriate and adequate software systems to preserve the security of information [113]. To ensure senior management is fully behind ISSs in organisations, they need to learn that IS has a direct relationship with the core of the organisation's operation. Consequently, the budget and enforcement of IS policy requires the full support of senior management [114].

4.3 Conclusion

This chapter presents a list of human factors based on a review of the literature. Human factors are extremely challenging forces for a variety of reasons: they are painfully difficult to test and evaluate and are a subjective

matter that is too difficult to separate from personal feelings and opinions when dealing with individuals who are different from one another, whilst each organisation has its own unique culture, values, and practices. We have categorised these human factors as direct and indirect. Since our findings are mainly based on the literature review, the following chapters in this research focus on evaluating these factors through an empirical investigation.

CHAPTER 5

Risk-Driven Investment Model (RIDIM)

Contents

5.1 Overview

The main contribution of this research is the development of a Risk-Driven Investment Model (RIDIM) to identify, assess and manage security incidents and related risks due to human factors as well as the cost and return on investment of proposed control measures. The proposed model is based on a holistic concept in which more than one aspect of an incident is considered. This includes the consideration of risks related security matters in addition to purely economical and non-technical, critical human factors. This chapter provides a review of the set of concepts used for this model, including Business Domain, Security Incidents (SIs), Risk and Return on Information Security Investment (ROISI). These concepts provide critical insights and understanding into conceptualising security incidents and risk so that appropriate control actions can be identified within the investment model.

5.2 Concepts for the Model

The RIDIM risk-driven investment model is based upon the conceptual understanding of an ISS within an organisational context. The model is based upon several concepts such as security incident, risk and return on investment within an organisational setting. All of these concepts are necessary to determine the adequate and appropriate level of investment in a control mechanism required to effectively address risks to information assets through Security Investment. The conceptual model addresses the risks from four angles: nature, impact, mitigation, method and cost [136]. The nature reflects the business type and quality of risk, the impact indicates the severity and quantification of said risk and mitigation deals with the control mechanism itself. Finally, the cost and return on cost demonstrate how risks impact the organisation economically. These four elements of risk are most relevant to the main objective of this research. This section outlines the main concepts in RIDIM.

5.2.1 Business domain related concepts

An effective ISS depends as much on knowledge of the business as on software architecture. Security professionals require the translation of business requirements and goals into an ISS solution capable of meeting those goals and requirements. Business domains and processes are varied, even within each sector itself. For example, retail banking, investment banking and insurance all lie within the 'finance industry' but have radically different domains and processes; despite being in the same industry, their business concepts are divergent. Without understanding business requirements and objectives as well as specific industry trends, it is difficult to design and construct any security system and leads to a lack of insight into risks and investment-related concepts and, ultimately, to an insufficient and inaccurate understanding and estimation of ROISI. This lack of understanding also extends to data, people, human factors and the specific use of processes that should be aligned with business objectives and security goals. An organisation's business domain and IT strategy are two factors that most influence the adoption of security countermeasures [115]. The impact of security breaches and, consequently, their cost and that of appropriate countermeasures are therefore varied. Business domains, risks and critical human factors all provide sources for ISS requirements (Figure 5.1).

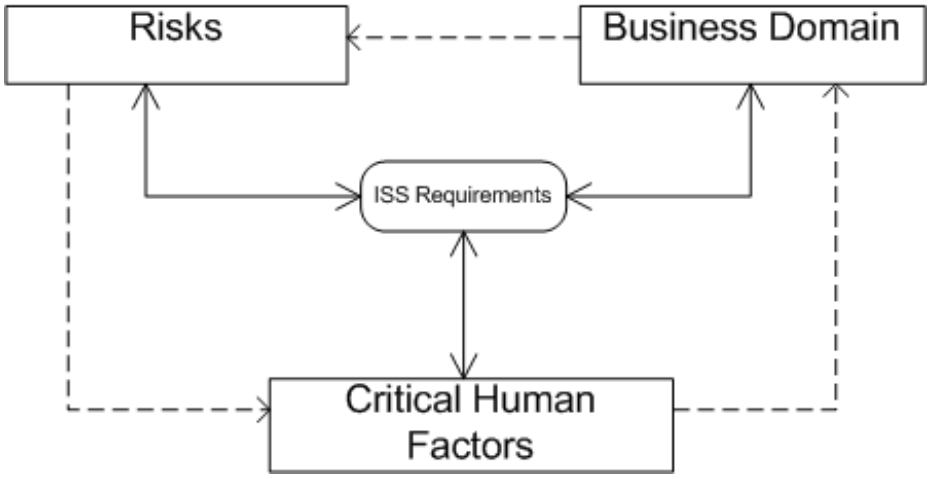


Figure 5.1. ISS requirements dependency.

Some authors suggest a link between the business domain and the IT domain [116]. The business domain entails processes, functions and objects; therefore, there is a clear link between the business domain and information security. In addition, the business domain maps to the ISS process and is decomposed into procedures, activities and tasks historically not defined under the business process [30]. The risks and human factors from the business domain are mapped to the functions and objects of the ISS. The business processes and functions are understood through IT, which aggregates one or more functions from the ISS. However, as IT and, consequently, security have been viewed as an agile project, they have not been grown into business domain. Agile projects are in contrast with

traditional business processes. They speed up the activities to save time and other resources. Based on ISS requirements and their relationship with business domain and risks, the identification of the business domain and its concepts involves:

- Defining business processes and their actors.
- The categorisation and valuation of assets.
- Determining security requirements: vulnerabilities and threats.
- Assessing risks.
- The identification of countermeasures and control mechanism(s).

The direct and indirect factors identified thus far include: Errors, Awareness, Skills, Experience, Apathy, Ignorance and Negligence, Stress, Budget, Culture, Communication, Security Policy Enforcement, Incentive and Disincentive Policy and Management Support. The direct human factors such as error, awareness, skills and ignorance have been mentioned in many academic and professional reports as the source of SIs; this is because they have direct and substantial impacts on SIs. It has been reported that human errors and other factors related to people caused two-thirds of data breaches and SIs in 2012 [4]. According to this report, a lack of system controls and human mishandling of confidential data were implicated. The incidents are costly and as each business sector is regulated differently, the cost is varied from one sector to other. The financial and healthcare organisations are excessively regulated, therefore the incidents attract more regulatory fines. The same report also estimated that 64 percent of SIs are directly related to human error. Despite the widely accepted human factor impact on SIs, the average cost of each incident varies across the globe: it is directly related to the type of threat, business domain and regulatory regime in different countries.

The critical human factors have been discussed, but analysing the risks to information assets requires an understanding of issues and concerns surrounding those assets. The five principles considered the most important in the domain of information security, regarded by some as the 'golden rules' discussed in the Chapter 2, are: Availability, Integrity, Confidentiality, Accountability and Auditability.

5.2.2 Security incident related concepts

Security Incidents (SIs) are regarded as sequences of events that undesirably affect the information system and assets of an organisation; therefore, SIs often include multiple threat events. Regardless of all the controls and protection mechanisms organisations build into their information system and applications, they still experience SIs. Information security standards such as ISO27001 expect that organisations be prepared for these incidents [20].

In order to respond to SIs, their general elements must be first understood and clarified. These elements can be defined as follows:

- The incident's agent: Who's actions impacted the system and assets?
- The incident's events: What events impacted the system and assets?
- The incident's object: Which part(s) of the system and assets were affected?
- The incident's features: How were the system and assets affected?

Significant losses can result from various types of damage. If damage is inflicted, it ceases to be a threat and becomes an attack. These attacks originate with the vulnerabilities of information processing systems. The type of breach is also important in studying ROISI because their impacts vary. Understanding the dynamics by which threats engage with a company's assets and controls allows security professionals to model risks. One of the outputs of such a model is the ability to see how the risk varies as the control settings change. If the company can estimate the cost required to turn a control setting up one or two clicks, and the model predicts how the risk will fall when this action is taken, then it is straightforward to do a ROISI calculation for each proposed change. The ROISI is the reduction in expected harm for the cost of the change.

Security incidents and potential losses may also originate with trusted internal employees who fool a system or external sources, such as hackers. However, it is not always possible to estimate information SI losses accurately because many of them cannot be discovered. This is for reasons such as adverse publicity. In addition, SIs are greatly dependent on human factors. Issues such as ineffective communication, error, apathy, stress and lack of awareness are behind threats such as social engineering. Different types of breaches require different types of controls and countermeasures. Because impacts are varied, the quantification of such impacts is not easy [117]. One of the main reasons for this is the nature of controls themselves, as mentioned earlier. Technical aspects and controls are clearer than non-technical forces such as human factors, people, culture and organisational attitudes towards security. Information security incident management also assists businesses in ensuring their continuity and developing their contingency planning processes. After understanding the general elements of SIs, the type of security incident itself can be defined in detail in terms of description, underlying threats and vulnerabilities, impact, duration and security controls.

Most organisations do not pay considerable attention to SI response procedure until their first SI occurs [39]. Consequently, many organisations lack incident response planning and have no means of preventing an incident or minimising its impact when it occurs. Advance planning is vital. A qualified SI response team as well as a detailed document that thoroughly prescribes the stages to be followed when a SI occurs should be put into place in any organisation. They must be able to detect incidents using various techniques such as intrusion detection systems and application firewalls. This monitoring mechanism will notify the information security

team in case of any intrusion or attack. As soon as an attack has been detected and the appropriate personnel informed, action can be taken to terminate or contain the SI.

5.2.3 Risk-related concepts

Risk management principally emphasises the successful completion of projects through the management and control of known risks. Information security risk management, as part of the bigger risk management initiatives, focuses on ensuring the total security of assets and information systems by managing and controlling security risks. The speedy evolution of risks in information security is overtaking this approach. Information security resilience requires acknowledgment that organisations must prepare now to deal with severe impacts from SIs that are impossible to predict, detect and prevent. Organisations must extend risk management to include risk resilience in order to manage, respond to and mitigate any adverse impacts of information SIs.

Security resilience also requires that organisations have the ability to predict, detect and prevent SIs by responding rapidly, efficiently and effectively to them as well as to their consequences. This entails understanding multidisciplinary units such as risk, investment and business domain and their functions in organisations to develop and evaluate control plans and settings for when SIs occur. With effective communication channels between all parts of the organisation, these measures can be adhered to by employees or contractors who might have been compromised in addition to shareholders, regulators and any other stakeholders who might be involved. Figure 5.2 depicts information security risk interdependency concepts in which the following core risk objectives can be defined:

- Identify critical organisational systems and assets.
- Assess and assign value and importance to the identified systems and assets.
- Identify the threats to and vulnerabilities of the systems and assets.
- Determine the known risk pattern.
- Determine the existing control measures or other risk-mitigating features.
- Identify the residual risks.
- Develop a risk profile and align it with investment in information security.
- Create a risk mitigation strategy.
- Determine inherent risks: value the unmitigated risk exposure.
- Obtain regular evaluation reports and update the risk profile.
- Document risk assessment process, including the risk acceptance criteria and criteria for risk assessment.

The core of the figure is information security risk, which is considerably impacted by threats and the monetary value. All risks are addressed by

controls and defined by information security features. In addition, risks influence and are defined by investment, which is in turn ultimately defined by the business. The business is the ultimate decision-maker for controls and investment because it owns the assets and is ultimately responsible for them.

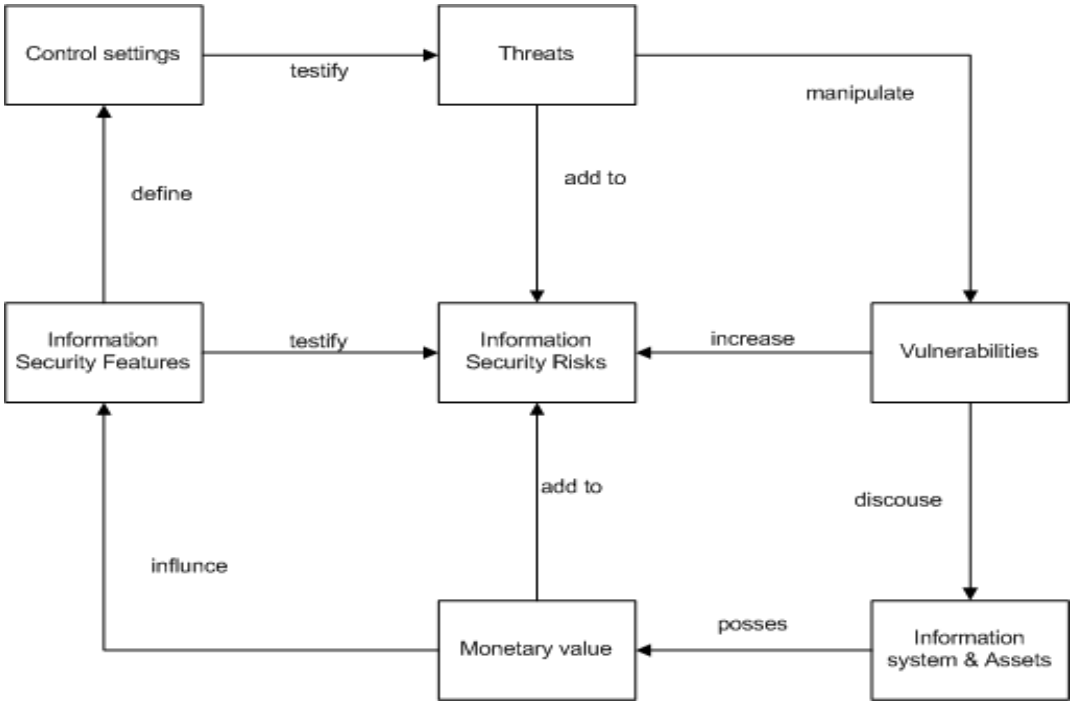


Figure 5.2: Information security risk concepts.

5.2.4 Return on information security investment: Related concepts

Tools and strategies are essential in keeping organisations cost effective whilst information security professionals endeavour to demonstrate the value of and Return On Information Security Investment (ROISI). Information security systems research literature indicates that there is a clear relationship between investments and SIs in ISS and enhanced organisational performance. Available tools and methods allow organisations to calculate and analyse the financial impact of a specific security control but cannot be used to analyse the cost-benefit of other factors such as critical human factors. Information security management systems are now increasingly based on economic principles such as cost-benefit analysis [48]. This is part of an information security financial metrics approach that has been developed mainly within the last 10 years. Providing the balance between information security cost and benefit is essential for organisations. However, organisations will invest to a greater extent in information security as long as the cost of investment is less than the cost of potential risk [49]. There are important variables in this measurement that are required to be as precise as possible. Accurate information about the likelihood of SIs occurring and their impacts must be acquired in order to assist the quantification of ROISI. However, it is important to remember

that there is a significant difference between quantifying and measuring ROI in ISSs and actually implementing new machinery systems and controls [50]. Before examining the ROISI-related concepts, a quick overview of the traditional approach to the return on investment, which is used in enterprises as a performance measure to assess the effectiveness of an investment, is presented. This involves a quantification of the aggregate return on an investment compared to its cost. The two most important concepts used in ROISI are:

- Return On Investment (ROI)
- Net Present Value (NPV)

This research uses the above classic financial metrics to describe and define some concepts related to ROISI.

Return on Investment (ROI) – Traditional Financial Metrics

Senior executives in many organisations often demand that the return on information security investment be calculated and presented to them. This seems like a typical business practice, although for major investments such as those made by financial organisations, the practice becomes very controversial when it comes to information security. The process should consider the credibility of the calculation with due care as the process entails consideration of all resources. Investment in information security could add some business value by reducing the occurrence of SIs or the response time to such incidents, which itself could improve the business reputation but not necessarily generate revenue. Information security departments thus have less flexibility to justify security investments, unlike marketing departments, which can quickly point to an increase in revenue or market share price to justify their expenditure.

Whilst much research has focused on the risk to information security and the economics of technical aspects of information security, far less attention has been given to the critical human factors and their impacts on the ROISI. As a result, there is a poor understanding of the economics of IS within organisations and inadequate formulation and measurement of security policies in dealing with non-technical matters, including critical human factors. This lack of attention has also impacted upon decision-making in organisations, particularly around investment. This research presents a model that can provide a better understanding, reasoning and quantification of ROISI regarding risks associated with critical human factors. The model works by firstly providing an understanding of the dynamics by which threats engage with organisational assets and controls. One of the outputs is the ability to see how the risk varies as the control settings change. If a company can estimate the cost required to turn a control setting up one or two clicks and the model describes how the risk falls when the control is turned up, then it is straightforward to perform an ROISI calculation for each proposed change. The ROISI is the expected

reduction in harm versus the cost of the change. The classical and general ROI calculation looks like this [118]:

$$ROI = \frac{Gain\ From\ Investment - Cost\ of\ Investment}{Cost\ of\ Investment}$$

The traditional calculation is fairly straightforward when organisations are dealing with a well-defined tangible investment, where profit is evident and where revenue is greater than the investment. In information security, however, whilst we can calculate the total cost, there is no revenue to be made. Information security typically averts loss rather than generating profit from its investment. In addition, other elements such as risk exist within the information security field but are not traditional ROI concepts. A simple return on investment for information security can be calculated in the following way:

$$ROISI = \frac{(Risk\ Exposure \times \%Risk\ Mitigated) - Mitigation\ Cost}{Mitigation\ Cost}$$

Organisations tend to minimise risks that threaten information assets. The classical financial approach to ROISI is thus not specifically relevant in information security planning. The return on security investment becomes hard to determine when it comes to non-technical aspects of information security systems, including critical human factors and associated cost implications such as training. It is therefore extremely difficult to calculate and quantify all the costs associated with potential risks and damage resulting from SIs. In addition, it is very difficult to estimate the precise likelihood of the occurrence of those incidents due to the volatile, erratic, dynamic nature of the critical human factors and the way they fluctuate as well as the inconsistent nature of human behaviour. Furthermore, no reliable data is available to substantiate such estimations. Information security, cost and return on investment are all concerned with monetary value, whilst human factors are quite difficult to frame within financial metrics. As a result, human factors are not easily understood by senior management teams and boards of executives because they require some sort of quantification or metric in order to be useful in investment decision-making and other important corporation strategies. Despite this difficulty, human factors can be quantified; risk concepts are first identified before being modelled against the changes made to the control settings, satisfying organisational requirements for an estimation of the financial consequences of information SIs. This provides organisations with a more objective cost versus investment comparison, which considers a variety of risks.

Net present value (NVT)

One way of computing the ROISI is via the net present value (NPV) method, where Io is the 'initial investment for security' measure [118].

$$NPV = -Io + \sum_{t=1}^{T} \frac{\Delta \mathrm{E}\,(\mathrm{L}t) + \Delta \mathrm{OCC}t - Ct}{(1 + i\ calc)^{\mathrm{t}}}$$

I_0 = Initial investment for security measure
$\Delta \mathrm{E}\,(\mathrm{L}t)$ = Reduction in expected loss in *t*
$\Delta \mathrm{OCC}t$ = Reduction in opportunity costs in *t*
Ct = Cost of security measure in *t*
$i\ calc$ = Discount rate

Organisations receive recommendations for information security investments based upon the outcome of this model, depending on whether a positive or negative value is calculated. This model and most other proposals in ROISI consider a single security measure rather than an entire ISS [48]. It has also been noted that the NPV yields a time value for an investment [50] and, therefore, the ROISI performs for the time value of investment which, technically speaking, would be inflation and cost of capital, and it fails to represent all elements of ISSs conclusively.

5.3 Risk-driven investment meta-model

In order to develop a risk-driven investment model, it is necessary to understand the relationships among the actors within the organisational context. In particular, we need to understand the dependencies between the actors and other security, risk and organisational concepts and how they are addressed before confirming that the dependencies we have assumed are in fact correct. To achieve this, the research uses elements from Secure-Tropos modelling language and Requirements Engineering based upon risk analysis, actors, goals, security investment and SIs. The meta-model represents the underlying conceptual elements and relationships among the features related to ISSs and Information Security Risk Management (ISRM). A consistency is required amongst all features when all concepts come together. The conceptual meta-model outlines the abstraction in terms of which other models are defined. The meta-model for risk-driven investment incorporates some models without a similar abstraction level. It includes meta-concepts such as goals, security investment and SIs as well as relationships between these concepts, such as detection and prevention. Figure 5.3 illustrates the meta-model of the proposed risk-driven investment approach, embracing goals, security investment, risk, SIs and protection mechanisms.

Actor: An actor is an entity that has strategic goals and intentions within a system and organisational setting. There are both human and ISS actors. In particular, human actors are associated with several critical factors such as awareness, communication and the involvement of management, which have been discussed previously. An ISS actor is associated with factors such as security policy and physical security. With respect to ISSs, it can be said that any security system ultimately responds to the fundamental

relationship between various social and technical actors and stakeholders, including system users and potential attackers and hackers, in an organisational context. Strategic actors have goals, beliefs, abilities and commitments and at the same time are semi-autonomous, constrained by their relationship and dependencies, yet not entirely manageable. In addition, they are dependent on each other on the basis of the fulfilment of goals. Initially, one must identify the stakeholders who have concerns in the ISS, the proposed context and the framework, whilst also considering the ISS's purpose and function. This is important, as each actor would be affected by the proposed change to the ISS to ensure the security is served and how the actors' strategic interests, main objectives and goals would be influenced. In this study and the proposed model, the actors are users (organisations, systems, people) and potential attackers such as those planning SEAs. The attributes of both are considered, and exactly where they are closely and constantly dependent upon each other is elucidated. The next step will look at the different ways in which the actors would be able to achieve their intended goals. The proposed model details how the various control mechanisms and their different attributes should be defined based on the actors whilst addressing security constraints, and it presents cost and the return on investment clearly. Each actor's objectives are reflected in the proposed model. It is then essential to identify whether the actors' different interests supplement or interfere with each other. In this model, the organisational interest of cutting costs whilst increasing return on investment precludes increased spending on security and the implementation of improved measures to address the weaknesses related to the critical human factors. Potential attackers have their own interests too, particularly exploiting people in order to gain access to organisations' information and systems; these interests are in complete contrast with those of the organisation, its system and its people. It is important to identify the existing vulnerabilities.

Goal: A strategic objective of a stakeholder (actor) for a system and its surrounding environment. An actor seeks to achieve that strategic objective, regardless of how it is achieved. The way in which a goal is to be achieved should be agreed upon by all actors, with formulation and development shared amongst the parties. The proposed model differentiates between security and organisational goals. Organisational goals represent goals that are important at an organisational level. Such goals include profitability, compliance, continuity, reputation and performance. Security goals support security needs. This means a secure goal serves actors' and associated with goal [119]. Availability, Integrity, Confidentiality, Accountability and Auditability (AICAA) are the main security goals, as explained previously. An adequate balance in security can be obtained by exchanging security requirements with other functional or non-functional requirements of the security system that is equipped, according to the goal.

Risk: Risk is the potential damage resulting from some current process or future SI. Incidents can arise from information processes in organisations being maliciously exploited: a SEA is an example of such exploitation. Risk

is present in every aspect of an information process. The proposed model considers three different consequences of attacks: financial loss, which is difficult to quantify and can encompass either direct monetary loss in financial accounts or indirect loss as a result of business being disrupted; legal fines, which organisations could be issued as a result of a SI that violates their legal obligations; and reputational loss, which can arise from an organisation publicly reporting the SI to a regulator. Consequences of reputational loss include difficulties in attracting new customers and, in some cases, negative effects on the company's credit rating. For each asset group, risks can be calculated by measuring the asset against the threat to which it is vulnerable using a risk matrix with predefined values, enabling asset values to be compared with threat and vulnerability levels.

Security incident: A SI is an event due to the threats caused by actors using different means and tools to compromise the system. Possible causes of SIs include: internal system compromise, stolen customer data, phony transactions, insider attacks and DDoS attacks. SIs in this research pose negative consequences and create risks within the organisational context.

Vulnerabilities: A weakness in ISS procedures, design, implementation or internal controls could result in a security breach. Despite being patched by a control mechanism, a system always has vulnerabilities. This concept can be addressed by using the vulnerability assessment, which provides guidelines for protection mechanisms. It defines and classifies system resources, assigns levels of importance to the resources, identifies potential threats to each individual resource, develops a countermeasure strategy and suggests measures that can minimise the consequences of SEAs.

Security investment: The capital that is made available for security solutions via protection mechanisms in supporting a goal. Security investment is, in this case, not a direct measure of profit but of the cost avoided in potential human-related security incidents. Security investment should therefore consider both technical and non-technical cost implications. The reason for this is that the cost of preventive measures for SEA SIs is varied, and the landscape of threats and risks are ever changing. At the same time, other attributes require attention. These include Business Impact Analysis (BIA), threat description, vulnerability assessment, risk evaluation and risk treatment.

Plan: a workable long-term (strategic), mid-term (tactical) or short-term (operational) framework for realising goals, adopted and utilised by actors. A protection mechanism requires a plan to achieve ISS security and organisational goals by ensuring strategic security and SI improvements. Long-term strategy considers a human factor portfolio (involvement of senior management) and risk analysis. A mid-term (tactical) plan also concerns a human factors portfolio (awareness and communication) and tactical improvements such as enhanced maintenance and communication. The short-term (operational) phase of the plan is concerned with the allocation of critical IT assets, a human factors portfolio and security implementation practice.

Protection mechanism: a set of controls for addressing security strategy and supporting a security plan that entails a protection or defence mechanism. It can be detective or preventive for SEA SIs. It also protects information assets and assists in patching system vulnerabilities. It can be either technical or non-technical and is listed as part of security investment.

Figure 5.3 presents the meta-model that combines all the necessary concepts discussed previously. These concepts are linked with each other to support the analysis of SIs and associated risk so that appropriate control action and required investment in the control are determined within an organisational setting. Though concepts such as SIs, security investment and humans as actors all play a major role, the protection mechanism is the *core* concept. A protection mechanism relies on strategic planning to provide detective and preventive methods for dealing with SIs. It assists in the patching of vulnerabilities and protecting assets, which are mainly information (soft-intangible) assets though tangible and physical assets can also be included. Once the investment is configured, the detective and preventive control mechanism could potentially mitigate financial, reputational and legal damage. The mid- and long-term strategy also support the protection mechanism in addressing awareness, communication and management support for (human) actors. An actor has vulnerabilities that can be exploited and influence SIs. The introduction of such detective and preventive controls creates negative consequences in the system without adequate validation. To address these impacts, the system requires validation against SIs to establish the leverage of the incident and the resilience of the actor(s) in the system. If the validation is not justified, then the protection mechanism must be equipped to fill the gap in planning and investment.

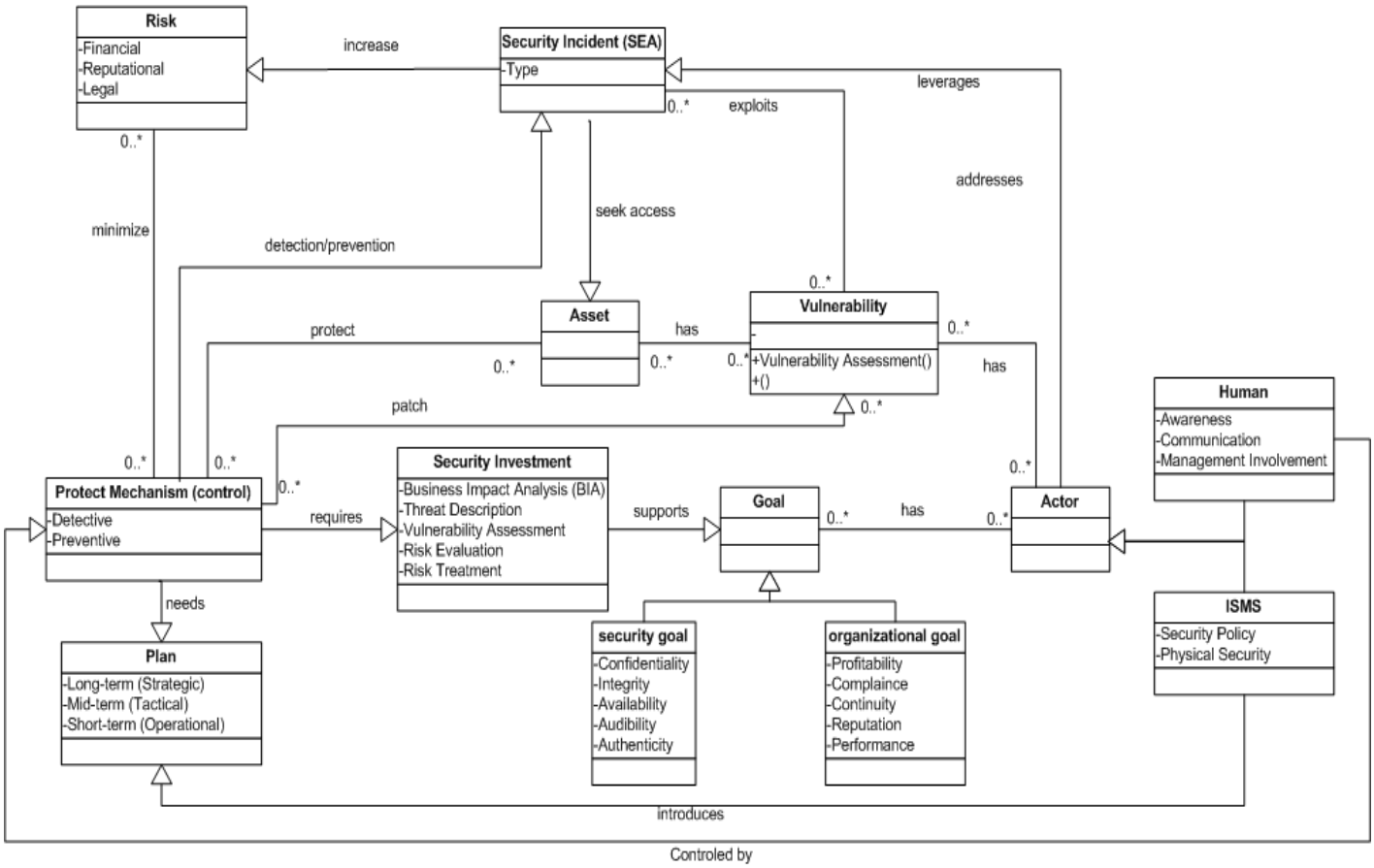


Figure 5.3: Risk-driven investment meta-model.

The figure provides a clear relationship between the concepts and their attributes.

5.4 Process

This section outlines the process involved in the risk-driven investment model. We have combined all discussed concepts used in the risk-driven investment model into a meta-model using Secure-Tropos and Requirements Engineering (RE) by presenting business, Security Incidents (SI), risk and Return On Information Security Investment (ROISI) related concepts [119] [120]. This process assists the development of the Risk-Driven Investment Model (RIDIM) by considering ISS concerns throughout the development lifecycle. Figure 5.4 shows a general form of the activity process that includes activity, function, step and attributes of RIDIM, with Figure 5.5 summarising the activities. Figure 5.6 outlines the steps within the process.

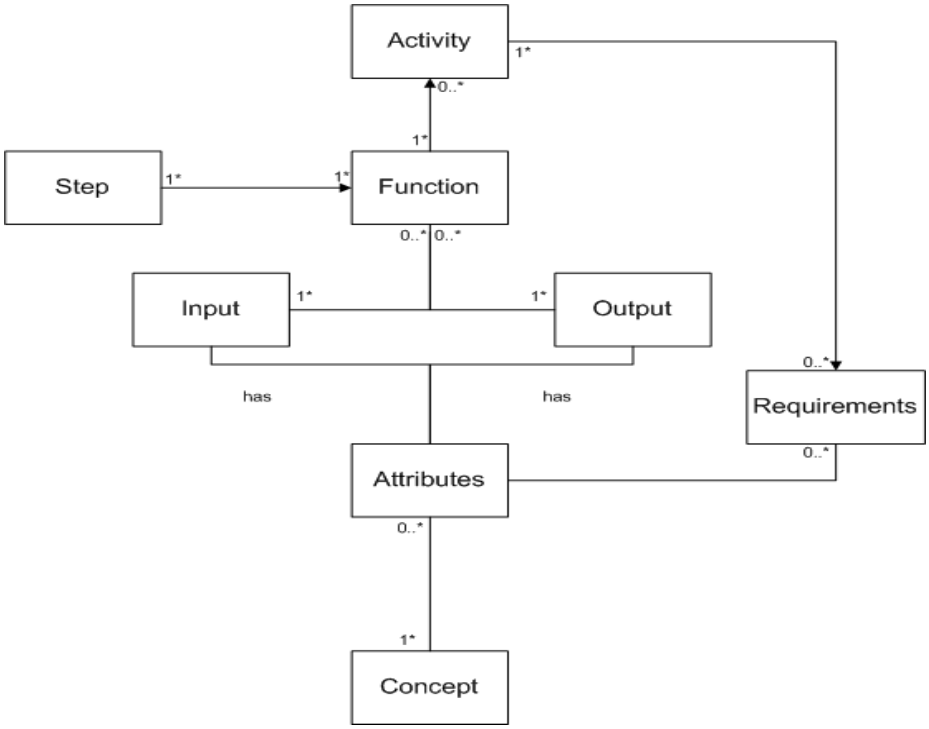


Figure 5.4: Activity process.

Risk-Driven Investment Process	
Activity 1 Identifying Business Domain	This activity focuses on analysing organisational entities such as actors, key process and goals so that appropriate incident analysis can be performed for calculating ROISI. It includes four steps: identifying actors, identifying key business process, defining organisational goals and defining security goals.
Activity 2 Analysis of the Incident	This activity analyses the incident and includes three steps: incident details, to determine the Risks and Severity of Incident and to develop security incident pattern
Activity 3 Gap Analysis	This activity provides an understanding of the fact that what control measures organisation require to have to ensure their conformity with regulatory bodies, the current situation and actions they require to take to ensure conformity.
Activity 4 Calculation of ROISI	This activity calculates the return of any security investment. It includes two steps, identifying potential control measures and calculation of ROISI

Figure 5.5: Summary of the activities.

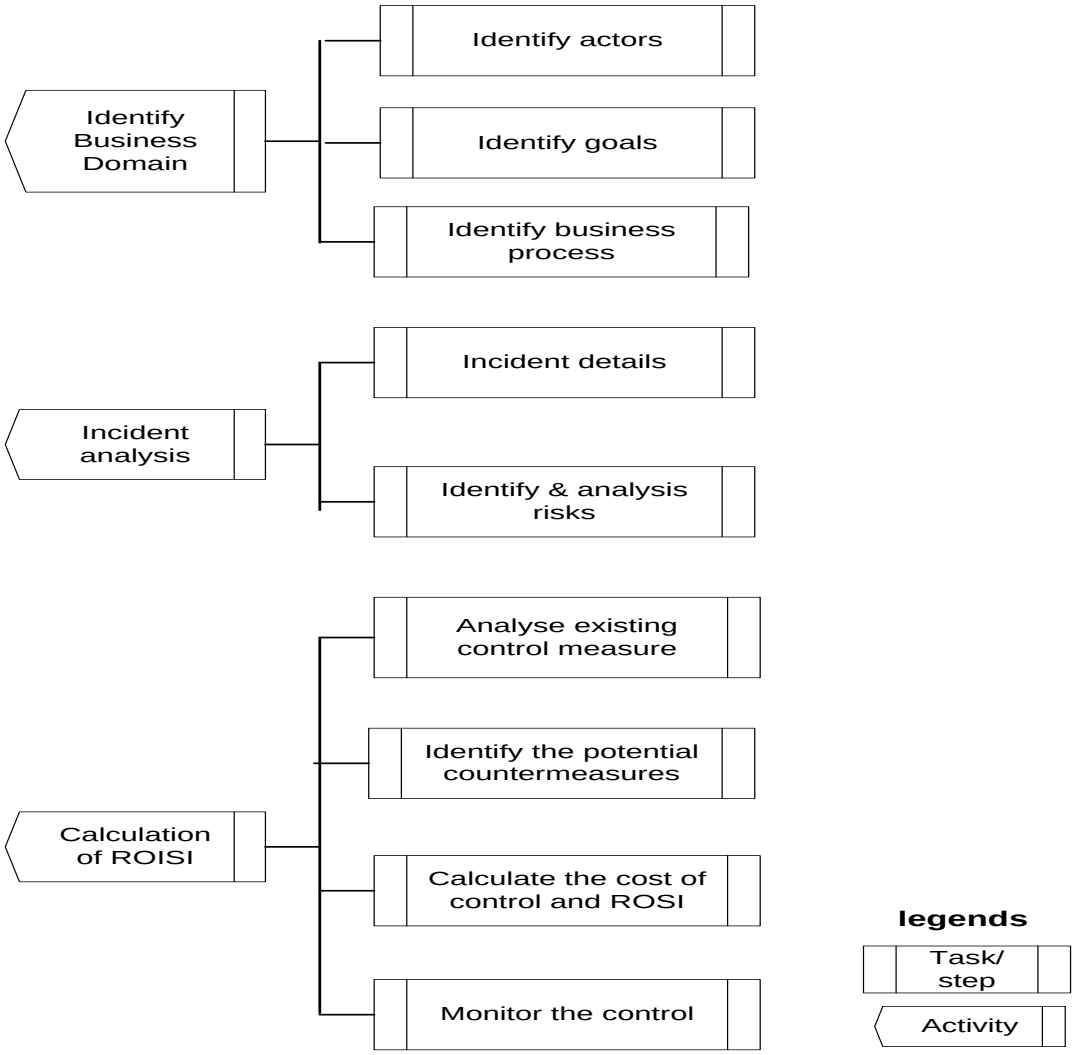


Figure 5.6: Risk-Driven Investment Process

5.4.1 Activity 1: Identify the Business Domain

This first activity of the process focuses on analysing organisational entities such as actors, key process and goals so that appropriate incident analysis can be performed for calculating the ROISI. The process of analysing internal factors within organisations includes four steps: identifying actors, identifying key business processes, defining organisational goals and defining security goals with regard to the ISS. This analysis facilitates the identification of factors related to the budget and the cost of security controls and mechanisms. Any project, including security projects in any public or private organisation, has to be justified for budget investment, whilst its success is often assessed subsequently. Organisational surroundings are as important as individual behaviour when an incident occurs [18]. Organisational analysis assists in the identification of information assets and leads to the development, documentation, implementation, evaluation and monitoring of the ISS, entailing procedures, standards, policies and recommendations that safeguard

confidentiality, integrity, availability, authenticity and auditability of such information systems and assets. The identification of information assets is the first step in securing them. As the measurement of information security performance and ROISI is driven by the reasoning of organisational factors, the three steps for this analysis are given below. At the end of this activity, an organisational entity artefact is produced. This artefact includes actors, business processes, goals and critical assets.

Step 1.1: Identify Actors

In this step we identify all actors, internal and external, within the organisational context using Secure-Tropos and Requirements Engineering. ISSs and people are internal actors described by their entities and specific strategic goals in an organisational context. An ISS provides two distinctive attributes: a security and a service model. The attacker is the external actor, an individual with an intention of gaining financial, political or/and personal incentives. ISO 27001/IEC proposes the founding of an Information Security Management System (ISMS) [20]. We follow these guidelines to define the activities and tasks of RIDIM. The backbone of the ISO 27002/IEC guideline forms an effective basis for ISS management support through several activities. Organisations should define their approach towards risk assessment in terms of the identification and documentation of risks. A uniform approach towards the evaluation, mitigation, transfer and/or acceptance of risks is needed. Senior management determines which security policies and controls are allocated to different sections of the business. Defining the boundaries and scope of an ISS is also important, as is the establishment of a security policy that requires management approval. Also crucial to an ISS is the formation of control objectives with a primary focus on the implementation of security policy and control activities. Security training provision, resource allocation, internal audits and monitoring and security program reviews are other key attributes of an ISS process. All ISS requirements are achievable when continual improvements are validated and insufficiencies are recognised. Shortfalls should be identified and developments instigated in order to gradually reduce the risk to the organisation.

Step 1.2: Define Goals

The goals incorporate the objectives, expectations and constraints of the organisational mission. This study considers organisation and security goals within the process. Providing the Availability, Integrity, Confidentiality, Accountability and Auditability (AICAA) of information assets are security goals for an organisation and critical factors for attaining its business goals. Senior management teams in all organisations commonly encounter difficulties in achieving organisational goals, whilst limited resources are available to them. Organisations seek to improve security to achieve their goals and objectives and thus they make an investment. Organisations should, however, be continually investing in information security as an ongoing process because threats are constant evolving and advancing. Decisions that are made about investment create value as they are

effectively business projects that are worth more than they cost. A detailed and complete understanding of the focus and scope of the risk analysis within organisations is thus essential, as is identifying the organisations' main assets in order to maintain and define organisational security goals and objectives. Assets are essential in the RIDIM model and help the entire risk analysis process in organisations. The assets are used to help in identifying risks with their value, and assessing their consequences and impacts in terms of pecuniary loss. A high level analysis of threats, vulnerabilities, incidents and mitigation process(es) should help to pinpoint what organisations are most concerned about and thus ensure that the focus of the analytical model is in line with organisational goals. It is very important to create a balance between organisational concerns and what is actually required in relation to security solutions and risk mitigation. Emphasis is placed on security architecture and the interplay of threat, risk analysis and security investment. Illustrated by practical and real-world examples of incidents, this discussion covers the subtle relationship between the exploitation of current and new mitigation methods, which consider human factors and investment, and the exposure to new threats, alongside organisational goals and objectives. Strong mitigations and countermeasures, which are attractive to organisations, and business decisions, which change the underlying assumptions in a way that invalidates the risk analysis, may threaten the viability of the organisational goals in a fundamental way.

Organisational goals and objectives with regard to security, risk, critical human factors and investment can be summarised as follows:

- Creating adequate balance between spending on information security and the effectiveness of security mitigation mechanism(s).
- Implementing a sufficient Threat Assessment and Risk Analysis to identify and clarify the severity of the risk and consider the right budget for the right cost.
- Aligning security and organisational goals to avert security violations, downtime and security-related costs and damages.
- Achieving security goals through training and awareness programs, which must be aligned with overall organisational goals and objectives, with the nature of the business and the culture of that organisation being considered.
- The effectiveness and adequacy of information security policies should be reviewed and re-measured against organisational goals to ensure that they are supported by the objectives of the organisation.

The result of a soundly executed mitigation process should thus be a set of recommendations closely supported by organisational goals. The process should identify important vulnerabilities, including critical human factors and architectural, design and conceptual weaknesses, as well as technical security mechanisms and tools, whilst providing a sound clarification on the return of investment in light of the business process. It should prioritise

the learnt vulnerabilities based on their likelihood of being exploited, cost and impact.

As security requirements are customer-oriented, it is important to overcome the redundancy, ambiguity and incompleteness of security goals by translating them into an analysis model that can be understood, defined and followed adequately and appropriately. The attainment of completeness by reducing redundancy is the main security goal. Furthermore, to lower complexity in subsequent organisational analysis activities, incident analysis, ROISI calculation and risk mitigation, the proposed model can be used to organise the requirements into a structure that reflects security goals. This study put Availability as the chief principle security objective for three reasons:

- Financial organisations are used as case studies in this research and the availability of the information system is the chief principle that ensures that the integrity and confidentiality of information assets are preserved. This doesn't mean that other information security goals are not important, but financial organisations cannot function if the system is not available and if the unauthorised access points and means for unauthorised modifications are not protected against. It would be very costly for a financial organisation if the system wasn't available in the first place.

- This research considers critical human factors and the role of people in ISSs, particularly in information SIs; therefore, availability is important to deter threat agents using communication means [3].

- Whether or not availability is prioritised depends greatly upon its impact on business. This becomes even more crucial as many financial organisations move their services to Cloud platforms, in which availability creates even more momentum.

Step 1.3: Identify Business Process

Business process can be defined as a service covering a business operation from start to finish that is provided to internal and external stakeholders and other interested groups. In an organisational context, the business process is a functioning process supported by and linked with ISS practice with respect to goals and objectives. An ISS operation is a composition of a business process and a compliance-imposing mitigation and control mechanism. The process includes the identification of required information and sensitivity of information for business continuity and disaster recovery. The protection of sensitive information is one of the greatest concerns for today's businesses; therefore, this step also identifies the critical assets that support the organisational missions and thus require appropriate protection.

At the end of the activity, the main outputs are actors, security and organisational goals, which all define the business domain of the business process. This gives a clear indication of the players and other concepts related to the process of the RIDIM model. The choice of financial organisation has been influenced by a number of factors, one of which is that financial organisations are highly appropriate for investigating the dynamics of evolving relationships between human factors, risk and investment in information security systems.

5.4.2 Activity 2: Incident Analysis

Once the organisational business domain entities are identified and analysed by the previous activity, incidents instigated by the critical human factors are then analysed in Activity 2. The main goal of the incident analysis process is to assist in remediating any loss that may have occurred to organisations and minimise the damage sustained by similar incidents in the future.

Step 2.1: Incident Details

When an incident occurs, it is crucial to know what to do, how to gather detailed evidence of the incident that meets legal criteria, and how to deal with the consequent regulatory, financial and reputational issues. It is, however, is imperative that incidents be reported promptly to allow the issue to be analysed and addressed and reduce any further risk. For this purpose, this first step advocates the following activities, known as 3R:

- Reconstruct attacked systems, fixing any security vulnerabilities that may have instigated the incident.
- Restore backup data and, if required, replace data of questionable integrity.
- Reinforce current security controls and, if needed, address issues identified during the SI analysis.

To fulfil the above steps, the details of incidents must be discussed in different sections.

1. **Description of the Incident:** What was involved in the incident and what were the network capabilities and security procedures? What was the impact on the network and computer systems?
2. **Threats/Vulnerabilities/Risks**: Identification of the incident: Has the situation been acknowledged as malicious? Notification process and interaction: Have the right people been notified and in a timely manner?
3. **Cost/Investment**: Business impact: What services were impacted, how fast were they reinstated, and what did that mean for the organisation?

4. **Root Causes of Incidents**: Technical and non-technical aspects of incidents: Why did the incident happen?
5. **Gap Analysis:** Identification of gaps in the information security system, scrutinising existing controls and root causes.

Description of the Incident

The description of an incident provides answers to a number of related questions. The main issues that require an explanation are:

- The time that taken for the organisation to find out that an incident had occurred;
- The process used for the detection of the incident;
- The sufficient identification and explicit understanding of the incident and its process;
- The nature of the incident and the role of critical human factors; and
- The estimation/calculation of the impact on the system.

Threats/Vulnerabilities/Risks

Following a description of the incident, this section assists in determining what vulnerabilities of the system can be exploited by such a threat and what risks are involved. Investigating the incident should provide information on how the system has been compromised despite existing control mechanism(s). Whilst the appropriate controls can be subsequently patched, employees need to be trained in email and phone authentication methods to detect invalid and hoax communications. In order for further risk to be mitigated and vulnerabilities to be minimised, the appropriate person/department should be informed as soon as possible about the incident. Also, a timely, accurate and adequate report to IRT should be made available to them. It is vital to identify the weak links and any known internal factors that may compromise the risk evaluation and the subsequent recommendations: These are the vulnerabilities in the risk analysis/mitigation process. Although a good knowledge of threats helps one in modifying the countermeasures and controls, vulnerabilities and consequences/impacts must be given consideration in the process before risks are rated. Threats are always present and risk may be higher than it appears; organisations need to be aware that they are vulnerable to things that are difficult to predict or imagine. Risk analysis is a process that incorporates three components: Threat, Risk and Vulnerability. These components should be defined on the basis of the organisations' assets that need to be protected and how vulnerable the organisations are to different threats. The likelihood and possible impact of a threat is then considered. Finally, consideration is given to how the organisation can reduce the likelihood of threats occurring and minimise their impact.

Cost/Investment

This step aims to identify the investment organisations are required to make in order to deal with SIs. Looking back at the incidents discussed previously, it becomes clear how extra investment in training on authentication methods in communication could enhance control mechanisms. Important issues related to cost and investment and business activities and objectives are listed below:

- Analysing the impact of the incident on the business.
- Identifying the services affected.
- Identifying the role of people in the incident, which enables more comprehensive and tailored training to be developed.
- Identifying if the use of different technological solutions, such as applying a different network topology with more redundancy in its server, could have lessened the impact of an incident.
- Analysing the Business Continuity Plan (BCP) in order to find out how quickly the service was restored
- Identifying the severity of the impact on the brand and customer satisfaction.
- Identifying if there are any legal implications of the incident.

Considering the above issues, it becomes apparent that providing a good balance between cost and security is essential. Organisations require a robust clarification and justification of security benefits and associated costs incurred. They need to consider investing in the security of their information assets whenever the fiscal cost is less than or equal to the benefit of the security measure(s) [121]. There are various tools that assist organisations in effectively managing information security cost and investment configurations, using various metrics for accurate and up-to-date information given to management. The business dashboard, despite not being directly related to information security, can be used or tailored to fit into an organisation's risk framework, and it can be a valuable tool that provides senior managers with a glimpse into the likely impacts of insufficient security investment.

Root Causes of Incidents

The main cause of the incident discussed above was the deception of an employee by an infected e-mail and hoax phone call. If the control mechanism had been able to detect socially engineered activities, then this attack could have been detected and dealt with appropriately and adequately. The performance of a control mechanism can be analysed using an incident response process, implemented by the organisation's Incident Response Team (IRT). The analysis is concerned with several aspects:

- The preparation of an adequate reporting procedure to inform the IR team.
- The IRT's communication procedure.

- Incident handling.
- Ensuring that the IRT receives relevant and adequate information.
- The IRT should reach out to appropriate people such as managers, technical specialists and legal teams and received adequate support from said individuals.
- The IRT should reach out to all appropriate external organisations such as government agencies.
- Sufficient and timely communication should be established between all stakeholders.
- Correct diagnoses of the incident.
- The formulation of a rapid and appropriate response.

Establishing the root causes of an incident requires a level of understanding beyond that of merely detecting that a system is infected; it requires an understanding of precisely what allowed and facilitated the compromise of the security system. In addition, the difference between the root cause and the trajectory of the compromise must be considered. Identifying root causes provides an understanding of the way malicious activities succeed in compromising systems, whilst finding the trajectory, or path, of the attack assists in understanding the delivery of the attack. There is a profound difference between these two goals. Consider an attack scenario in which the server is compromised by a Command & Control attack as the result of the payload of a RAT. The attack path describes how an employee was deceived to deliver a RAT payload. If the organisation then blocks the C&C attack and address the specific RAT payload, there is nothing stopping another similar attack occurring another day. The root cause, on the other hand, considers the human factor vulnerabilities and the role they played in delivering the payload. In order to identify the root cause, the sequence of events must be fully understood by reconstructing exactly what happened in the process of the SEA. A forensic investigation into the details and a reconstruction of what occurred provide precise answers to queries relevant to the incident. The role of human factors in this regard can be identified and the root causes of the incident subsequently addressed.

Gap Analysis

The gap analysis provides an understanding of which control measures organisations require to ensure their conformity with regulatory bodies. However, there are limitations in the gap analysis process. Human factors are part of the gap analysis and they have a subjective nature. Addressing some goals related to this subjective matters is quite difficult as they may evolve and change during the sequence of finding solutions. The nature of human factors themselves brings another challenge. There may be several alternative solutions available, making for a highly flexible process. A well-executed gap analysis can deliver the organisation with guidelines for conformity.

This research considered a number of gap analysis techniques and methods to compare its approach to the industry benchmark. One very appealing

cyber security analysis tool is that used by Lockheed Martin. However, this analysis doesn't provide a full and comprehensive approach to critical human factors and security investment. Without consideration of critical human factors and security investment, such analysis lacks a comprehensive understanding of related risks and their impacts.

Step 2.2: Identification and Analysis of Risks

Organisations want to better combat complex threats and comply with heightened regulatory demands. They are improving security efforts by forming viable risk management programs that measure improvements in information security posture. Risk analysis combined with decision-making around addressing those risks forms risk management. Determining risk severity is part of the risk analysis process. This process allows senior management to determine whether they have met their due diligence responsibility when making a decision. This decision could be about a new project, capital expenditure, investment strategy or other business processes such as the modification and/or establishment of new information security control measures. Risk analysis should be used to maximum effect to complement risk management decisions, which aim to assess the extent to which due diligence is being employed and provide adequate information security controls. Due diligence has a number of different definitions based on the nature of the business. How due diligence is measured depends greatly upon the relative facts of each case. Risk analysis also addresses intangible and subjective contributing factors, such as the role of critical human factors or conformance.

As defined above, risk is the combination of threat, probability and impact stated as a value in a predefined scope. A risk matrix has been introduced in which the probability and impact has been given a quantitative scale. The risks, root causes, owner of the risks and mitigating actions are defined and explained in this assessment. Inherent and residual risks are demonstrated quantitatively. At this point, the risk register session is complete with an overview of the risk assessment process. This process then requires a review of the business attributes, namely Availability, Integrity, Confidentiality, Accountability and Auditability (AICAA), in order to identify and examine the threats. It then identifies any existing controls or safeguarding measures in place. When that process is complete, each threat is examined to determine its probability of occurrence and impact to the business process. In this research, each threat was examined using the existing control as a guide to assign a relative risk level to each threat. Once the risk levels were established, possible controls were identified that could reduce the threat risk level to an acceptable range. The output of this activity is an incident pattern that includes the results of the 'incident details' and 'risk analysis' steps. Table 5.1 shows the incident pattern and describes its attributes.

Incident components			Description
Incident Name			The incident that occurred within the organisation
Incident details			Incident details including sequences of events during the attack.
Incident-Related Concepts	Asset		Affected tangible and intangible asset(s)
	Vulnerability		Weakness of the system and organisation.
	Risk		Affected areas due to the incident, e.g. financial/ reputational/ legal
	Actor/ causes	Human	Human factors related to the incident such as awareness/ communication/management involvement.
		ISS	Related organisation issues such as security policy, physical security etc.
Investment-Related Concepts	Protection Mechanism		Existing protection mechanism
	Business Impact Analysis (BIA)		Understanding impact criticality, identifying business functions, gathering impact data, determining impact, BIA data points.
	Gap		Considers the effectiveness of control measures and the gap in existing control that facilitated the incident. Looks at the risks, vulnerabilities and control measures.
	Risk Evaluation		Level of risk due to the incident, i.e., high, medium or low.
	Risk Treatment		Refers to the plans to mitigate the risk.
	Goal	Security Goal	Security goal needed to be achieved to overcome the incident, e.g. Availability, Integrity, Confidentiality, Accountability and Auditability (AICAA).
		Organisational Goal	Organisational goal needed to be achieved to overcome the incident, e.g. profitability, compliance, continuity, reputation, performance.

Table 5.1: Security Investment-Incident Pattern (SIIP)

SEA security incidents have now been defined, categorised and determined. Their pattern behaviour, their related concepts such as vulnerability and threat and, more importantly, the risk concepts and consequent risk assessment, analysis and treatment have also been identified and defined.

The next activity in this research involves analysing the gap in existing controls and defining the control measure elements for the economic analysis.

5.4.3 Activity 3: Calculation of ROISI

Once the incident is properly analysed, this final activity calculates the return on any security investment and contributes to the enhancement of existing ISS practice, mainly in terms of human issues. It is therefore important to justify whether greater security investment is necessary in light of an incident occurring. This activity consists of four steps.

Step 3.1: Analysing existing control measures

This step analyses the existing control mechanisms within an organisation and evaluates their effectiveness at repelling SIs. In particular, the measured effectiveness determines the gap in existing controls and missing necessary practice. This gap is briefly identified in Activity 2. The control measures considering human factors are varied and change from one organisation to another, depending on organisational culture. However, there are common controls that can be shared in any organisation. One of the major contributing factors for setting up the human factor-related controls is a culture of security. This is followed by security policy, security awareness, contracts of employment, service contracts, end-user codes of conduct, segregation of duties and third-part and contractors' obligations.

It is also necessary to estimate the loss incurred by an incident. Each loss is accompanied by a cost. The loss is associated with the details of the incidents' transactions, such as assets used in business or lawsuit settlements, whilst cost affiliates with the expenses to provide security control measures. The loss of assets includes tangible and intangible assets [122]. Losses in a SEA can therefore be tangible and intangible, both of which have financial impacts on any organisation, depending the service they provide. Losses can occur in:

- Access to the system
- Revenue
- Data availability
- Data integrity
- Data confidentiality
- Reputation

The main costs of an incident are:

- Increased insurance premiums
- Administrative expenses (extra training, internal cost-auditing)
- Time (availability of data and system)
- Hardware and software costs (external cost)

- Implementation costs (customisation, consultation, training, testing and communication)

The incident profile will be completed when the control mechanisms are identified and introduced. However, the exiting control measures must first be identified and then categorised against the valuation criteria. The different types of control measure are given below:

- Security policy
- Security awareness
- Contracts of employment
- Service contracts
- End-users' codes of conduct
- Segregation of duties
- Third-party and contractors' obligations.

Finally, it is necessary to determine the effectiveness of a control measure based on the following scales:

- Effective
- Ineffective
- Adequate
- Inadequate

Measuring the effectiveness of controls is challenging. The above scale can be measured against established guidelines and current controls.

Table 5.2 illustrates the details of the security control measures:

Incident (I_n)	**Causes (C_n)**	**Frequency (F_n)**	**Severity (S_n)**	**Loss (Ln)**	**Cost (Co_n)**	**Control Mechanism (M_n)**
I_1	C_{n+1}	F_1	S_1	Ln_{+1}	CO_1	M_{n+1}
I_2	C_{n+2}	F_2	S_2	Ln_{+2}	CO_2	M_{n+2}
I_3	C_{n+3}	F_3	S_3	Ln_{+3}	CO_3	M_{n+3}
I_4	C_{n+4}	F_4	S_4	Ln_{+4}	CO_4	M_{n+4}
I_5	C_{n+5}	F_5	S_5	Ln_{+5}	CO_5	M_{n+5}

Table 5.2: Existing control measure.

The table provides information about an incident, providing information that will later be used in the return on investment calculation. It shows the cause, frequency and severity of an incident and the subsequent loss expected, leading to the introduction of a control with a specified cost.

Step 3.2: Identify the potential control measures

Once the existing control measures are analysed, it is then necessary to identify the possible actions based on the risks and review of the control

measures. This step identifies one technique that can be used to identify potential countermeasures for addressing the causes of incidents and the damage done to the existing defence mechanism. It is clear that the existing control measures do not work and that the system requires a review or the introduction of new control measures. The value of reviewing a system or providing new controls is directly related to the loss caused by the incident. Technically speaking, how much money is at stake? In addition, the review strategy should reside within a regulatory framework and be appropriate for the size and business nature of the organisation. It should also consider the business continuity and disaster recovery plans as well as the frequency and severity of incidents. Potential control measures should therefore determine potential problems in the implementation of the current risk management structure. This can be followed by the identification of any shortfalls in the information security system. It is also important to understand the risk mitigation process and the necessity of adequate investment in security. In addition, the reputation of organisations is important, and potential control measures should consider it. Reputation has the potential to be very badly compromised in security incidents.

Existing Control Measures

Current protection mechanisms rely mainly upon various security standards such as ISO27001, in which training and awareness programs are considered [20]. However, there are two important avenues that have not been considered thus far. Firstly, the nature of attacks are changing in line with changes in the type of technological devices and online services commonly used, e.g. mobile devices and the move from local data storage to the Cloud. Secondly, some elements of human factors become more important than others due to the remodelling of communication technology. Factors such as communication and support for management teams in the context of ISSs in organisations are as vital as training and awareness programs.

Step 3.3: Calculate the cost of a control and ROISI

This step calculates the cost of proposed controls so that management can determine the benefits of the investment. It aims to optimise the trade-off between the expected attack losses EA(L) and the cost of economical capital CE(C) on the one hand and the investment in information security controls IS(C) and investment in insurance I(I) on the other. Thereby the suggested capital to be invested in information security control mechanisms will be optimal. Based on this, the total negative liquidity can be shown as:

$$NL(T) = EA(L) + CE(C) + IS(C) + I(I)$$

In order for the ROISI to be accurate, the above concepts should be expanded to provide more detail into the losses and costs involved. To calculate the return on investment in information security, the following must be considered across three different stages: stage one involves the calculation of the cost of a single expected attack in an incident; stage two

involves the calculation of the risk exposure factor and risk reduction, taking into account security control measures and insurance and assuming that that security controls and investment in an insurance policy reduce loss; stage three involves the calculation of the ROISI in an absolute quantity, based on the annual cost of protection, insurance and other costs.

Prior to stage one, the preliminary expected cost should be computed from the following parameters:

- External Services Cost ES(C)
- Purchasing Cost P(C)
- Employee Cost E(C)
- Administrative Cost A(C)
- Legal Costs L(C)
- Other Costs O(C)

Therefore, the total expected cost of an attack TEC(T) would be:

$$TEC(T) = ES(C) + P(C) + E(C) + A(C) + L(C) + O(C)$$

It is also the loss of the revenue from both existing (L1) and potential customers (L2). The Total Revenue Loss RL(T) can be calculated as follows:

$$RL(T) = L1 + L2$$

One can now begin stage one, in which the following parameters are considered:

- Single Expected Attack Loss (SLE)
- Total Expected Cost of an Attack TEC(T)
- Insurance Claim IC(I)
- Revenue Loss from existing/potential clients RL(T)
- Average Margin AM(A)

$$SLE= TEC(T) – IC(I) + (RL(T)) * AM(A)$$

After the single expected attack loss has been calculated, one is then able to calculate the annual expected attack loss based on the likelihood (L) of the SEA occurring. This can be performed using the following formula:

$$ALE = SLE * L$$

Step 3.4: Monitor the control

This final step is uses to evaluate whether the revision or establishment of new countermeasures can reduce the risks and prevent the causes of the

attack. Therefore, if the new countermeasures weren't able to prevent the causes of incident then we require introducing another set of countermeasures.

Technical and non-technical costs of incidents

SEAs have both technical and non-technical cost implications for organisations. The technical costs of SEAs are varied, and they inspire such inconveniences as having to update all current network patches and dealing with phishing emails, insecure mobile devices and cloud security issues. Non-technical costs of incidents include the need for re-training and re-programming awareness materials, amongst other training-related matters. The link between the cost of an incident and new investment becomes clear after the loss due to a single expected attack is analysed. However, the dependency between the cost of an incident and new investment relies on there being a high likelihood of the attack, whilst the possible attacks could be even more financially damaging and disruptive to the organisation. This will push the cost of new investment much higher than cost of an incident. It is proposed that this should be monitored and controlled by the incident response team, who have the capacity to deal with it to contain financial burdens.

Determine benefit

Clearly the benefits of preventing SEAs become apparent for any organisation of any size. Identifying the explicit benefits of a preventive model for SEAs, which needs to be deployed, are essential. Considering the discussed RAT incident above, the benefit of providing an adequate understanding of the complexity of SEA attempts become very evident. The key benefits of SIRM are: fast and quick preventive measures for SEAs attempts, more efficient user experiences when dealing with e-mail and phone communications and reduced support needs.

Investment

Organisations must invest in all aspects of IT to deal efficiently and adequately with SEAs. The key investment points are: training, upgrades and more detailed classifications of data and information.

Conclusions and Key Findings

The most challenging objective of an ISS is to support the organisation in meeting its business objectives. The ability of an ISS to achieve this is dependent upon the usefulness of its metrics in delivering the effectiveness of security projects and controls in fulfilling their business requirements. In addition, an effective justification of the return on investment with a measurement of cost for achieving the security level being validated was presented. The calculation of ROISI is an important metric to track. Such security metrics can assist in monitoring the controls by translating them in terms of direct and indirect effects on the organisation in various capacities.

These effects include the interruption of critical systems, regulatory conformity and reputational impacts. In addition, the ROISI metric helps to improve the organisation's effectiveness at dealing with mature threats as well as enhancing security controls against emerging threats such as SEAs and other SIs. Apart from meaningful ISS metrics and ROISI calculations, monitoring the control measures assist in the monitoring of vulnerabilities and the reduction of them in a timely manner. It also considers how the organisation's assets are impacted by SIs. ROISI calculation can be used to evaluate the effectiveness of the security controls, though because organisations have different objectives and strategies it is quite hard to use such an approach. One of the key objective of an ISS is to determine the value of the assets that they are protecting. Without ROISI metrics, organisations would risk spending more on protecting assets than the value of the assets themselves, which would effectively yield a negative return on security investment.

5.5 Conclusion

The Risk-Driven Investment Model (RIDIM) uses security incidents and their related risks as well as the cost and return on investment of such a cost to propose adequate control measures. The underlying process of holistically modelling risk, SIs and investment is provided in detail by this research. This approach systematically uses SIs with a combination of risks, critical human factors and security investment consideration and integrates such activities into Requirements Engineering. Compared other studies, this is a unique method. The business-related domain was identified before SI concepts were analysed. The risks and security investment concepts were then defined and a process in which the existing and potential control measures are considered using gap analysis was proposed. The outcome of the gap analysis was an identification of the security incident pattern.

CHAPTER 6

Evaluation and Discussion

Contents

6.1 Overview

This chapter focuses on the evaluation of the proposed risk-driven investment model, assessing the strengths and weaknesses of the RIDIM and its applicability to the ROISI. The evaluation uses an empirical investigation method involving case and survey studies as shown in Figure 6.1. Data is collected and analysed systematically through two case studies and a survey. A calculation of the ROISI is provided to analyse the effectiveness, scalability and usability of the RIDIM, in addition to gauging its practical applicability. Finally, the evaluation appraises the ability of the research contributions to answer the research questions.

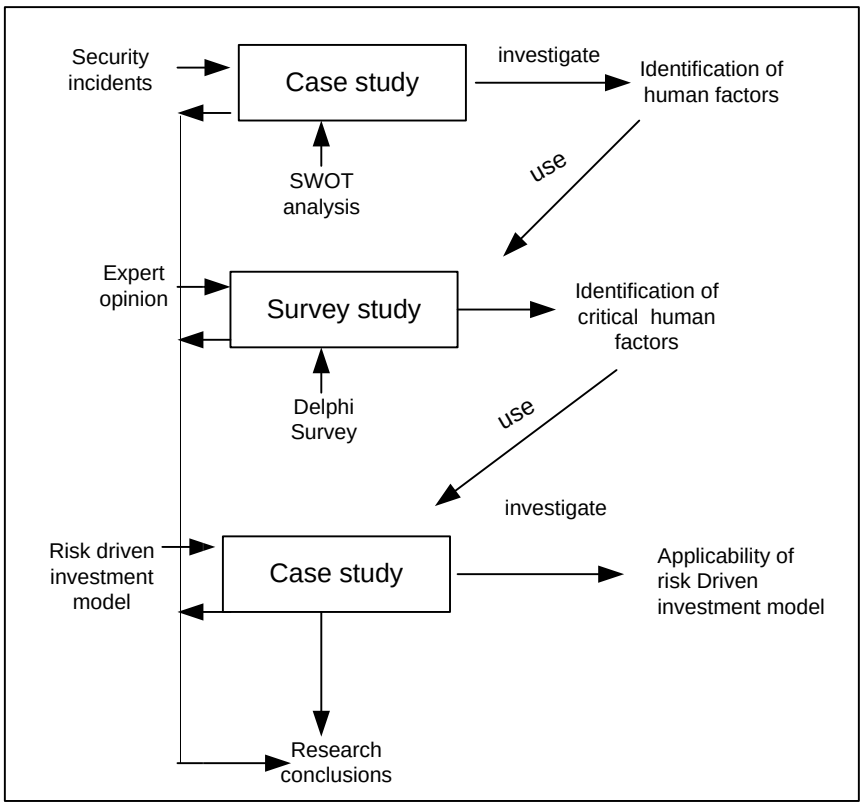


Figure 6.1: Evaluation of the research using an empirical investigation.

6.2 Empirical Evaluation and Data Collection

This research selected an empirical approach for its evaluation of the main contributions of the study. There is increasing demand within the information security field for the contribution of empirical studies, as they are thought to be effective in enhancing knowledge [123]. In the information security domain, it is hard to choose a suitable empirical method that is well qualified for a specific research context. Information security concerns a number of disciplines and grapples with the ever changing nature of technology, information system knowledge, the rigorous and subjective nature of human factors, security incident ramifications and many other ambivalences and social and organisational constraints [124]. The empirical study has been confirmed to be an efficient research method for collecting relevant data to examine issues such as security incidents in the information security domain, in which it supports the benchmarking of information security investment and analysis of human factors [125].

The combination of survey and case study research methods was nominated for the evaluation of the proposed approach in this research. In the domain of information security, these methods have been commonly used [126]. The techniques enable one to obtain data on the impact of critical human factors, risk and ROISI in relation to RIDIM. This method of collection relies on parameters such as business domain, risk management information and control over the variables of interest such as

risk assessment, risk register and risk control [127]. This study confirms the applicability of these parameters and provides a fairly accurate understanding of the role of human factors and their related risks. Qualitative data from participant questionnaires, interviews and brainstorming sessions has been analysed to comprehend the study result.

The data collected mainly comprises the answers of participants to the open and closed questions posed in the survey and case study. In particular, a set of closed questionnaire and semi-open interview questions are used for the data collection. The closed questions are concerned with the critical human factors, and are used to analyse SIs. The semi-open questions are mainly descriptive and comparative and are used to identify the participants' perceptions of the ISS and related concepts such as cost and investment and critical human factors as well as the advantages and disadvantages of the risk-driven investment approach. A letter of consent was provided, which required the signatures of the participants. The SI case studies explore the role of critical human factors and assist in the calculation of the return on the information security investment. Figure 6.2 shows a process for implementing and evaluating the RIDIM model; this process is the output of the activities described in Chapter 5.

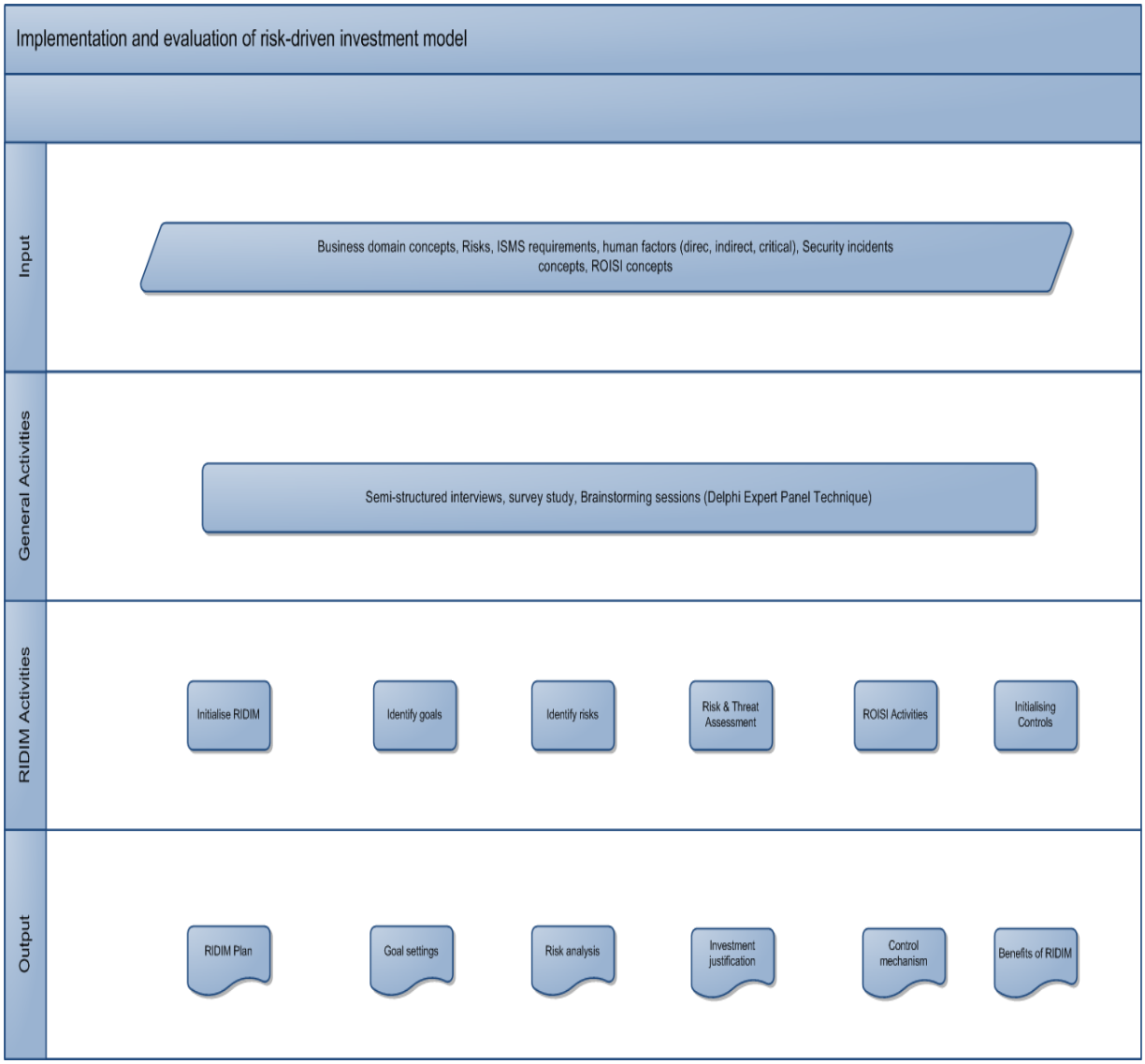


Figure 6.2: Evaluation details.

6.3 Challenges of empirical studies in information security

As the research findings indicate, there are difficulties in applying a comprehensive risk-driven investment process to an information security project. For instance, a recent survey study showed that one of the main reasons why ISSs are not always employed is cost [48]. Some information security practitioners do not consider ISSs process attentively, whilst others lack adequate knowledge and experience to perform ISS activities [10]. This research has identified some challenges in conducting an empirical study in the information security domain:

- Information security assignments have a fixed-period development lifecycle due to constant pressure being applied from the organisations'

boards of directors, who are concerned with time, cost, regulatory regimes and quality control. A full and wide-ranging ISS is not achievable on all occasions and in all organisations. During the development process, it is not always possible to identify and monitor all activities such as risk detection, planning and threat assessment. In addition, critical characteristics of human factors and difficulties associated with presenting a figure-based report to the board within a running project create more challenges and difficulties. This leads to limitations in the availability of data for the validation of the empirical study.

- Many organisations and their employees lack the motivation to understand and perform information security risk management. They view security as a hindrance, rather than an enabler, that creates extra and unnecessary activities. The absence of such drive and understanding threatens the validity and reliability of the result of an empirical study because the data gleaned is consequently less reliable.

- Because human factors, which greatly affect ISSs, are very subjective matters then, by nature, information security risks become subjective issues too. There are many uncertain variables in the security risk-driven process that can be either undervalued or overvalued. Furthermore, organisations have different cultures and expectations, which makes each individual information security project unique. Such uncertainty and ambiguity impacts the data, restricting the assessment of the effectiveness of the security risk-driven method.

Only a handful of research focuses on the use of risk and security investment management methods in ISS projects.

6.4 Study Setup

In order to present the extent of the validity of the proposed approach and its relevance in the context of this study, four study setup stages are provided. In any empirical research method, it is necessary to present a detailed overview of the study and affiliated measurements to be defined [128]. This offers an accurate conceptual characterisation of the facts that, if absent, could prompt an incorrect conclusion about the framework. In addition, many studies in the field of information security attempt to quantify facts and situations that are inadequately understood. This can impact significantly upon the soundness of the study result and quality of the whole study; therefore, to ensure clear and unequivocal findings, the study setup must be precise enough to allow the study to be analysed in a thorough and orderly manner.

The main focus of this evaluation is to identify the impact of the risk-driven security investment model on the effectiveness of an ISS project, particularly the effectiveness of an approach in attaining overall project goals and negating the impact of critical human factors. However, presenting a precise quantification of the study setup is a fairly challenging

task because of the difficulties involved in implementing comprehensive RIDIM activities into the ISS project. It is important to mention that the shortage of empirical data in the IS field also contributes to this. This research considers four main study setups, which are appropriate for the proposed approach. This ensures a more accurate output of the empirical evaluation.

• **SWOT techniques for identifying main human factors:** The first study evaluates the characteristics of the main human factors. It focuses on the input used and the interviews conducted in the approach. The scalability of using a SWOT technique is analysed. The initial survey and interviews in this empirical study identified the main direct and indirect human factors associated with an ISS project. The case study results specified the subjectivity associated with the main human factors.

• **Delphi expert panel technique for prioritising critical human factors:** The second study focuses on the prioritisation of the main human factors by analysing the result of the Delphi technique. The main incentive of the proposed method is to develop an accurate account of the critical human factors in an ISS project. It specifies the characteristics-related factors.

• **Calculating the ROISI:** The third study emphasises the use of a case study to calculate the return on information security investment. The main benefit of this approach is that it allows a correct estimation of the return on an investment to be calculated and its association with the financial impact of the critical human factors in an ISS project to be determined.

• **Overall RIDIM activities:** The fourth study focuses on the integration of the risk-driven security approach into ISS development. It focuses on several concepts such as risk, threat, investment and business and security goals.

6.5 Case Study 1: Identification of Human Factors

This section presents a case study and its result: the identification of human factors. We use two real incidents that occurred in two organisations. A confidentiality agreement was required in order to present the incidents anonymously. The main goal of this study is to:

- Identify a list of human factors that impact on information security management systems.
- Analyse the incident based on human factors using SWOT.

To achieve these goals, two assumptions were formulated:

- Human factors (direct and indirect) are one of the main causes of information security incidents.
- Information security incidents undermine the effectiveness of an ISS.

6.5.1 Incident Context

As stated previously, two incidents are considered for the case study. This section presents the incidents.

Incident 1

This incident concerns a financial organisation. It was one of the most consequential security breaches with regard to data protection. It attracted the attention of all information security professionals. The security breach highlighted the issue of organisational failings in handling very complex issues where people and technology are concerned. In this particular case, customers' confidential information was transferred from the organisation's headquarters to another centre on portable devices, and the information was not encrypted. The devices went missing and all the information was lost. This method of data transfer had been a regular practice in the organisation. The organisation's information security policy required portable devices carrying information to be encrypted. Despite the policy being in place, most of the portable devices, including CDs and USB memory devices, contained unencrypted information. This failure to conform to policy had not been picked up in any auditing and risk assessment sessions.

Incident 2

This incident also occurred in a financial organisation, and it involved the exposure of system vulnerability. Once again, the combination of people and technology failed to match up, leading to a situation similar to that in the first incident. Unencrypted information was sent by post to a third party and all the backup information was corrupted due to a hardware failure. According to the Financial Conduct Authority – the FCA (Formerly Financial Services Authority - FSA)- due to a lack of training staff were unable to identify the potential risks. In this incident, there were two important factors that lead to the exposure of the system and a security breach. First, encryption had not been carried out and information handling breached security policy and procedures. Poor training and awareness programs were blamed for the incident, as well as a lack of enforcement of the security policy. Secondly, the hardware failure led to the temporary loss of backup. The security policy was responsible for the absence of a contingency plan for disaster recovery and a business continuity plan. Both organisations were fined heavily by the regulatory authority, and their business and professional reputations were significantly damaged. For many organisations, the reputation of the business plays a more important role than the financial penalties in the wake of information

security breaches. The stock markets react to IS incidents particularly when confidential data are exposed due to unauthorised access [23].

6.5.2 Identification of human factors

To review and analyse the incidents, interviews were conducted in the two organisations where they occurred. Interviews were conducted in a semi-structured and in-depth manner and followed up with informal discussions. All interviews were carried out in the organisations' premises in pre-booked appointments. Interviews were recorded with digital audio recorders and notes were taken. Figure 6.3 shows the SWOT process for analysing the incidents; this contributes towards the construction of an ISS strategy development framework. The incidents, together with direct and indirect human factors (identified in Chapter 4), feed into the SWOT analysis, whilst the strengths and weaknesses work to provide an environment where opportunities and threats emerge. This is happening on the basis of what SWOT defines as strengths that create opportunities for effective ISSs, whilst weaknesses create threats that undermine the effectiveness of ISS. The outcome is the development of an ISS strategy based on the opportunities and threats that the ISS faces.

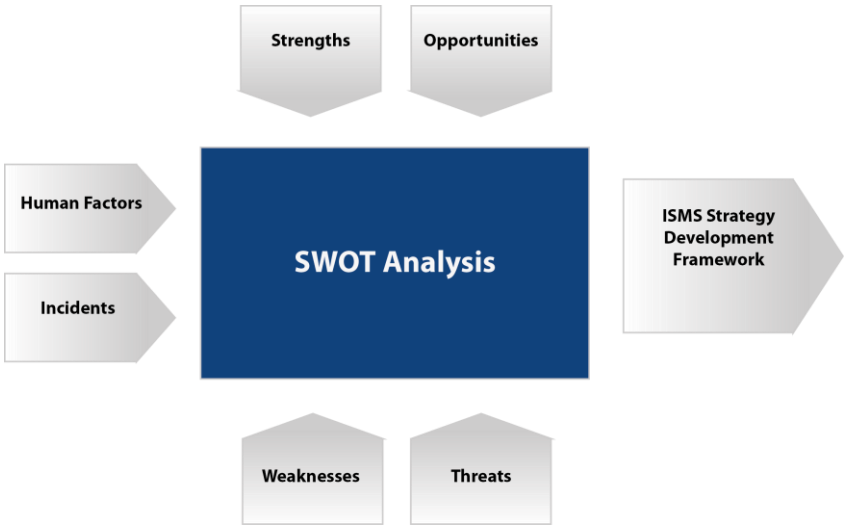


Figure 6.3. SWOT Analysis for this study.

6.5.2.1 Result

For the purpose of evaluation, the survey and interview responses relating to human factors were first identified. They were matched to the analysing tools. The irrelevant information was isolated, and the relevant information was broken down into small compartments. These compartments served as categories to reflect the SWOT factors in the analysis tool. The categories pertained to the direct and indirect human factors involved in ISSs, which were already identified early on. The category responses were mapped to

SWOT factors to provide a model for improving the role of humans in ISSs. The questions were identified and structured based on the issues relating to the incidents and humans. The human factors were also divided into two sub-categories: direct and indirect factors. A total of 24 questions were asked of each participant and each interview, held over 2 sessions, took more than 3 hours to complete. The questions were designed to form a consistent rationale from responses whilst preserving confidentiality. Table 6.1 shows the outcome of the responses based on SWOT elements, which were identified from the literature and the organisations' documents, shown in Table 1. For the purpose of quantifying data, the percentage of responses was allocated to each element of SWOT analysis based on the result of the interviews. This portion was calculated based on the number of people who were interviewed and the number of people who responded to the specific issues. For instance, out of 25 interviewees, all mentioned "errors" as one of the ISS weak points. Detailed interviews were conducted to gather in-depth qualitative data on human factors based on a conceptual framework adopted from the literature exploring organisational contexts, socio-technical elements and ISS concepts. A sample of Chief Information Security Officers (CISO), Chief Information Officers (CIO), IT Managers, Senior Managers, Middle Managers and employees from different departments as well as academics was collected for the in-depth interviews. The interviews and data collected from them reflected the reality of the interpretations. This is an opportunity to follow the research investigation path [23].

Factors	**Indirect/ Direct factor**	**Human factors**	**SWOT factors**	**% Of response**
Errors	D	Adequate training programs, but not effective	W1	100
Awareness	D	Awareness programs reduced confusion	S1	100
Skills	D	Ineffective IS training hits people's skills	W2	40
Experience	D	Most people have inadequate practical knowledge in the field of IS	W3	60
Apathy	D	Many people show a lack of interest in the issues surrounding IS	W4	60
Incentive/Disincentive	D	Policy in place, but lack of implementation	W5	40
Ignorance/Negligence	D	Not all breaches are intentionally planned	W6	50
Stress	D	Too many policies and regulations put extra pressure on people and impact IS	W7	70
Budget	In	Adequate budget planning for IS expenditures	S2	60
Culture	In	Security culture was adequate	S3	100

Communication	In	Inadequate communication was in place	W8	60
Security Policy Enforcement	In	IS policy adequate, but ineffective for various reasons such as lack of communication	W9	50
Management Support	In	Fully in place	S4	100

Table 6.1: Human factors.

6.5.2.2 Review of the incidents

Strengths

Awareness (S1) was considered by all interviewees as one of the important aspects of strength that influenced people in both organisations. However, they asserted that there are certain areas that require attention in order to enhance awareness, such as training in security practice. Based on the account given by managers at all levels in both case studies, organisations received an adequate budget allocation (S2). This relates to the support and effort of management in fulfilling security. All interview participants felt strongly about the security culture, and all approved of it (S3). One of the participants believed that the SI in their organisation was partly due to the lack of communication between the security policy enforcement process and employees. All participants declared that in their organisations they received an adequate level of support from management (S4). One of the senior managers pointed out that in his organisation, the board of executives understood the importance of ISSs and always supported investment in that area. This leads to an adequate allocation of budget, which in turn plays an important role in the preparation of security policy. Non-managerial employees also said that they enjoy a very good level of support from their managers.

Weaknesses

All interview participants singled out ineffective training programs, which led to errors and omissions being made by people (W1). They highlighted human error as the greatest factor in the category of weakness. However, individual behaviour and attitudes towards ISSs greatly influenced IS. One senior manager said that training is the most important factor in his organisation and he has put in place mandatory training sessions for all staff. He also expressed that his organisation uses access control techniques with identification, authentication, and authorisation processes. This clearly demonstrates that his organisation uses all available technology to fulfil the requirements of the ISS. However, most interviewees in both studies said that the training they received had long been unfit for the purpose of the work. They maintained that training did not cover all aspects of the security policy and that employees had to follow a policy that had not been covered fully in training. It can thus be concluded that training programs were inadequate and ineffective and that appropriate training to support the real

needs was necessary. This conclusion is in line with the outcomes of other research such that of Adams and Sasses (1999), who found that people (users) were not sufficiently informed about IS matters [84]. All interviewees highlighted human error as the greatest weakness, and this has a direct relationship with the lack of appropriate training. This was followed by a lack of awareness, observed by a number of interviewees. They believed this deficiency was because of the relationship between human error and security breaches in their organisations. However, these observations should not distract from the great influence of issues such as apathy and stress, which some respondents claimed were equally as important. All respondents identified people's skills as inadequate because training programs were ineffective (W2). However, lack of skill was not solely responsible for the SIs. Interviewees generally agreed that skills play a role in the effectiveness of an ISS. Interviewees were adamant that having relevant experience in the IS field plays a significant role in dealing with ISS requirements (W3). They believed that if the people who were involved in the SIs had had adequate experience, they would have dealt with the incidents more efficiently. There was a contrast of opinions amongst the interviewees in response to the question about apathy (W4). Whilst senior managers criticised some individuals for their lack of interest in following security policy, people in the lower hierarchy blamed other elements as the cause of the apathy, such as the lack of incentive policy implementation, breakdown in communication and ineffective training.

Some respondents, in particular those lower in the hierarchy, believed that human apathy did not affect the recent incidents in their organisations at all. Conversely, senior managers stressed that the lack of enthusiasm in some people was partly responsible for security breaches. Incentive policy received support from all participants (W5). Having said that, there were disagreements about the incentive policy as this is directly related to the issue of cost and has a monetary impact on both the organisations and individuals. All interviewees felt that an incentive policy could conceivably create opportunities to enhance security policy implementation, but overall they claimed that the policy is only written and not implemented. Most of the respondents recognised the issue of ignorance as a weakness, but they believed that recent SIs could not be entirely blamed on ignorance (W6). Stress as a cause received the total support of all participants (W7). They mentioned that workload causes stress and that this has played an important role for people who were involved in the SIs. Senior managers blamed ignorance, attributing it as the cause of incidents where data encryption was not implemented. In despite of this, some interviewees in the lower ranks of organisations stated that encryption applies to some data but not all. Three interviewees blamed the recent incidents on people's behaviour. They pointed out that people sometimes behave irrationally when faced with security restrictions. However, the rest of the interviewees were complacent about the behaviour of their teams in relation to security policy enforcement. Interviewees responded to the communication factor with great concern (W8). All respondents felt that there was a lack of communication between people and departments in their organisations. The breakdown of communication was one of the major causes of SIs. All

respondents identified security policy enforcement as one of the major factors in ISSs (W9). They stressed that whilst security policies were in place, the effectiveness of their enforcement could be disputed.

Opportunities

Most of the participants acknowledged the strength through opportunity that current ISSs in the studied incidents provide. They pointed out that security-training programs provide a basis for both organisations to promote a security culture built deep into the work environment. Senior managers in both incidents expressed their views on opportunities for their organisations to reduce costs by updating security policy. This would be the result of senior management support and involvement in the security policy preparation, implementation, and evaluation process. Providing adequate communication and a systematic approach within an organisation creates an environment in which a proposed ISS can be implemented effectively and efficiently.

Threats

Respondents at all levels of organisational hierarchies and in both case studies identified a number of threats. They believe that the threats are related to the security policy and the current ISS practices. However, people in various departments perceived threats quite differently. Whilst senior managers were concerned about the reputation and cost implications, others were anxious about extra pressure and stress. Management believed that to combat threats such as malicious activities, industrial espionage, hardware failure and compromises in the confidentiality, integrity and availability of information, they would require new policies and more training and awareness programs. Senior managers associated threats mainly with reputation and staggering cost. At the same time, they were concerned about the burden of cost in investing in an ISS. On the other hand, the rest of the team was anxious about other issues such as increased workload, stress and performance. Organisations, however, were rightly concerned about the greater threats that could significantly compromise the accessibility and reliability of their critical information system infrastructure.

6.5.3 Overall Observation

The outcome of this study presents a general account of the SIs being investigated. All SWOT factor themes were identified and discussed. With respect to the strengths and weaknesses, the outcome indicates that both the strengths and weaknesses depended on specific human factor attributes such as culture, employees' relationships and communication. Strengths such as training and awareness programs were also identified as weaknesses because they were not sufficient in eliminating errors, which caused the biggest blow to confidence in the security policy. The elements of opportunity concentrated on the constant review of the security policy, and updating and providing comprehensive training and awareness programs

whilst taking measures to deepen security culture. The theme of threats focused on improvement in employee emotions and feelings related to stress and workload, which would lead them to behave as expected in any information security decision-making.

Based on the findings and analysis of the data, it is concluded that the research goals were achieved and can be justified. The assumptions of the study were accurate and relevant. With respect to the first assumption, it was concluded that direct and indirect human factors were the main cause of the incidents. These factors were demonstrated in interviews, reviews of literature and organisation documents. Participants clearly mapped a strong relationship between human factors and security breaches in their organisations. Both of the incidents impacted negatively on the organisations and undermined the effectiveness of their information security practices. Indeed, the SIs were due to human problems rather than any technical fault. Organisations often ignore human-related factors in developing effective information security. The observation is that awareness and training are necessary for positive security behaviour and create strengths and opportunities that enhance organisational security posture. Also necessary is effective communication, the support of senior management and adequate investment. Inadequate skills, lack of awareness, lack of investment and intentional or unintentional error can contribute to virtually any potential risk to information security. SIs can severely threaten an organisation by damaging its reputation and attracting financial penalties. However, it is very difficult to explain the dynamics of how individuals interact with computers and surrounding systems and how this affects the decisions made around information security.

6.5.4 Threats to the validity of the analysis

General threats to studies such as this one relate to the difficulties of collecting data for reliable results and to the generalisability of the findings. To counter such threats, a validity examination of possible threats was carried out at the very beginning of the study. For example, data was collected not only from interview responses but also from documents available in the public domain; therefore, the reliability of the data collection was improved by using multiple data sources and by analysing the interview responses. All interviews were systematically planned and responses were auditable because they were recorded.

The study is based on two SIs; therefore, the generalisation of the findings about human factors is limited. However, the research followed existing literature and formulated a list of direct and indirect factors, mapping the identified factors with SWOT analysis before performing the study. The interview participants had adequate knowledge to respond to the questions with relevant answers and actively participate in the informal discussion. They also appreciated our research effort and its link with real incidents. Informal discussion sessions were an effective technique for understanding the participants' views on the incidents. However, the research has not covered the roles of external consultants and contractors, who have no

obligation to receive internal training. This weakness in the system must be dealt with before organisations agree to the terms of consultancy firms.

6.6 Survey Study: Identifying Critical Human Factors

In Section 6.2, the main direct and indirect human factors were identified. However, because an empirical study demands more specific and clear analysis, those factors must be prioritised so that the critical human factors can be elucidated. The main goal of the survey is to prioritise the human factors based on the observations of the survey participants.

6.6.1 Delphi Survey

In order to define critical human factors, the Delphi expert panel technique is used. The Delphi method is seen as a popular and established tool in the field of information security [71] [129] [130]. The factor analysis process was also considered initially but ruled out in favour of the Delphi technique for a number of reasons. In Delphi, participants could disclose their reasoning and confidentiality is easier to maintain [71]. In addition, Delphi provides a quicker analysis and thus is more useful when cost and return on investment matters are involved [130]. The main problem with factor analysis is its reliance on data, and it is less reliable when it comes to matters such as human factors, which have social and psychological dimensions. The Delphi method is a stable and consistent method that can be used to achieve the consensus of a group of experts [129]. The Delphi technique was incorporated in three stages, as shown in Figure 6.4.

1. Brainstorming sessions to identify human factors.
2. Narrowing down main human factors.
3. Prioritising and ranking human factors.

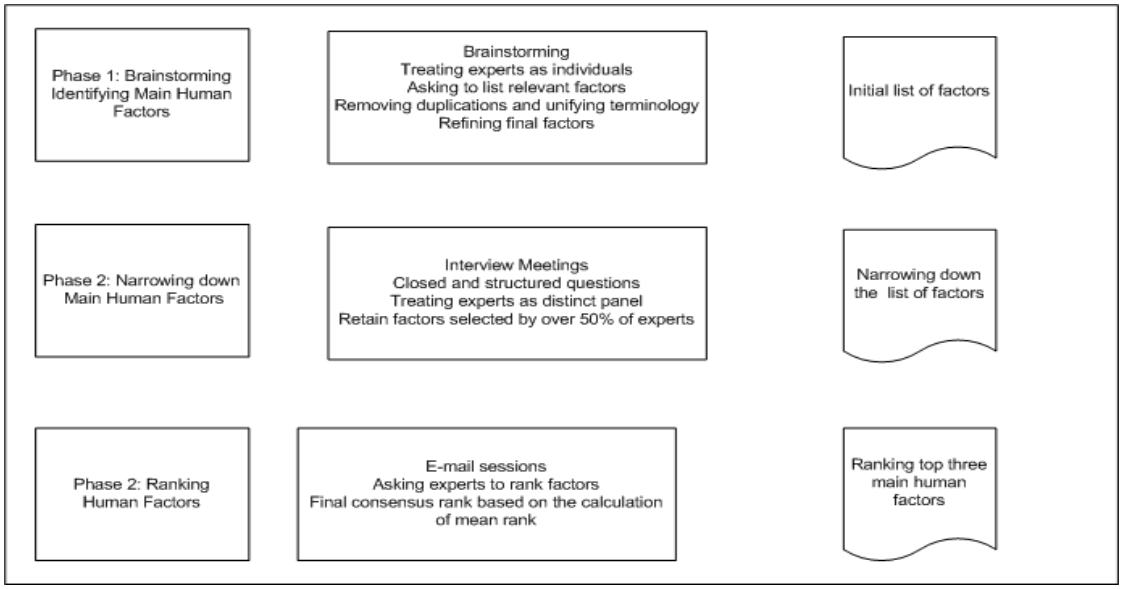


Figure 6.4: An overview of the phases of Delphi expert panel

Phase 1: Brainstorming

In this phase, a group-brainstorming session with structured questions was conducted to stimulate main human factors, which have a subjective nature and are thus qualitative data. A survey involving 62 respondents belonging to 7 organisations was performed. The brainstorming sessions were run separately in all seven organisations, and all participants agreed upon a set of factors influential in their ISS project experiences. Table 6.2 provides an overview of the organisations, ISS projects and survey participants.

Participant Organisations Info	
Organisation outline	Respondents were experts belonging to industry and academia.
ISS projects	Main human and people issues related to security projects.
Participant details.	The total number of participants was 62. They came from multiple levels of their organisations, including Chief Information Security officers (CISO), Chief Information Officers (CIO), IT managers and participants from academia.

Table 6.2: Overview of the participants' organisations.

The participants were also asked to justify the reasons for their selection and ranking of the factors. They were given two weeks for their responses. In the first phase, 34 of the 62 experts (52%) offered their assistance, generating a list of 13 human factors for ISSs that were similar to the factors identified in this research through multiple methods. The outcome of this process was the identification of the 13 human factors listed in Table 6.3;

those ranked 1-5 are very significant, whilst 5-13 indicates varied significance.

Phase 2: Narrowing down main human factors

Phase two of the survey study comprised 18 open-ended questions and 24 closed questions in the form of a questionnaire presented to the participants. The feedback received from the brainstorming sessions was incorporated into the questions to ensure the refinement of the human factors. In order to reduce any possible bias by neglecting factors or by factors that were not present, the participants were given an opportunity to offer feedback on the factors they wished to share.

Phase 3: Ranking main human factors

The third phase of the process involved sending questionnaires to the entire group that included 13 main human factors identified in the previous two phases and the average importance and rating determined in Phase 2. Figure 6.5 illustrates the participant composition in Phase 3. This was included with a set of justifications and a reasoning of the selections. Tables 6.4 and 6.5 depict the number of respondents in this stage by percentage. Figure 6.6 shows the three main factors with their sub-factors.

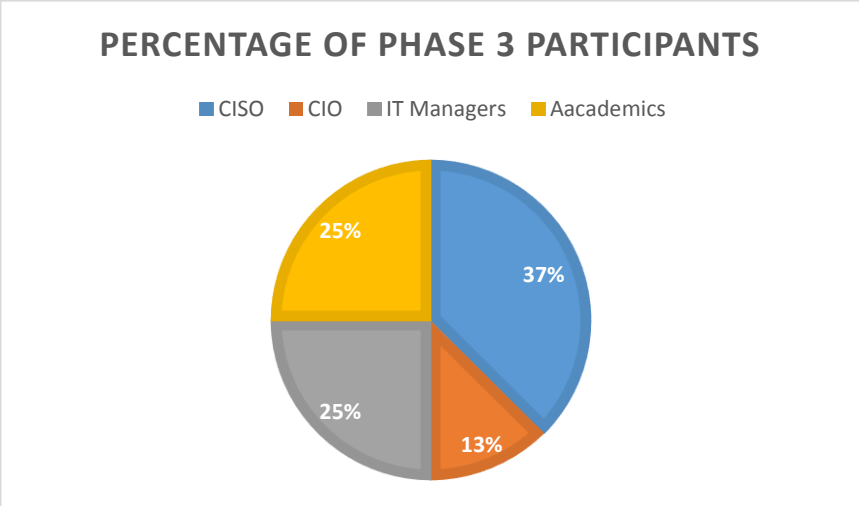


Figure 6.5: Composition of participants in Phase 3.

The participants in Phase 3 were experts, selected to ensure that expert opinions were considered. Through the use of the above expert panel, an opportunity was created to investigate and prioritise critical human factors in the case study organisations.

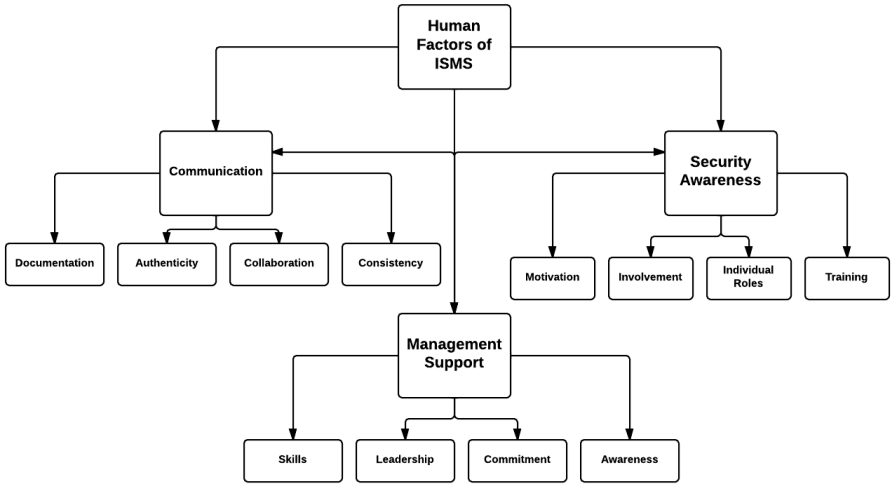


Figure 6.6: The three top-ranking human factors and their associated sub-factors.

Factors	Phase 1 (Mean)	Phase 2 (Mean)	Priority
F1	6.5	6.5	1
F2	6.0	4.5	2
F3	4.5	4.0	3
F4	2.5	2.0	8
F5	2.0	2.0	9
F6	3.0	3.0	5
F7	2.5	2.5	7
F8	3.5	3.5	4
F9	3.0	2.5	6
F10	1.5	1.5	11
F11	2.5	1.0	10
F12	1.0	1.5	12
F13	1	1	13

Table 6.3: Ranking of factors by prioritisation.

Factors Ranking	Human Factor	Description
1	Communication (F1)	Concerning the exchange of messages and ideas between people inside and outside the organisation.
2	Awareness (F2)	People's understanding of their responsibilities.
3	Management support (F3)	Management to advocate and deliver a clear message of ISS policy to the rest of the organisation.

4	Budget (F4)	Concerned with adequate budget planning.
5	Errors (F5)	Can be described as a divergence in a system that works accurately.
6	Skills (F6)	Skills facilitate the function of a role.
7	Experience (F7)	Concerns people's backgrounds.
8	Incentives/Disincentives (F8)	Reward good behaviour and punish bad attitude.
9	Security Policy Enforcement (F9)	A document in which the information security procedures and rules are outlined
10	Culture (F10)	Values, beliefs, practices, attitudes, behaviour, reputation, and ethics.
11	Stress (F11)	Individuals' stress in corporations can be caused by heavy workloads and tight project deadlines.
12	Apathy (F12)	Employees' unwillingness and complacent attitude toward the goals and objectives of the organisation.
13	Ignorance and Negligence (F13)	Not paying enough attention to security policy.

Table 6.4: Ranking of human factors by importance.

6.6.2 Discussion

For the purpose of this research, it was essential that the main direct and indirect human factors be prioritised in a process through which critical human factors could be identified. Narrowing down the main factors allows the study to concentrate on critical factors, to minimise errors and gain maximal scalability from the proposed approach. Communication, awareness and management support are ranked as the top three critical and important human factors by the survey participants. They are also interlinked, because without management support it is difficult to raise awareness among an organisation's staff. Communication is vital in any organisation. In particular, ineffective communication pose any potential risks within organisation. Whilst budget allocation, human errors and individual skills are positioned below the top three factors, their importance is evident. The strong relationship between management support for information security initiatives and budget allocation for such projects puts

these two in a unique position. This relationship between management support and budget are mostly concerned with the capacities and qualities of individuals relevant to the position they occupy in the organisation hierarchy. The examination of participants' responses also reveals the importance of culture in each organisation, which is mainly fed by senior management team(s). Such an approach by senior management to amplify security culture has a distinct impact on the specific security culture. It also affects individuals' stress and willingness to following security system objectives. Furthermore, the study confirms that the choice of theoretical basis for this research was a correct and relevant choice. The socio-technical environment has a significant impact and relevancy to many areas of technological advances, including information security and its challenges and opportunities.

6.7 Case Study 2: Implementation of the Risk-Driven Investment (RIDIM) Model

The previous case and survey studies are mainly focused upon understanding the critical human factors within the information security system context [137]. Several observations have been made from the case studies, and human factors were prioritised for use in the second study. This study implements the proposed risk-driven investment model in a real world scenario.

6.7.1 Study Constructs

The main study construct is:

- *To demonstrate the applicability of the risk-driven investment model in a real world scenario*
- *To understand the issues around managing human factors for the overall information security management system.*

6.7.2 Scenario Context

The scenario used for this study is based on real and successful SEA incident that occurred in a financial institution within the UK. It was a very well-targeted phishing attack.

An employee received an email from one of the managers referencing an invoice hosted on a cloud file sharing service. A few minutes later, the same employee received a phone call from another manager within the organisation, instructing her to examine and process the invoice. However, the invoice was a fake and the manager who called the employee was an attacker. The apparent invoice was in fact a Remote Access Trojan (RAT) that was designed to contact and command-and-control (C&C) the server. By using the RAT, the attacker took control of the employee's computer instantly. The attacker only managed to breach a part of the server as the multi-layered encrypted server prevented him from gaining access

to all the other servers. This attacker used a socially engineered attack for financial gain. Before the attack was stopped, they succeeded in stealing assets worth around £50,000.00.

6.7.3 Introduction to the RIDIM process

Activity 1: Identifying Business Domain

The main focus of this activity is to provide an understanding of organisational actors, goals and business processes. The scenario concerns a financial organisation.

Step 1.1: Identify Actors

As described in Section 5.4.1, ISSs and people are internal actors that are defined by their entities and specific strategic goals in an organisational context. The attacker is an external actor who intends to gain a financial incentive. In this scenario, the false financial transaction initiated by the attacker is an SEA. The first and most critical asset compromised was part of the server of this company. Financial information was another important asset that was compromised. Both can be categorised as high value assets. We have listed critical human factors based on the results of previous studies. In particular, it is clear that a lack of security awareness contributed to the successful planned SEA. The absence of an adequate authentication process also assisted the attacker in establishing a false communication channel. Finally, if senior management had had adequate skills and awareness, then it would have been able to offer support and put appropriate control measures in place.

Step 1.2: Define Goals

The Availability, Integrity, Confidentiality, Accountability and Auditability (AICAA) of information assets are considered as security goals and part of business goals. The main threat in this case study was the installation of malware that assisted the attacker in gaining access to the server. The user's carelessness, due to lack of adequate training, was a vulnerability that the server exploited. A potential risk of loss arose as the result of the threat exploiting the vulnerability. This clearly demonstrates the lack of a proper firewall and software security protection. Considering the nature of the incident, this company should define an adequate risk mitigation strategy whilst considering the cost of implementing controls and the potential costs of not doing so. In addition, the company should prioritise, evaluate and implement appropriate risk-reducing activities to address the specific risk it faces and estimate its degree of risk exposure.

Step 1.3: Identify Business Process

The business activity is invoice processing. The technology used was cloud-based and the attack was a form of SEA in which malware was installed to

control part of a server and process a malicious financial activity. The stakeholders in this process are the firm, the employee who processed the invoice, the attacker and the information system and security system. As the incident had very little effect on the continuity of the corporation's routine business, a business continuity plan plays a lesser role than that of a disaster recovery plan. A disaster recovery plan identifies the affected parts of the system to ensure that future operations and, specifically, backups will not be affected. In addition, the compromised part of the server requires the attention of the ISS with regard to maintenance and improvement with adequate investment.

Activity 2: Incident analysis

Step 2.1 Description of the Incident

This activity provides an analysis of the incident, looking at the details of the incident and identifying risks. The researcher were informed that the incident had been reported promptly after it had occurred, though the extent to which is has been reported to the regulatory bodies is not certain. All of these issues are important in analysing the risks involved. The incident was rooted mainly in the exploitation of vulnerabilities in the server, although critical human factors, as described in Activity 1, were also actively involved. The exposure has directly impacted the company. The incident was a SEA, in which malware called (RAT) that was designed to contact and command-and-control (C&C) the server was installed. In short, human factors and an inadequate security detection and prevention system contributed to the incident. As a result:

- The organisation found out quite quickly that an incident had occurred.
- Senior management team confirmed and agreed upon the incident respond policy. The detection of the incident was monitored with the guideline of the incident response policy.
- The identification of the incident was carried out sufficiently, thanks to malware detection software.
- The attack was in the form of a SEA and facilitated by a lack of clear communication policy regarding authentication as well as an inadequate level of awareness.
- The immediate loss was around 50K, the amount that has been compromised. The potential fines imposable by the regulator and insurance and mitigation costs require a calculation.

Threats/Vulnerabilities/Risks

A vulnerability in the network and critical human factors were exploited, causing financial risk. The compromised part of the system requires new detection and prevention controls; a better awareness program is also needed. Whilst new network patches are needed, employees are also required to be trained in a more effective way to deal with email and phone

authentication methods and thus detect invalid and hoax communications. The risk and vulnerability mitigation process requires that action be taken by the information security team. It is vital to identify the weak links and any known internal factors that may compromise the appropriate risk evaluation and subsequent recommendations.

Cost/Investment

The costs to the firm following the incident as well as the critical issues that need to be addressed through investment are outlined below.

- An immediate loss of 50K was sustained.
- The cost of patches for the network and server should be clarified.
- The possible cost of modifying training program(s).
- The possible cost of authentication of communication.
- The possible cost of disruption to services and the BCP process.
- Identifying the severity of the impact on the firm.
- Identifying if there are any legal implications of the incident.

The sSenior management team should clearly consider the implications of the above issues and their cost to the organisation.

Root Causes of Incidents

Identifying the root causes helps to determine the exact causes of incidents from a risk point of view. In risk management, root cause analysis is an important tool in identifying the factors that drive risks. The root cause analysis asks the question of why a given set of risks occurred and not how. Consider the attack scenario in which the server was compromised using Command & Control, the result of the payload of a RAT. The attack path describes how the employee was deceived into delivering a RAT payload. If the organisation therefore blocks the particular C&C attack and addresses the specific RAT payload, this does not prevent others from occurring. The root cause, on the other hand, defines the human vulnerabilities and the role they played in delivering the payload. In order to identify the root cause, the sequence of the events must be fully understood by re-constructing exactly why the incident happened. A forensic examination of what occurred provides precise answers to queries relevant to the incident. The role of human factors in the sequence of events should be identified and, subsequently, the root causes of the incident addressed.

Step 2.2 Identifying and analysing the risks

At this point, the register session, an overview of the risk assessment process, is complete. This process then requires a review of the business attributes Availability, Integrity, Confidentiality, Accountability and Auditability (AICAA) to identify and examine the threats. It then identifies

any existing controls or safeguarding measures in place. When that process was completed, the team examined the probability of each threat occurring and their impact on the business process. Each threat is examined using the existing control as a guide to assign a relative risk level to it. Once the risk levels are established, possible controls can be identified that could reduce the threat risk level to an acceptable range (Figures 6.7 and 6.8). These two figures provide an example of the risk registry of a company, called Company X in this research to maintain anonymity. The process can be summarised as follows:

- Threats were identified
- Risk levels were established
- Controls were selected

Identifying the threats and choosing controls is essential, but the most important element in an effective risk assessment process is determining the risk levels. Organisations need to know where problems lie before making any decisions about how to deal with them.

Company X Risk Register

Portfolio: Company X

Ref.	Risk	Root causes	Owner	INHERENT RISK SCORE (No Control)			Mitigating Actions	Embedded Monitors/Early Warning Indicators	RESIDUAL RISK SCORE (With Control)			Date of Last Review
	(Threat to achievement of business objective)	(How the threat could arise)		Probability	Impact	Matrix Zone	(What we are doing to manage the threat)	(How we know if we are succeeding)	Probability	Impact	Matrix Zone	
	Format: EVENT leading to CONSEQUENCE resulting in EFFECT ON BUSINESS OBJECTIVE						Format: Who, What action, How frequent, How evidenced?	Format: include comment on effectiveness.				
AL01	Loss of money	Lack awareness because of inadequate and out of date training program	Shareholders and senior management	4	5	R	Updating training program	Review any anmolies, if possible.	2	3	Y	08/12/2016
		Lack of effective authentication protocol for communication	Shareholders and senior management	2	3	Y	Patching encryption and authentication security gaps	Regular review of the patching	1	2	G	08/12/2016
AL02	System compromise	Lack of network security patching	IT and senior management	1	4	Y	Patching network	Regular review of the patching	1	4	Y	08/12/2016
AL03	Compromise of information assets	Lack of clear data classification and late response by the Incident Response Team	IT and senior management	2	3	Y	Reviewing calssifications of data with support of senior management	Providing assistant and direction for regular auditing and support of senior management for updating classification	1	4	Y	08/12/2016

Figure 6.7: Risk impacts analysis.

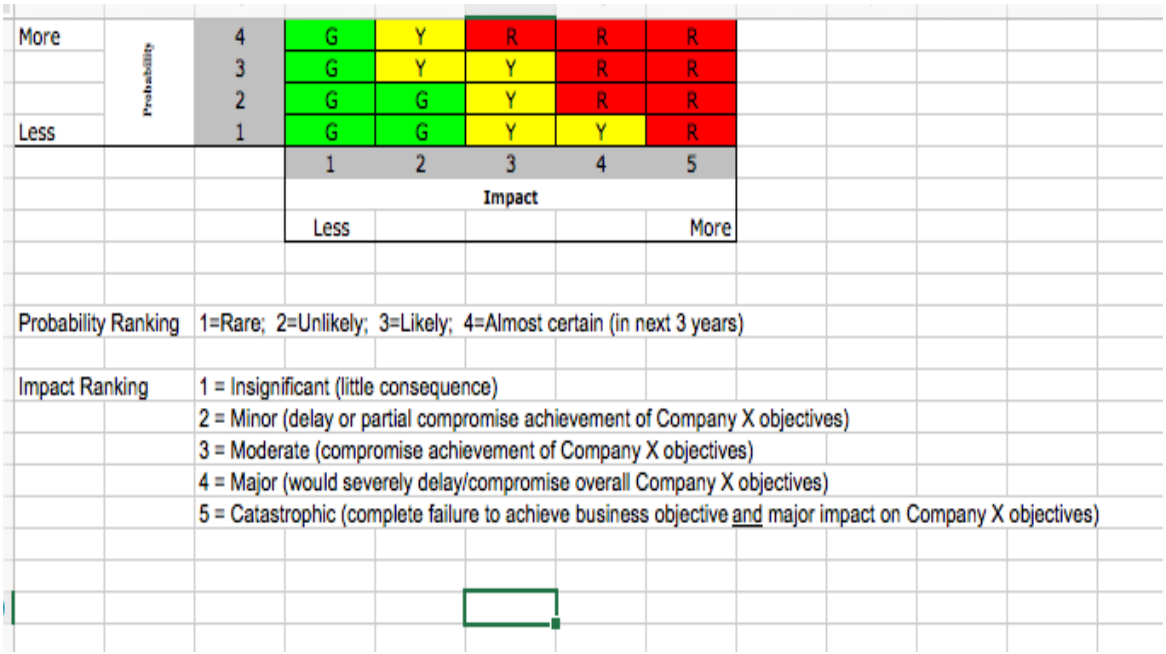


Figure 6.8: Risk analysis matrix.

Considering the outcome of the risk analysis, the severity of this incident had a moderate impact and cost in relation to Company X's objectives. It revealed a major failure with regard to critical human factors and awareness and training programs there. In the risk analysis register, a number of mitigating actions are listed and residual risks are addressed with controls. Table 6.5 demonstrates the additional controls and new risk levels after the risk analysis, which could be acceptable to the business or at least accepted as residual risk.

Threat	Existing Controls	Select New or Enhanced Control(s)	New Probability / Impacts	New Risk Level	Acceptable Level (Yes/No)
Insecure e-mail could be sent by an unauthorised sender	E-mail handling policy in place and are being developed. Concern about employee awareness program to be addressed	E-mail handling policy in place. Concern to be addressed regarding employee awareness program and new employee position	1/2	Likely	Yes
Using consumer online file-sharing services on work devices to store and	Limitation placed on access to data	Limitation on access to data and on what users can do with those files (read, write, modify	2	Unlikely	Yes

share sensitive data.		and/or share).			
System compromise	Authentication Encryption in place	To develop and upgrade current authentication and encryption and enhance employee awareness training	1	Unlikely	Yes
Communication failure	Authentication in place	To develop better and stronger authentication for communication channels and update the employee awareness program	2	Unlikely	Yes

Table 6.5: Additional control and new risk levels.

Considering the outcome of the risk analysis, the Security Investment-Incident Pattern (SIIP) artefact, which suggests the security-investment needs of organisations, is given here. This pattern describes an integrated security solution in which all pattern requirements and attributes (provided in Table 5.1) have been employed to give the core elements of ISS security properties. This includes critical human factors and investment requirements, and it considers most other elements of business functions.

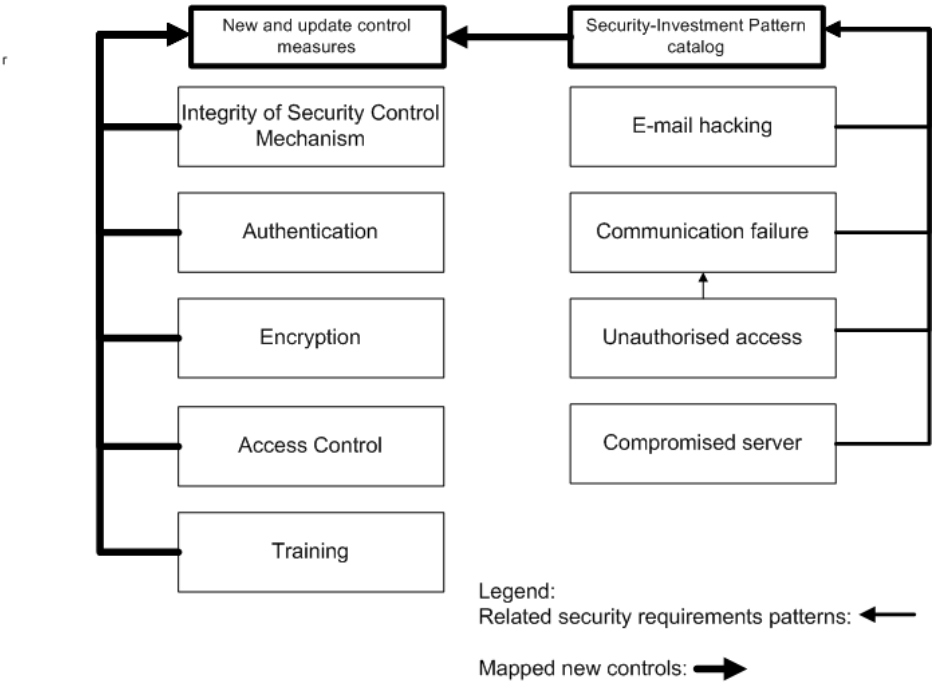


Figure 6.9: Security Investment-Incident Pattern (SIIP) Artefact

Activity 3: Calculation of the ROISI

Step 3.1: Analysing existing control measures

Existing control measures include security awareness training, authentication, firewalls and encryption. However, the training manuals require an update, encryption mechanisms must be reviewed, an authentication processes should be established for all types of communication and the firewalls should be updated. All of these can address the vulnerabilities and residual risks. Column 2 in Table 6.5 provides a list of existing control measures.

Step 3.2: Identify the potential control measures

Once the existing control measures are analysed, it is then necessary to identify possible actions based on the risks and review the control measures. The effectiveness of identified potential control measures determines the gap between existing and missing controls. This gap is briefly identified in Activity 2. This step identifies the possible techniques that can be used to identify potential countermeasures for addressing the causes of incidents and damage done to existing defence mechanisms. It is clear that they do not work and that the system requires a review, possibly accompanied by the introduction of new control measures. The value of reviewing or providing new controls is directly related to the loss incurred because of an incident. Table 9 provides a list of potential control measures.

Step 3.3: Calculate the cost of a control and the ROISI

This section provides an estimation of the losses incurred and the calculation of the ROISI. A positive outcome would shows that investment in new control measures is justified and a negative outcome indicates a lack of financial justification for the new control measures.

Estimation of the losses and Return on Information Security Investment (ROISI)

For the purpose of this study, a preliminary calculation of the expected cost of preventing loss arising from incidents is presented, using the following parameters: External Services Cost ES(C), Purchasing Cost-P(C), Employee Cost-E(C), Administrative Cost-A(C), Legal Costs-L(C) and Other Cost-O(C); therefore, the total expected cost of a new and updated control mechanism would be:

$$TEC(T) = ES(C) + P(C) + E(C) + A(C) + L(C) + O(C)$$
$$TEC(T) = 10K+5K+2K+0+1K= £18,000.00$$

The next step is to calculate the Total Revenue Loss $RL_{(T)}$ from both existing (L_1) and potential customers (L_2). The estimation for Company X, based on its business and revenue, is given as:

$$RL(T) = L1 + L2$$
$$RL(T) = £50{,}000 + 0 = £50{,}000$$

One can now examine the following parameters, mentioned earlier:

- Single Expected Attack Loss SLE
- Total Expected Cost of an Attack TEC(T)
- Insurance Claim IC(I)
- Revenue Loss from existing/potential clients RL(T)
- Average Margin AM(A)

$$SLE= ((TEC(T) – IC(I)) + (RL(T))) * AM(A)$$
$$SLE = ((23K – 5K) + (50K) * 15\%$$
$$SLE = £30{,}500.00$$

This figure is the total Single Expected Attack Loss (SLE), which is based upon the risk exposure just indicated and the probability of the incident happening only "once a year", and it takes into consideration the threats, vulnerabilities and existing control mechanism. If a training program is run every three months, costing £2,000 internally and £2,000 externally and results in an 80% reduction in SIs for this company and its 15 employees, assuming an average cost of £22,000 per employee, then the annual cost of the new control protection will be £5,320.00.

The total New Single Expected Attack Loss (NSLE) after the new control mechanism has been implemented would be:

$$NSLE = SLE * (100- \% \text{ reduction of SLE}) = £6{,}100.00$$

Thus the Annual Lost Expectancy (ALE) based on one-year risk exposure would be:

$$ALE = NSLE * \text{Frequency (annually)} = £24{,}400.00$$

The Risk Reduction, $R_{(r),}$ can therefore be calculated as:

$$ALE = SLE – NSLE = £6{,}100.00$$

If the ROISI is positive, the investment is justified; if it is negative, then investment cannot be justified.

$$ROISI = R(r) – \text{Annual cost of protection } (£5{,}320.00) = £780.00$$
$$ROISI = R(r) / (£5{,}320.00) * 100\% = 14.66\%$$

Step 3.4: Monitor the control

We can conclude that the establishment of new countermeasures can reduce the risks and prevent the causes of the attack. They are also justified economically and this organisation is able to rationalise its decision to invest in new control measures, which ultimately minimises its risk exposure.

Technical and non-technical cost of incidents

SEAs create both technical and non-technical cost implications for organisations. Technical costs of SEAs are varied and they include having to update all current network patches and dealing with phishing emails, insecure mobile devices and cloud security issues. Non-technical costs of incidents include re-training, re-programing awareness materials and other training-related matters.

Determine benefit

Clearly the benefits of preventing SEAs are apparent for any organisations of any size. The benefits of deploying a preventive model for SEAs are explicit. In the RAT incident discussed above, the benefit of providing an adequate understanding of the complexity of SEA attempts becomes evident. The key benefits of SIRM are: fast and quick preventive measures against SEA attempts, more efficient user experiences when dealing with e-mail and phone communications and reduced support needs.

Investment

Organisations need to invest in all aspects of IT to deal efficiently and adequately with SEAs. The key areas that require investment are: training, upgrades and more detailed classifications of data and information. Further investment in improving network capabilities may also be beneficial. In addition, a penetration test is required as well as further capacity to assess vulnerabilities. The development of employees' technical skills through a new training program is advised.

Justification for the Investment

The new investment is justified and can be presented to the executive board to be actioned. Investment should be considered in the initial stages of ISS development just like any other critical enterprise objective. Only with an adequate resources and appropriate awareness and IS-related training can SIs be addressed. An in increase security investment initiatives in organisations with consideration of a clear action plan, alongside a range of improvement strategies that give them a real return on any security investment, is required. Insignificant investment in information security can have dire consequences for organisations. Proactive security investment decisions are therefore vital for organisations and should be incorporated into an enterprise security architecture that enables security capabilities across all business activities in a consistent manner.

6.7.4 Discussion

Applying the RIDIM model in a real case study demonstrates that the model is useful for other incidents, including those in which critical human factors are a grave concern. Based on the consensus of the experts, the use of general concepts of risk, cost and investment and human and organisational contexts, the applicability of the model can be extended to other incidents. It has been highlighted that seeking new investment in security, requires a clear financial justification. The RIDIM can be used in any organisation, regardless of size or business nature. Although there are a number of information security standards and regulations that are quite helpful in providing security metrics, the nature of organisations, their culture and critical human factor specifications differ, and these new dimensions are better treated by a comprehensive model such as RIDIM. As the nature and impacts of risks differ due to the factors listed above, security solutions are consequently varied. Organisations seem generally overwhelmed by the number of incidents they experience and from the ever increasing requests from IT and/or information security professionals for yet more investment. Senior management teams were confused by requests for more investment due to their belief that current investment in IS was adequate. They asked why SIs still occurred despite existing investment?What risks do organisations face and what sort of investment in improved defence capabilities is required? The answers to these questions are demanded by many organisations, and the researcher believe that RIDIM provides part of the solution.

6.8 Study Limitation

The model presented in this research overcomes some of the limitations in respect to reasoning critical human factors on the return of security investment. However, this study also has its own limitations. One of the major limitations of this model is that it only supports incidents based on an investment context. This could make the model less attractive to an executive board. Secondly, due to the nature of human factors, quantification does not reflect the monetary value of the factors precisely. Subjective concepts such as human factors are difficult to be applied and used practically. Human and socio-technical forces are quite hard to be quantified. The research design has in its own limitation in respect to the possible bias by the researcher. Some of the qualitative data collected by the researcher may have been influenced by their subjective interpretations. Although detailed data on the role of human factors and their characteristics were gathered, the subjective views of the researcher provided an opportunity for bias to creep into the approach. The case studies were chosen due to the large organisations involved.

6.9 Conclusion

This research introduces a risk-driven investment model in information security that enables organisations to analyse the risks and return on

investment in security controls and deal with SIs. The process makes use of secure-tropos, requirements engineering and risk management concepts. Using security, risk, business and SEA concepts allows us to model and explain the role of critical human factors quantitatively and in relation to risk and investment. Risks, business domain, SIs and investment concepts in an organisational perspective are not left unexamined by using our model. The proposed process leads to a clear definition of risks, incidents and investment in relation to human factors. Nevertheless, this model does not guarantee that organisations will fully be capable of calculating the return on their investment in security controls. This is because most incidents are related to critical human factors, which are notoriously hard to put figures to or value quantitatively. However, RIDIM supports organisations in obtaining numerical figures for all relevant costs relating to incidents. Additionally, the researcher intend to propose methods in their future work that will further support organisations in validating the control mechanisms yet more accurately.

CHAPTER 7

Conclusion

Contents

7.1 Overview

Effective risk management practice forms the core of an organisation's Information Security Management System (ISS). The risk management process is about identifying, analysing, evaluating and treating risks and sets the stage for protecting organisations' assets. An ISS project combines business, socio-technical and technology concepts, including critical human factors, risks and investment, at every phase of development. Such concepts have an extremely high influence on the success of such projects. Thus, ISS projects are affected by multidimensional factors during the course of their design, implementation and evaluation. Consideration of the influence of critical human factors, risks and security investment in meeting the project goals should be given to construct a more consistent and reliable risk assessment methodology. The literature review concluded that a comprehensive ISS risk assessment methodology focusing on the critical human factors in conjunction with the cost of adequate controls is hardly ever considered in practice. Information security projects are often analysed from the technical perspective, with a great emphasis placed on minimising costs. Such projects are almost never analysed from a non-technical standpoint and the return on investment concept is overlooked, without objective and holistic consideration; therefore, a holistic and comprehensive risk assessment methodology that adequately considers critical human factors and the return on security investment is required to ensure an effective ISS. This thesis contributes towards this. The researcher's personal involvement in ISS projects and literature reviews contributed to the motivation for this study.

7.2 Outcome of the Research

Based upon the substantial scrutiny that the current literature and practices reviewed by this research have been given, it is apparent that the security industry, businesses and academics all underline the importance of human

factors in ISSs. This research contributes by explicitly reasoning and analysing the main human factors in ISSs, linking them to project-specific goals, risk and security investment. Hence, the research proposes a risk-driven security investment model for analysing the risks and security investment based on human factors. The final contribution of this research is to empirically and experimentally analyse the proposed approach for its applicability and to reason the impact of those factors on an ISS project. The research delivers a reasoning of main human factors and their ISS-related complications in a structured form. The study contemplates a requirements engineering approach and Secure-Tropos modelling concepts for the information security project. The approach assists in the reasoning and analysis of the role of main human factors in ISSs and their relation with the concepts of risk, security investment and return on investment. Secure-Tropos language is used to characterise all relevant concepts, such as actors, risk, threat, investment and controls.

The RIDIM model and its concepts provide a comprehensive view of all relevant elements of ISSs from a holistic point of view and support the analysis of risks due to security incidents as well as the return of security investment. The RIDIM enables ISS in the design process in which all project components and indicators of the effectiveness of the project, such as main and critical human factors, risk, investment and controls, are considered in a synchronised fashion. It also calculates the risk resulting from critical human factors and their impacts on the investment on the control measures and the return of that investment as result of the mitigation. The research elaborates upon and integrates the underlying activities of the RIDIM into the methods and roles of the Requirements Engineering and Secure-Tropos process models. The artefact-oriented model is used to construct the risk-investment specification and its associated concepts such as goals, risk, investment, vulnerabilities and actors. All critical human factor-related concepts and attributes are illustrated by the RIDIM, as are the risk-investment descriptions. This research develops a risk-investment taxonomy and constructs a questionnaire consisting of 30 open and closed questions that are arranged into a requirements errors checklist.

The purpose of the closed questions and checklist was to determine the risks related to critical human factors and requirements errors. The result of the empirical examination of this study indicated that the risk-investment approach had a positive impact on the success of an ISS. The novelty of the thesis arises from the following achievements:

- Identifying the main features of human factors in an ISS theme
- Introducing a risk-driven security investment approach for ISSs
- Analysing human factors, risks and security investment in the ISS process.
- Applying the RIDIM Model to reason human factors in ISSs

The study results provide a sound and clear understanding of main human

factors and their relation to risk and security investment. The RIDIM is a capable risk-investment tool that informs of the risks that exist in an ISS project. The focus of this research is very different from that of other studies due to the human, organisational and technical lenses it views information security through.

7.3 Research Questions: Outcome

Three research questions were posed initially. Following the development of the study work and empirical investigation, the summaries below provide an answer to those questions.

7.3.1 Research Question 1

Question 1: What are the main characteristics of human factors within an ISS context?

This question mainly requires an analysis and reasoning of human factors in addition to the identification of the main and critical factors. The outcome discussion of this question provides a clear understanding of the role of human factors in ISSs and well-defined main and critical factors as a set of prioritised human factors. This process is well-suited to the development of ISS projects. The research considers SWOT, survey and Force Field methodologies for the purpose of this question. These methods and techniques have been used for the reasoning and elicitation of subjective matters such as human factors in research similar to this. Such survey and brainstorming processes with key actors and stakeholders help significantly in providing an understanding of the highly subjective and difficult issue of human factors. The organisations featured in this research seem have little knowledge of the severity and importance of human factors, as well as of their varieties and classifications. The analysis of human factors were performed under a practical theory that is affiliated with the investigation of the multifaceted and prejudiced nature of human factors. The RIDIM model drew from this analysis and identification of critical human factors to define a model that could address the risk-investment issues relating to control mechanisms and ensure the effectiveness of the defences provided by an ISS.

7.3.2 Research Question 2

Question 2: How do we analyse and reason human factors, risks and security investment in the development process of an ISS?

This research question focuses on identifying and reasoning the relationships between human factors, risks and security investment in the process of developing an ISS. The proposed RIDIM approach supports this analysis. The study conducted survey and case studies that included real world security incidents. The main human factors were split into two categories: direct and indirect. Direct factors are intimately related to individuals, whilst indirect factors connect individuals with organisational factors and contexts. The research then defined the dependencies between

risks, business domain and critical human factors in the ISS process. This research continued to embrace the security investment concepts and the return on such investments to address risks resulting from untreated critical human factors. The use of security incident case studies helped to provide an understanding of the economic impact and effect of risks that resulted from the critical factors.

7.3.3 Research Question 3

Question 3: How can the security risk-driven model support the analysis of the effect of human factors in the ISS development process?

Research question 3 concerns the identification of risks related to critical human factors and investment related to control mechanisms in ISS projects; it also calculates the ROISI. The survey and case study results addressed this research question. The analysis of the case study yielded a quantification of the ROISI, which allowed for a justification of the introduction of new control measures to address the risk resulting from critical human factors. The research utilised project specifications, real security incidents, survey questions and brainstorming sessions to identify and assess risk factors and critical human factors. The recommendations provide a link between human factors, risk, incidents and the impact of an individual risk on the control measures depending on the influence of the risk and the cost of the mitigation. The research aimed to establish the level of risk posed by critical human factors to an ISS project so that risk management can effectively address this vulnerability and ensure a successful project outcome.

7.4 Empirical Study Results: Conclusion

A survey was conducted to identify the critical human factors in ISS projects. The survey participants comprised practitioners of various ranks across 7 organisations as well as a number of academics. All participants had had at least 2 years' work experience within the organisations. The details of their roles and the number of participants are provided in the previous chapters. The result showed that the top three prioritised and critical human factors were: 1) Communication, consisting of four sub-factors: Documentation, Authenticity, Collaboration and Consistency; 2) Security Awareness, comprising four sub-factors: Motivation, Involvement, Individual Roles and Training; and 3) Management Support, comprising four sub-factors: Skills, Leadership, Commitment and Awareness. It was determined that the absence of clear communication, unstable and ambiguous security awareness programs and a lack of commitment and capability among senior management teams were the most important risk factors. Some of these risk factors were also highlighted in the reviewed literature, although not as the result of such a clear and consistent method.

7.4.1 Case Studies

Two real security incidents were used as case studies for the purpose of analysing and identifying the main human factors. Case Study 1 was performed using SWOT analysis and discussed in the interview sessions with participants. Case Study 2 used a SEA incident for the quantification of risks and investment. The purpose of this case study was to demonstrate the applicability of the RIDIM approach. The research has made several observations from the case studies. Understanding the subjective nature of human factors before implementing risk management activities is very useful as it ensures that those involved in the project are conscious of the impressionistic nature of the human factors from the outset. This characteristic then shapes the plan and scope of the RIDIM activities. Risk identification and analysis is the most critical part of the information security management system. Risks need speedy care and RIDIM allows handling these risks from the early development. The study concludes that it is always necessary to prioritise human and risk factors most highly in order to manage and mitigate potential threats. ISS specifications demand sufficient attentiveness to human and risk factors as well as investment in security controls.

7.5 Limitations of the RIDIM

Several limitations of the proposed approach were noted. Firstly, this model only focuses on investment for security incidents. It would therefore be somewhat challenging to present such an investment to an executive board or senior management team in any company as any such security-related projects are hard to sell. In addition, due to the nature of human factors, quantification does not reflect the monetary value of these factors exactly. The limitation on the availability of data for the validation of the empirical study provided another challenge. In regard to scalability, the RIDIM encountered difficulties within a large organisational context. A large organisation requires a large scale ISS development project, which attracts a large amount of risk derived from major and critical human factors, leading to an intensification of the complexity of the risk-driven model. ISSs have many requirements that need to be fulfilled, and it is extremely hard to identify and map every single of them to human and risk factors. The large number of project specifications and human factors brings considerable challenges to constructing, maintaining and documenting the risk-investment specification context. It is thus not always possible to build the model to cover every risk event in ISS projects, which are themselves continuously evolving and under time and budgetary pressure. Consequently, the opportunity to use the RIDIM to detect and resolve every risk with an adequate cost and control mechanism may not be available in every ISS project. . In order to make the RIDIM project-specific, it must be customised and bespoke. This can be advocated for through the involvement of stakeholders in the organisation, and the RIDIM can be configured fully with organisational risk management policies and processes.

The empirical investigation found that risks should be defined at a very early stage during ISS project planning. To better establish a link between the RIDIM and risks, further research is required. These risks include the residual and inherited risks present within organisations. The process of mitigating risks will benefit from this investigation, whilst more investment should go to more effective security control measures.

The model was applied successfully to an ISS development process in regard to the adaptability of the RIDIM. This was a complete implementation based on a SEA security incident. To generalise the findings of this research, they were compared with those of other studies in the literature. This comparison showed constructive resemblances and some distinctive outcomes.

7.6 Future Research

RIDIM identifies project-specific goals, actors, costs and risks and provides an adequate understanding of objectives that require the mitigation of information security risks. One of the main benefits of the RIDIM is that it is quite simple. It conforms to the information security domain specifications with an understanding of critical human factors, risks and security investment in relation to ISS goals and objectives. Despite these benefits, the model has several limitations. Further research would help to link and adapt this model fully to the risk management analysis currently used by organisations. Automation of the process can also useful for the implementation of the approach. The automation can be designed and implemented by providing a tools such as the Security Dashboard. The model can be used more effectively if it is presented with a practical tool. Furthermore, more empirical investigation is required to generalise the issues relating to human factors so that organisations can take necessary countermeasures before any incident materialises.

7.7 General Conclusions

The role of information security is expanding each day, and though IS has become a core pillar of the structure of enterprises, an ever growing number of security breaches causing enormous financial losses are observed. This is due to many reasons, although the increase in the complexity of information security systems has contributed greatly. As the impacts of security incidents on organisational performance are undeniable, determining the role of critical human factors has become more challenging. Senior managers feel that these challenges need to be addressed urgently and in the quickest possible time to satisfy firms' objectives, executive boards, business reputation and gain legal conformity to avoid legal penalties and fees. This also contributes to enterprise competiveness. Human factors bring great uncertainty and pose risks every stage. Such risks have adverse impacts on the achievement of ISS projects. Organisations should proactively make adequate, appropriate and intelligent decisions about controlling such risks. This research contributes a structured and clear method to support the analysis of human factors in the ISS

development process and enables ISS activities to be easily incorporated into the Requirements Engineering phase. The researcher believes that the risk-driven security investment model and its implementation has a strong impact on effective ISS practice in the information security domain.

Appendix 1: References

[1] Tipton, F. & Krause, M. 2008. Information Security Management Handbook, NW, Auerbach Publication.

[2] Buith, J. & Bootsma, H. 2006. TMT Global Security Survey 2006 [Online]. DeloitteDex. Available: https://www.deloitte.com/view/en_GX/global/industries/technology-media-telecommunications/11c22d3195ffd110VgnVCM100000ba42f00aRCRD.htm# [Accessed 04/06 2010].

[3] Alberts, C.J. and Dorofee, A., 2002. Managing information security risks: the OCTAVE approach. Addison-Wesley Longman Publishing Co., Inc..

[4] Corporation, S. 2013. Ponemon & Symantec Find Most Data Breaches Caused by Human and System Errors [Online]. Symantec Corporation. Available: http://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-digital.pdf [Accessed 15/06/2016].

[5] Layton, T. P. U. 2005. Information Security Awareness, Author House.

[6] Parker, D.B., 1999. Security motivation, the mother of all controls, must precede awareness. Computer Security Journal, 15, pp.15-24.

[7] Calder, A. and Watkins, S.G., 2010. Information security risk management for ISO27001/ISO27002. It Governance Ltd.

[8] Lacy, D. 2009. Managing the Human Factor in Information Security, How to win over staff and influence business managers, Chichester, John Wiley & Sons Ltd.

[9] W Krag Brotby, C. 2012. Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement, Taylor & Francis.

[10] Broderick, J.S., 2006. ISMS, security standards and security regulations. information security technical report, 11(1), pp.26-31.

[11] Vance, A., 2010. Why do employees violate is security policies? Insights from multiple theoretical perspectives. University of Oulu.

[12] G. Amoroso, E. 2011. Cyber Attacks Protecting National Infrastructure, Burlington, Elsevier Inc.

[13] Peters, S. 2015. The 7 Best Social Engineering Attacks Ever [Online]. Available: http://www.darkreading.com/the-7-best-social-engineering-attacks-ever/d/d-id/1319411?image_number=5 [Accessed 20/03/2015].

[14] Kraemer, S. & Carayon, P. 2006. An Adversarial Viewpoint of Human and Organizational Factors in Computer and Information Security: Final Report. Wisconsin-Madison: University of Wisconsin-Madison & Information Design Assurance Red Team (IDART), Sandia National Laboratories.

[15] MacEachren, A.M., Jaiswal, A., Robinson, A.C., Pezanowski, S., Savelyev, A., Mitra, P., Zhang, X. and Blanford, J., 2011, October. Senseplace2: Geotwitter analytics support for situational awareness. In Visual Analytics Science and Technology (VAST), 2011 IEEE Conference on (pp. 181-190). IEEE.

[16] Albrechtsen, E. & Hovden, J. 2010. Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. Computers & Security, 29**,** 432-445.

[17] Giorgini, P., Mouratidis, H. and Zannone, N., 2006. Modelling security and trust with secure tropos. Integrating Security and Software Engineering: Advances and Future Vision, pp.160-189.

[18] Willison, R., 2006. Understanding the perpetration of employee computer crime in the organisational context. Information and organization, 16(4), pp.304-324.

[19] (ISO), I. O. F. S. 2011. ISO/IEC 27005:2011 Information Security Management System (ISMS) Risk Management.

[20] (ISO), I. O. F. S. 2013. ISO/IEC 27001 - Information security management. Online International Organization for Standardization (ISO).

[21] Alavi, R., Islam, S. and Mouratidis, H., 2015. Human Factors of Social Engineering Attacks (SEAs) in Hybrid Cloud Environment: Threats and Risks. In Global Security, Safety and Sustainability: Tomorrow's Challenges of Cyber Security (pp. 50-56). Springer International Publishing.

[22] Stuart, B. H. 2007. Analytical techniques in materials conservation, John Wiley & Sons.

[23] Campbell, K., Gordon, L.A., Loeb, M.P. and Zhou, L., 2003. The economic cost of publicly announced information security breaches: empirical evidence from the stock market. Journal of Computer Security, 11(3), pp.431-448.

[24] Bryman, A. 2008. Social Research Methods, Oxford, Oxford University Press.

[25] O'hanley, R. & Tiller, J. S. 2014. Information Security Management Handbook Sixth Edition Volume 7, Boca Raton, Taylor & Francis Group, LLC.

[26] Matulevičius, R., Mayer, N. and Heymans, P., 2008, March. Alignment of misuse cases with security risk management. In Availability, Reliability and Security, 2008. ARES 08. Third International Conference on (pp. 1397-1404). IEEE.

[27] Sokol, A.H., 2013. NIST Cloud Computing Standards Roadmap. NIST Special Publication, pp.500-291.

[28] ISACA. 2009. An Introduction to the Business Model for Information Security. Available: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/An-Introduction-to-the-Business-Model-for-Information-Security.aspx [Accessed 01/03/2013].

[29] Rebollo, O., Mellado, D., Fernández-Medina, E. and Mouratidis, H., 2015. Empirical evaluation of a cloud computing information security governance framework. Information and Software Technology, 58, pp.44-57.

[30] Guo, J., Xu, L., Gong, Z., Che, C.P. and Chaudhry, S.S., 2012. Semantic inference on heterogeneous e-marketplace activities. Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on, 42(2), pp.316-330.

[31] Islam, S. and Dong, W., 2008, May. Human factors in software security risk management. In Proceedings of the first international workshop on Leadership and management in software architecture (pp. 13-16). ACM.

[32] Herzog, P. 2010. Security, trust, and how we are broken. ISECOM.

[33] Jahankhani, H., Fernando, S., Nkhoma, M.Z. and Mouratidis, H., 2007. Information systems security: Cases of network administrator threats. International Journal of Information Security and Privacy (IJISP), 1(3), pp.13-25.

[34] Lee, J., Chapin, S.J. and Taylor, S., 2002. Computational resiliency. Quality and Reliability Engineering International, 18(3), pp.185-199.

[35] Sarkar, K.R., 2010. Assessing insider threats to information security using technical, behavioural and organisational measures. information security technical report, 15(3), pp.112-133.

[36] Hadnagy, C. & Wilson, P. 2010. Social Engineering: The Art of Human Hacking, Wiley.

[37] Redmill, F., 2002. Human factors in risk analysis. Engineering Management Journal, 12(4), pp.171-176.

[38] Verizon Enterprise Solutions, .2014. 2014 Data Breach Investigations Report (DBIR).

[39] Puhakainen, P. 2006. A design theory for information security awareness. University of Oulu.

[40] Janczewski, L.J. and Fu, L., 2010, October. Social engineering-based attacks: Model and new zealand perspective. In Computer Science and Information Technology (IMCSIT), Proceedings of the 2010 International Multiconference on (pp. 847-853). IEEE.

[41] Siponen, M., Pahnila, S. and Mahmood, M.A., 2010. Compliance with information security policies: an empirical investigation. Computer, 43(2), pp.64-71.

[42] Greitzer, F.L., Strozer, J.R., Cohen, S., Moore, A.P., Mundie, D. and Cowley, J., 2014, May. Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits. In Security and Privacy Workshops (SPW), 2014 IEEE (pp. 236-250). IEEE.

[43] Karpati, P., Sindre, G. and Matulevicius, R., 2012. Comparing misuse case and mal-activity diagrams for modelling social engineering attacks. International Journal of Secure Software Engineering (IJSSE), 3(2), pp.54-73.

[44] Jagatic, T.N., Johnson, N.A., Jakobsson, M. and Menczer, F., 2007. Social phishing. Communications of the ACM, 50(10), pp.94-100.

[45] Shakarian, P., Shakarian, J. and Ruef, A., 2013. Introduction to cyber-warfare: A multidisciplinary approach. Newnes.

[46] ISO, I., 2009. 31000: 2009 Risk management–Principles and guidelines. International Organization for Standardization, Geneva, Switzerland.

[47] Mayer, N., Heymans, P. and Matulevicius, R., 2007. Design of a Modelling Language for Information System Security Risk Management. In RCIS (pp. 121-132).

[48] Brecht, M. and Nowey, T., 2013. A closer look at information security costs. In The Economics of Information Security and Privacy (pp. 3-24). Springer Berlin Heidelberg.

[49] Chai, S., Kim, M. and Rao, H.R., 2011. Firms' information security investment decisions: Stock market evidence of investors' behavior. Decision Support Systems, 50(4), pp.651-661.

[50] Brotby, W.K. and Hinson, G., 2013. PRAGMATIC Security Metrics: Applying Metametrics to Information Security. CRC Press.

[51] Iivari, J. and Hirschheim, R., 1996. Analyzing information systems development: A comparison and analysis of eight IS development approaches. Information Systems,

21(7), pp.551-575.

[52] Bagchi, K. and Udo, G., 2003. An analysis of the growth of computer and Internet security breaches. Communications of the Association for Information Systems, 12(1), p.46.

[53] Aitoro, J. R. 2008. OMB reports 60 percent increase in information security incidents [Online]. GOVERNMENTEXECUTIVE.com. Available: http://www.govexec.com/dailyfed/0308/030208a1.htm [Accessed 15/09 2009].

[54] Hayden, L., 2009. Human information security behaviors: Differences across geographies and cultures in a global user survey. Proceedings of the American Society for Information Science and Technology, 46(1), pp.1-16.

[55] Blackler, F. and Brown, C., 1986. Alternative models to guide the design and introduction of the new information technologies into work organizations. Journal of Occupational Psychology, 59(4), pp.287-313.

[56] Palvia, S.C., Sharma, R.S. and Conrath, D.W., 2001. A socio-technical framework for quality assessment of computer information systems. Industrial Management & Data Systems, 101(5), pp.237-251.

[57] Straub Jr, D.W., 1990. Effective IS security: An empirical study. Information Systems Research, 1(3), pp.255-276.

[58] D'Arcy, J., Hovav, A. and Galletta, D., 2009. User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. Information Systems Research, 20(1), pp.79-98.

[59] Beatson, J.G., 1991. Security-a personnel issue. The importance of personnel attitudes and securityeducation. In Proceedings of the Sixth IFIP International Conference on ComputerSecurity.

[60] Kun, L.G. and Bray, D.A., 2002. Information infrastructure tools for bioterrorism preparedness. Engineering in Medicine and Biology Magazine, IEEE, 21(5), pp.69-85.

[61] Tricker, R. I. 1984. Corporate Governance: Practices, Procedures and Powers in British Companies and Their Boards of Directors, Aldershot, UK, Gower Press.

[62] Appelbaum, S.H., 1997. Socio-technical systems theory: an intervention strategy for organizational development. Management Decision, 35(6), pp.452-463.

[63] Denning, D. E. 1999. Information Warfare and Security ACM Press. New York, NY, USA.

[64] Desman, M.B., 2001. Building an information security awareness program. CRC Press.

[65] Pavlidis, M., 2011. Designing for Trust. In CAiSE (Doctoral Consortium) (pp. 3-14).

[66] Bulgurcu, B., Cavusoglu, H. and Benbasat, I., 2009. Roles of information security awareness and perceived fairness in information security policy compliance. AMCIS 2009 Proceedings, p.419.

[67] Mitnick, K.D. and Simon, W.L., 2011. The art of deception: Controlling the human element of security. John Wiley & Sons.

[68] St Amant, K., Still, B. and Reed, S., 2007. Handbook of research on open source software.

[69] Dwivedi, P. and Alavalapati, J.R., 2009. Stakeholders' perceptions on forest biomass-based bioenergy development in the southern US. Energy Policy, 37(5), pp.1999-2007.

[70] Okoli, C. and Pawlowski, S.D., 2004. The Delphi method as a research tool: an example, design considerations and applications. Information & management, 42(1), pp.15-29.

[71] Mulligan, P., 2002. Specification of a capability-based IT classification framework. Information & Management, 39(8), pp.647-658.

[72] Maitland, N.B. and Osei-Bryson, K.M., 2014. Hybrid VFT/Delphi Method to Facilitate the Development of Information Security Strategies in Developing Countries.

[73] Knight, M. and Dennis, O., 1999. I. The 20th Century and Works Covering More Than one of Divisions II–V. Alm, 130, p.32.

[74] Lewin, K., 1943. Defining the'field at a given time.'. Psychological review, 50(3), p.292.

[75] Schein, E.H., 1996. Kurt Lewin's change theory in the field and in the classroom: Notes toward a model of managed learning. Systems practice, 9(1), pp.27-47.

[76] Al-Awadi, M. and Renaud, K., 2007, July. Success factors in information security implementation in organizations. In IADIS International Conference e-Society.

[77] Carstens, B.C., Stevenson, A.L., Degenhardt, J.D. and Sullivan, J., 2004. Testing nested phylogenetic and phylogeographic hypotheses in the Plethodon vandykei species group. Systematic Biology, 53(5), pp.781-792.

[78] Loucopoulos, P. and Karakostas, V., 1995. System requirements engineering. McGraw-Hill, Inc..

[79] Beckers, K., Faßbender, S., Heisel, M., Küster, J.C. and Schmidt, H., 2012. Supporting the development and documentation of ISO 27001 information security management systems through security requirements engineering approaches. In Engineering secure software and systems (pp. 14-21). Springer Berlin Heidelberg.

[80] Mouratidis, H., Giorgini, P. and Manson, G., 2004. Using security attack scenarios to analyse security during information systems design.

[81] Mouratidis, H. and Giorgini, P., 2004. Analysing security in information systems.

[82] Rajasekar, S., Philominathan, P. and Chinnathambi, V., 2006. Research methodology. arXiv preprint physics/0601009.

[83] Guo, J., Hu, Z., Chan, C.K., Luo, Y. and Chan, C., 2008, August. Document-oriented heterogeneous business process integration through collaborative e-marketplace. In Proceedings of the 10th international conference on Electronic commerce (p. 39). ACM.

[84] Adams, A. and Sasse, M.A., 1999. Users are not the enemy. Communications of the ACM, 42(12), pp.40-46.

[85] Avižienis, A., Laprie, J.C., Randell, B. and Landwehr, C., 2004. Basic concepts and taxonomy of dependable and secure computing. Dependable and Secure Computing, IEEE Transactions on, 1(1), pp.11-33.

[86] Besnard, D. and Arief, B., 2004. Computer security impaired by legitimate users. Computers & Security, 23(3), pp.253-264.

[87] Wilson, M. and Hash, J., 2003. Building an information technology security awareness and training program. NIST Special publication, 800, p.50.

[88] Ernst and Young. 2008. 10th Annual Global Information Security Survey Achieving a Balance of Risk and Performance. London. UK. Ernst and Young.

[89] Siponen, M.T., 2000. A conceptual foundation for organizational information security awareness. Information Management & Computer Security, 8(1), pp.31-41.

[90] Aytes, K. and Conolly, T., 2003. A research model for investigating human behavior related to computer security. AMCIS 2003 Proceedings, p.260.

[91] Werlinger, R., Hawkey, K. and Beznosov, K., 2009. An integrated view of human, organizational, and technological challenges of IT security management. Information Management & Computer Security, 17(1), pp.4-19.

[92] Briggs, R., Edwards, C. and Pickard, J., 2006. The business of resilience: corporate security for the 21st century. Demos.

[93] Leek, S., Turnbull, P.W. and Naude, P., 2003. How is information technology affecting business relationships? Results from a UK survey. Industrial marketing management, 32(2), pp.119-126.

[94] Chalmers, D., 2004. The representational character of experience. The future for philosophy, pp.153-181.New York: Oxford University Press.

[95] Parkin, S.E., van Moorsel, A. and Coles, R., 2009, October. An information security ontology incorporating human-behavioural implications. In Proceedings of the 2nd International Conference on Security of Information and Networks (pp. 46-55). ACM.

[96] Thomson, K. and van Niekerk, J., 2012. Combating information security apathy by encouraging prosocial organisational behaviour. Information Management & Computer Security, 20(1), pp.39-46.

[97] Kabay, M.E., Robertson, B., Akella, M. and Lang, D.T., 2002. Using social psychology to implement security policies. Computer Security Handbook, Sixth Edition, pp.50-1.

[98] Bartol, K. and Martin, D. 1994. Management, New York, McGraw- Hill Inc.

[99] Schein, E. H. 1999. The Corporate Culture Survival Guide. San Francisco: Jossey-Bass.

[100] Vroom, C. and Von Solms, R., 2004. Towards information security behavioural compliance. Computers & Security, 23(3), pp.191-198.

[101] Bequai, A., 1998. Balancing legal concerns over crime and security in cyberspace. Computers & Security, 17(4), pp.293-298.
[102] Tudor, J. K. 2001. An integrated approach to security in the organization. Information Security Architecture.

[103] Kankanhalli, A., Teo, H.H., Tan, B.C. and Wei, K.K., 2003. An integrative study of information systems security effectiveness. International journal of information management, 23(2), pp.139-154.
[104] Bazavan, I.V. and Lim, I., 2006. Information security cost management. CRC Press. NW, Auerbach Publications.

[105] Islam, S. and Falcarin, P., 2011, September. Measuring security requirements for software security. In Cybernetic Intelligent Systems (CIS), 2011 IEEE 10th International Conference on (pp. 70-75). IEEE.

[106] Dhillon, G. and Backhouse, J., 2000. Technical opinion: Information system

security management in the new millennium. Communications of the ACM, 43(7), pp.125-128.

[107] Ruighaver, A.B., Maynard, S.B. and Chang, S., 2007. Organisational security culture: Extending the end-user perspective. Computers & Security, 26(1), pp.56-62.

[108] Lim, J.S., Ahmad, A., Chang, S. and Maynard, S.B., 2010. Embedding Information Security Culture Emerging Concerns and Challenges. In PACIS (p. 43).

[109] Pattinson, M.R. and Anderson, G., 2007. How well are information risks being communicated to your computer end-users?. Information Management & Computer Security, 15(5), pp.362-371.

[110] Ericsson, G.N., 2010. Cyber security and power system communication—essential parts of a smart grid infrastructure. Power Delivery, IEEE Transactions on, 25(3), pp.1501-1507.

[111] Chenine, M., Ullberg, J., Nordstrom, L., Wu, Y. and Ericsson, G.N., 2014. A Framework for Wide-Area Monitoring and Control Systems Interoperability and Cybersecurity Analysis. Power Delivery, IEEE Transactions on, 29(2), pp.633-641.

[112] Vacca, J.R., 2012. Computer and information security handbook. Newnes.

[113] Jordan, E. and Fung, P., 2002. Implementation of Information Security: A Knowledge-based Approach. PACIS 2002 Proceedings, p.40.

[114] Von Solms, R., 1999. Information security management: why standards are important. Information Management & Computer Security, 7(1), pp.50-58.

[115] Yeh, Q.J. and Chang, A.J.T., 2007. Threats and countermeasures for information system security: A cross-industry study. Information & Management, 44(5), pp.480-491.

[116] Versteeg, G. and Bouwman, H., 2006. Business architecture: A new paradigm to relate business strategy to ICT. Information Systems Frontiers, 8(2), pp.91-102.

[117] Hovav, A. and D'arcy, J., 2005. Capital market reaction to defective IT products: The case of computer viruses. Computers & Security, 24(5), pp.409-424.

[118] Von Faisst, U., Prokein, D.V.O. and Wegmann, D.K.N., 2007. Ein Modell zur dynamischen Investitionsrechnung von IT-Sicherheitsmaßnahmen. Zeitschrift für Betriebswirtschaft, 77(5), pp.511-538.

[119] Haralambos Mouratidis, H.M. and Giorgini, P., 2007. Integrating security and software engineering: advances and future visions.

[120] Van Lamsweerde, A., 2009. Requirements engineering: from system goals to UML models to software specifications.

[121] Gordon, L.A., Loeb, M.P. and Zhou, L., 2011. The impact of information security breaches: Has there been a downward shift in costs?. Journal of Computer Security, 19(1), pp.33-56.

[122] Brykczynski, B. and Small, R.A., 2003. Reducing internet-based intrusions: Effective security patch management. Software, IEEE, 20(1), pp.50-57.

[123] Runeson, P. and Höst, M., 2009. Guidelines for conducting and reporting case study research in software engineering. Empirical software engineering, 14(2), pp.131-164.

[124] Al Hogail, A., 2015. Cultivating and Assessing an Organizational Information Security Culture; an Empirical Study. International Journal of Security and Its Applications, 9(7), pp.163-178.

[125] Young, R.F., 2008. Defining the information security posture: an empirical examination of structure, integration and managerial effectiveness (Doctoral dissertation, University of North Texas).

[126] Pfleeger, S.L. and Kitchenham, B.A., 2001. Principles of survey research: part 1: turning lemons into lemonade. ACM SIGSOFT Software Engineering Notes, 26(6), pp.16-18.

[127] Easterbrook, S., Singer, J., Storey, M.A. and Damian, D., 2008. Selecting empirical methods for software engineering research. In Guide to advanced empirical software engineering (pp. 285-311). Springer London.

[128] Sjoberg, D.I., Dyba, T. and Jorgensen, M., 2007, May. The future of empirical methods in software engineering research. In 2007 Future of Software Engineering (pp. 358-378). IEEE Computer Society.

[129] Okoli, C. and Pawlowski, S.D., 2004. The Delphi method as a research tool: an example, design considerations and applications. Information & management, 42(1), pp.15-29.

[130] Maitland, N.B. and Osei-Bryson, K.M., 2014. Hybrid VFT/Delphi Method to Facilitate the Development of Information Security Strategies in Developing Countries.

[131] Verizon Enterprise Solutions, .2016. 2016 Data Breach Investigations Report (DBIR).

[132] Carnegie Mellon University, SEI (Software Engineering Institute) [Online] Available: www.cert.org/octave/osig.html. [Accessed 25/06/2016].

[133] Turris, S.A., Steenkamp, M., Lund, A., Hutton, A., Ranse, J., Bowles, R., Arbuthnott, K., Anikeeva, O. and Arbon, P., 2016. International consensus on key concepts and data definitions for mass-gathering health: process and progress. Prehospital and disaster medicine, 31(2), pp.220-223.

[134] Powell, C., 2003. The Delphi technique: myths and realities. Journal of advanced nursing, 41(4), pp.376-382.

[135] Flick, U., von Kardoff, E. and Steinke, I. eds., 2004. A companion to qualitative research. Sage. Vancouver.

[136] Iverson, D., 2013. Strategic risk management: a practical guide to portfolio risk management (Vol. 1). John Wiley & Sons.

[137] Alavi, R., Islam, S., Jahankhani, H. & Al-Nemrat, A. 2013. Analyzing Human Factors for an Effective Information Security Management System. International Journal of Secure Software Engineering (IJSSE), 4, 50-74.

Appendix 2: Interview Questions (Open Questions)

Our interviewees were included the following stakeholders:

1) Senior executives
2) Senior managers
3) Middle managers
4) Employees

Each group interviewed with questions that were related to their positions. However, some questions were common. The following questions were formulated:

1. How your role fits in your organization and what role do you play in design and implementation of ISS in your organisation and whether it reports up via the CIO/CTO/CISO? IS your role technology, risk or business aligned? Could you please elaborate your answer?

2. Do you cover all the key areas of ISS and regulation in the training programmes in your organisation and are they current in terms of recognised threats (in your knowledge)?

3. Do you have any IS awareness programme in your organisation and do you find them efficient and effective? Do they response to your needs in dealing with IS issues?

1.1

4. How would you describe the culture of your organization in terms of its security risk appetite? Do you find your organisation culture being in line with IS policies and procedures?

5. How do you socialise proposed policies to ensure that employees don't adversely impact the business? In the other words, how far do employees get involved in policy implementation? Can you give me any examples?

6. How would you describe your practical knowledge in the IS field? Could you please give me any examples?

7. Do you feel that you are encouraged to response to the IS policies or feel reluctant (apathy) to implement them? Could you give me an example?

8. Do you have any incentive policy in your organisation to reward your engagement for the following of ISS? Could you give me an example and elaborate your response?

9. Do you believe there are deliberate acts in your organisation for sabotaging the ISS?

10. Do you feel under pressure from the IS policies and procedures? If yes, how would you see this impacts on your IS practices?

11. Are you convinced that your organisation allocates a reasonable budget to deal with IS issues? Could you estimate the proportion of budget or manpower resource given over to technical rather than people and softer areas?

12. Could you provide any examples of where employees have provided feedback on security policies and standards?
    12.1 Have you been able to respond to these suggestions?
    12.2 Are such feedback mechanisms formal or informal and how are they encouraged?

13. Is there a senior management led security committee and how does it interface to the board/executive Committee?
    13.1 Do technologists lead it and does it have appropriate business representation?
14. Does the board of governance support information security initiatives?
    14.1How could IS effectiveness in this support and engagement be measured?

15. What measurements has your organization considered to address the so-called "Enemy within" or rogue employee factor without alienating people?
    15.1 When such incidents are found and acted upon, are they publicised? Is there a policy?
16. How do you describe the communication between senior managers and the rest of the people in your organisation, in regards to ISS?

17. Do you think that the IS policy enforcement in your organisation is fully implemented and it is adequate?

18. Do you feel that you receive right level of support from senior management in regards to ISS? Please elaborate your response and give example.

19. How do you demonstrate to the board that information security has value? Do you use the risk concepts in this process and if yes, do they help?

20. How do you justify the information security budget requirements to the board? Do you the return of investment concept and if yes, do you use any specific method/s?

Questions	Position	Senior Executives	Senior Managers	Middle Managers	Employees
Q1		✓	✓	✓	✓
Q2		✓	✓	✓	✓
Q3		✓	✓	✓	✓
Q4		✓	✓	✓	✓
Q5		✓	✓	✓	✓
Q6				✓	✓
Q7		✓	✓	✓	✓
Q8		✓	✓	✓	✓
Q9				✓	✓
Q10		✓	✓	✓	✓
Q11		✓	✓	✓	
Q12		✓	✓		
Q13		✓			
Q14		✓	✓		
Q15		✓	✓	✓	✓
Q16		✓	✓	✓	✓
Q17				✓	✓
Q18				✓	✓
Q19		✓	✓		
Q20		✓	✓		

Appendix 3: Survey Study (Closed Questions)

Survey Study

---

1) **What is the title of the person performing the Information Security Officer role at your institution?**

- ○ Chief Information Officer / IT Director
- ○ Chief Information Security Officer
- ○ Chief Security Officer
- ○ Chief Compliance Officer
- ○ Chief Risk Officer
- ○ None - we don't have that role
- ○ Other: _____

2) **To whom does the person performing the Information Security Officer role report?**

- ○ Chief Executive Officer / President
- ○ Chief Information Officer / IT Director / Technology Manager
- ○ Board of Directors / Audit Committee
- ○ Chief Risk Officer
- ○ Chief Compliance Officer
- ○ Chief Security Officer
- ○ Chief Auditor
- ○ Other: _____

3) **What are your greatest spending priorities?**
Check all that apply:

- ☐ Regulatory Compliance Improvements
- ☐ Risk Management Improvements
- ☐ Staff
- ☐ Contractors/Third-Party Service Providers
- ☐ Training
- ☐ Customer Awareness
- ☐ New Services
- ☐ New Branch Servicing

- ☐ Emerging Technologies
- ☐ Other: _____

4) **How do you grade your institution's ability to counter external and internal information security threats?**

_____

5) **How do you assess your customers' confidence in your institution's ability to safeguard their financial and informational assets?**

_____

6) **Which types of fraud have you experienced over the past year?**
Check all that apply:

- ☐ ATM
- ☐ ACH
- ☐ Credit/Debit Card
- ☐ Payments
- ☐ Insider
- ☐ Wire
- ☐ Other: _____

7) **Which area of fraud do you feel best prepared to prevent?**

- ○ ATM
- ○ ACH
- ○ Credit/Debit Card
- ○ Payments
- ○ Wire
- ○ Insider
- ○ Other: _____

8) **How important do you see the support of senior management on security related issue?**

_____

9) **What do you find most effective in information security policy?**
Check all that apply

- [ ] Communication
- [ ] Awareness
- [ ] Management Support

Other:

10) Please prioritise your responses in question 9:

11) How many awareness and training session you provided last year?

12) How do you assess the success of your organisation's training and awareness plans?

- ○ We deployed them, and it worked as expected
- ○ We deployed them, and it did not work as expected
- ○ We deployed them, but have not yet assessed its success
- ○ We did not deploy them
- ○ We do not have a defined plan
- ○ Other:

13) On a scale of 1-5 (1 low, 5 high), how do your rate your confidence in the security controls maintained by your institution?

14) On a scale of 1-5 (1 low, 5 high), how do your rate your institution's success in dealing with issues related to people?

15) On a scale of 1-5 (1 low, 5 high), how do you rate your institution's success in training programs?

16) On a scale of 1-5 (1 low, 5 high), how do your rate your institution's success in monitoring insider threats?

17) How do you expect regulation to impact human factors in your organisation's security policy?

18) Does your organization use a social networking for communication?

19) Does your organization have a social networking policy for employees?

20) Do you monitor your employees' social networking activity?

21) Does your organisation provide separate awareness activities for employees and senior managers?

22) If you answered the last question yes, how do you grade the effectiveness of your security training and awareness activities for employees?

23) How do you grade the effectiveness of your security training and awareness activities for the board/senior management?

---

24) Beyond "additional resources," what one factor could have the biggest positive impact on information security in your organisation?

- Regulatory Compliance
- Emerging Technologies
- Policies and Procedures
- Training and Education
- Employee Awareness
- Customer Awareness
- Management Support
- Communication
- Other:

25) Considering your response to question 6, how much this incident cost in regards to affected areas such as, data, servers or business process?

26) Considering your response to question 6, how much this incident cost in regards to new purchases, external cost, employee, legal and insurance excess?

27) Considering your response to question 6, how much cost covered by insurance policy?

28) Considering your response to question 6, how much lost of revenue impacted you from potential clients/customers?

29) Considering your response to question 6, are you aware of any other cost? If yes, how much?

30) Please add any comments you may have about the questions or anything else you'd like to add about your organisation's security appetite and policy.

If you would like to be notified of survey results, please provide your email address in the box below: