TOWARDS A COMPREHENSIVE EVIDENCE-BASED APPROACH FOR INFORMATION SECURITY VALUE ASSESSMENT

Daniel Schatz

University of East London

School of Architecture, Computing & Engineering

This dissertation is submitted in partial fulfilment for the degree of

Doctor of Philosophy

December 2018

ABSTRACT

This thesis is motivated by the goals of understanding in depth which information security value aspects are relevant in real-world business environments and contributing a value-prioritised information security investment decision model suitable for practitioners in the field. Pursuing this goal, we apply a mixed method research approach that combines the analysis of the relevant literature, expert interviews, practitioner survey data and structural equation modelling and multicriteria decision analysis. In the first step, we address the identified terminology gap to clarify the meaning of 'cyber security' by analysing authoritative definition sources in the literature and presenting an improved definition distinct from that of 'information security'. We then investigate the influence of repeated information security breaches on an organisation's stock market value to benchmark the wider economic impact of such events. We find abnormal returns following a breach event as well as weak statistical significance on abnormal returns for later breach events, confirming that data breaches have a negative impact on organisations. To understand how security practitioners view this topic, we conduct and analyse semi-structured interviews following a grounded theory approach. Our research identifies 15 principles aligned with a conceptual information security investment framework. The key components of this framework such as the business environment, drivers (*threat landscape, legal and regulatory*) and challenges (*cost of security, uncertainty)* are found to be a crucial part of value-prioritised information security investment decisions. We verify these findings through a structural model consisting of five latent variables representing key areas in value-focused information security investment decisions. The model shows that security capabilities have the largest direct effect on the value organisations gain from information security investment. In addition, the value outcome is strongly influenced by organisation-specific constructs such as the threat landscape and regulatory requirements, which must therefore be considered when creating security capabilities. By addressing one of the key uncertainty issues, we use a probabilistic topic modelling approach to identify latent security threat prediction topics from a large pool of security predictions publicised in the media. We further verify the prediction outcomes through a survey instrument. The results confirm the feasibility of forecasting notable threat developments in this context, implying that practitioners can use this approach to reduce uncertainty and improve security investment decisions. In the last part of the thesis, we present a multicriteria decision model that combines our results on

value-prioritised information security investments in an organisational context. Based on predefined criteria and preferences and by utilising stochastic multicriteria acceptability analysis as the adopted methodology, our model can deal with substantial uncertainty while offering ease of use for practitioners.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF PUBLICATIONS

Schatz, D. and R. Bashroush (2016). "Economic valuation for information security investment: a systematic literature review." Information Systems Frontiers: 1-24. **Based on Chapter 2**

Schatz, D., Bashroush, R., Wall, J. (2017). "Towards a More Representative Definition of Cyber Security." Journal of Digital Forensics, Security and Law **12**(2): 8. **Based on Chapter 3**

Schatz, D. and R. Bashroush (2016). "The impact of repeated data breach events on organisations' market value." Information and Computer Security **24**(1): 73-92. **Based on Chapter 4**

Schatz, D. and R. Bashroush (2018). "Corporate Information Security Investment Decisions: A Qualitative Data Analysis Approach." International Journal of Enterprise Information Systems (IJEIS) **14**(2): 1-20. **Based on Chapter 5**

Schatz, D. (2016). "Security Predictions 2016: A Data Analysis Approach." ISACA Journal **4**. **Based on Chapter 6**

Schatz, D. and R. Bashroush (2017). "Security Predictions – A Way To Reduce Uncertainty." Manuscript submitted for publication. **Based on Chapter 6**

Schatz, D. and R. Bashroush (in press). "A structural model approach for assessing information security value in organizations." International Journal of Strategic Decision Sciences. **Based on Chapter 7**

Schatz, D. and R. Bashroush (2018). "Structured multi criteria decision making in value prioritised security investments" Manuscript submitted for publication. **Based on Chapter 8**.

ACKNOWLEDGEMENTS

I would like to thank those who made this research possible. I thank my wife and family for their support and patience that allowed me to complete this research. I'm grateful to my supervisors Dr. Rabih Bashroush and Dr. Julie Wall for their guidance and academic support. In addition, I'd like to thank Dr. David Preston for his help and encouragement. Finally, I'm grateful to all colleagues and peers who volunteered their experience and expertise without which this research would not have been possible.

1 INTRODUCTION

In our modern economy, information is rapidly becoming one of the most important assets in global markets. It is no longer just a by-product, but rather a driver of new and improved business models that generates considerable value. Hence, interest in this area is increasing just as rapidly—and not just in legitimate businesses (The Economist, 2017). Criminals are quick to spot opportunities and are adapting to these new value streams. Indeed, organised crime is embracing and exploiting billions of dollars of digital opportunities (Dethlefs, 2015; Hyman, 2013; Ponemon Institute, 2017). With losses at this magnitude and still rising, the importance of protecting information assets is apparent.

The security of information assets in organisations has been a research subject for many years (Badenhorst & Eloff, 1990; Blakley, McDermott, & Geer, 2001; K. D. Loch, Carr, & Warkentin, 1992; Siponen & Oinas-Kukkonen, 2007), largely focusing on technology and technological risks. This research foundation has helped professional institutions build topic-specific bodies of knowledge that guide information security practitioners on how to protect information in their organisations. However, the question is not just how to protect, but how much resources to spend on the protection of information (Hoo, 2000). Despite early research on the economic aspects of information security (Ekenberg, Oberoi, & Orci, 1995), academic research was rather limited until the turn of the millennium when the papers by Anderson (2001) and Gordon and Loeb (2002a) raised interest in this topic.

Today, information security is among the top concerns for policymakers and corporate board members. They demand answers from their support structures as to how information security risks can be managed effectively (Clinton, 2014). In contrast to, for example, the physical security space, answers on impact and cost are not straightforward to ascertain because the rapid developments in information security leave subject matter experts with limited historical data to support reliable risk models (Shetty et al., 2018). In the absence of such data, information security professionals rely on subjective knowledge (i.e. expert judgement), assumptions, vendor recommendations and industry best practices to manage information security risks. The result is a battle on several fronts. It involves the challenge to understand the current and future threats to organisations' information assets, prioritise those with the highest probability to be realised on the highest valued assets and investigate the value propositions of countermeasures. Not only is this a highly complex undertaking based on estimates and assumptions, it is merely the preamble to proving that the selected control investment is worth doing. The security practitioner must therefore justify the investment in security controls by showing the value it adds compared with the other projects in the organisation competing for the same pot of money.

In basic terms, security value can be seen as the combination of end result from benefits and costs associated with maintaining the security and integrity of the organisation (Dhillon & Torkzadeh, 2006). In less simplistic terms, value at organisational level is represented through an organisation specific value focused view which takes a more abstract form, considering fundamental objectives valued by the decision maker (Keeney, 1994). This value view is investigated in detail throughout this thesis, particularly in chapters 2 and 5. Taking a resource-based position on value (Bowman & Ambrosini, 2000; Lepak, Smith, & Taylor, 2007) we view information security through the service dominant prism with value defined in terms of an improvement in system well-being which can be measured in terms of a system's adaptiveness or ability to fit in its environment (Vargo, Maglio, & Akaka, 2008).

1.1 Research Questions

Several academic models have been proposed to assess the value and economic benefit of information security investments, each with their various challenges, benefits, practicability and scope. As we will find in this research, many of the models, particularly those of earlier approaches, are largely theoretical, leaving the practical challenges unmentioned or unsolved. While such models do contribute to achieving a better approach towards information security investments, their theoretical nature makes them only applicable to a limited subset of information security scenarios. In other words, they do not address the real-world challenges or scenarios practitioners face as found by our research (Chapter 5). Further, while research in this area is developing, leading to ever-improving approaches, it also contributes to the proliferation of niche solutions. This makes it difficult for practitioners to identify and select a useful methodology to adopt. Moreover, it is further complicated by blurred definitions between models focusing on the economic aspects of organisational information security (i.e. the micro level) and those dealing with cyber security questions at the macro level. Hence, the focus and motivation of this research is to provide a value-prioritised information security investment decision model suitable for practitioners in the field.

To address the noted challenges and gaps, the research investigates the following overarching questions:

I. What do we mean by cyber security and how does it differ from information security?

II. Which information security value models are currently proposed to manage and evaluate information security investments in organisations?

III. What are the key factors relevant to information security investments and do these diverge, conflict or harmonise across models?

IV. How do information security practitioners view the topic of information security value? What factors are relevant in the real world?

V. Which of the gaps identified in the research questions would, if addressed or resolved, lead to advancement in this space?

1.2 Objectives

The goals of the investigation are thus to

- Define the difference between cyber security and information security to delineate security investments beneficial at the micro and macro levels
- Gain an exhaustive understanding of the information security value aspects relevant in real-world environments by following a convergent qualitative quantitative mixed method research approach

- Investigate and evaluate a way in which to reduce uncertainty in information security risk decisions
- Identify latent structures and apply the results to create a value-prioritised information security investment model that is usable, relevant and applicable to real-world decision scenarios

1.3 Methodology

To achieve the objectives described above, a thorough and robust research approach is followed in which we

- Analyse the current authoritative definitions of cyber security
- Observe and analyse the economic impact of security incidents on market value
- Review the models and practices proposed in the academic and professional literature to evaluate information security investments at the micro level
- Gather and analyse primary data on information security value assessment through semi-structured interviews and surveys
- Decompose and analyse existing models and practices highlighting issues, dis/advantages and shortcomings to identify gaps or similarities
- Investigate and reassemble latent structures and key components in the context of information security value to create a value-prioritised multicriteria decision model

The overall research followed a general research cycle approach inspired by action research (McNiff & Whitehead, 2011). The research cycle was consulted at key points during the work to re-evaluate the problem space, adjust the research goals and plan as well as reflect on the findings. This led to the adjustment of the plan as well as the extension of the research to address specific problem areas such as ambiguous terminology and uncertainty in the threat landscape. This research thus represents the outcome of a full research cycle. However, the concluding reflection step inevitably leads to new ideas for improving the model and the realisation that the information security landscape is in constant flux.

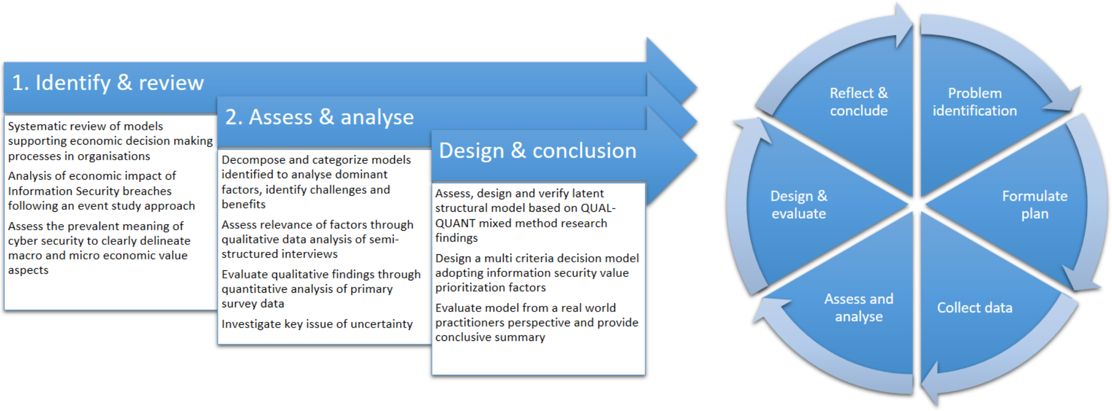

1. Identify & review
Systematic review of models supporting economic decision making processes in organisations
Analysis of economic impact of Information Security breaches following an event study approach
Assess the prevalent meaning of cyber security to clearly delineate macro and micro economic value aspects
2. Assess & analyse
Decompose and categorize models identified to analyse dominant factors, identify challenges and benefits
Assess relevance of factors through qualitative data analysis of semi-structured interviews
Evaluate qualitative findings through quantitative analysis of primary survey data
Investigate key issue of uncertainty
Design & conclusion
Assess, design and verify latent structural model based on QUAL-QUANT mixed method research findings
Design a multi criteria decision model adopting information security value prioritization factors
Evaluate model from a real world practitioners perspective and provide conclusive summary
Reflect & conclude
Problem identification
Formulate plan
Collect data
Assess and analyse
Design & evaluate

Figure 1 - Research steps and lifecycle

As illustrated in Figure 1, the first phase of the research investigated the general question of impact, reviewed the state of the proposed models and clarified the cyber security terminology. The systematic literature review (SLR) provided the basis for the decomposition and categorisation of current economic evaluation approaches and frameworks. SLRs provide a structured method for critically examining, interpreting and evaluating the entirety of current research evidence in a certain field or area, leveraging a strict framework and predefined questions (Kitchenham & Charters, 2007). On the impact investigation a event study methodology approach was followed. Event study is a statistical approach relying on the assumption of efficient markets to identify abnormal returns resulting from an event. (MacKinlay, 1997) explains that the usefulness of such a study stems from the fact that, given rationality in the marketplace, the effects of an event will be reflected immediately in security prices. To assess the definitions of cyber security, we apply basic text analysis as well as semantic similarity methods (Hearst, 1999). We consider initial lexical form of the token, lemma form of the word, part-of-speech (POS), weighted specificity of the word, semantic representation (Martin & Berry, 2007; G. A. Miller, 1995) and a list of syntactic dependencies with the other words in the same sentence (Lintean, 2011). To capture as much context as possible, we chose StanfordNLP (De Marneffe, MacCartney, & Manning, 2006) as the configuration option for tokenization, POS tagging, lemmatizer as well as syntactic parsing.

In phase two, primary data were obtained through qualitative (semi-structured interviews) and quantitative methods (surveys). In our interviews, we investigated how practitioners approach information security investments in their work environments. As this requires interaction and close cooperation with practitioners in the field, we chose a qualitative research approach to emphasise the lived experience; this approach is also suitable for locating meaning and connecting such meaning to the social world (Miles & Huberman, 1994).

Grounded theory (Glaser, Strauss, & Strutzel, 1968) is a suitable approach for this research. Hence, we combined the results of our qualitative analysis with the findings of the SLR to gather further primary data from practitioners in a survey that captured which aspects of information security value decisions are most relevant from their perspective. We then used partial least squares structural equation modelling (PLS-SEM) to test a conceptual model derived from our mixed methods research. The core of PLS is a family of alternating least squares algorithms that emulate and extend principal component analysis as well as canonical correlation analysis (Henseler, Hubona, & Ray, 2016). It is an appropriate choice for our research. As described by Hair Jr, Hult, Ringle, and Sarstedt (2016), it is particularly useful for studies of the sources of competitive advantage and key success factors as it can predict and identify the target constructs. This is desirable because research on information security economics is relatively new and the theoretic fundamentals are still under development. PLS-SEM is advantageous when the structural model is complex and the constructs have many or very few indicators. Also, it can work with non-normally distributed data (Roldán & J. Sánchez-Franco, 2012).

In the third phase of the research, the results of previous work were combined to create a multicriteria decision model for value-prioritised information security investments.

Multicriteria decision making can be described as a collection of formal approaches adopted to explore complex decision matters considering multiple, typically conflicting, criteria of both a quantitative and a qualitative nature. Based on the work by Keeney and Raiffa (1976) as well as the seminal paper by Zionts (1979), multicriteria decision making is built on decision theory and notably driven by Operational Research. Liou and Tzeng (2012) provide an excellent overview of recent development in this space; see also Greco, Ehrgott, and Figueira (2016) for an extensive survey on this matter. We use Stochastic Multiobjective Acceptability Analysis (SMAA) to support our model with MCDA utilising the inputs as described in the respective chapters. Introduced in (Lahdelma, Hokkanen, & Salminen, 1998) SMAA represents a family of MCDA methods for problems where the uncertainty is so significant that it should be considered explicitly.

1.4 Thesis overview

This section provides a chapter-by-chapter overview of the thesis and highlights the contributions by chapter. Figure 2 illustrates the thesis flow.

This chapter (**chapter 1**) introduced the research background, objectives and structure of the thesis. It also briefly discussed the research phases, the work conducted in each phase and how the work evolved through the research lifecycle.

To understand which approaches to evaluating information security value in organisations have been discussed in the literature, we provide an SLR on this topic in **chapter 2.** We search several academic databases for relevant primary studies and extract the key details from the identified studies to answer our research questions.

In **chapter 3**, we investigate what cyber security means based on an exhaustive review of authoritative definitions to highlight the difference to information security. This is an important step, as some practitioners use the term cyber security analogous to information security, whereas others see a distinct difference in what these terms represent. Understanding the differences in scope and context is thus crucial to security value decisions in organisations. It also provides the platform on which to answer our research questions and highlights the most representative definition of cyber security at the time of this research.

Chapter 4 investigates the influence of one or more information security breaches on an organisation's stock market value as a way in which to benchmark the wider economic impact of such events. We use an event study-based approach where a measure of the event's economic impact can be constructed by using the security prices observed over a relatively short period.

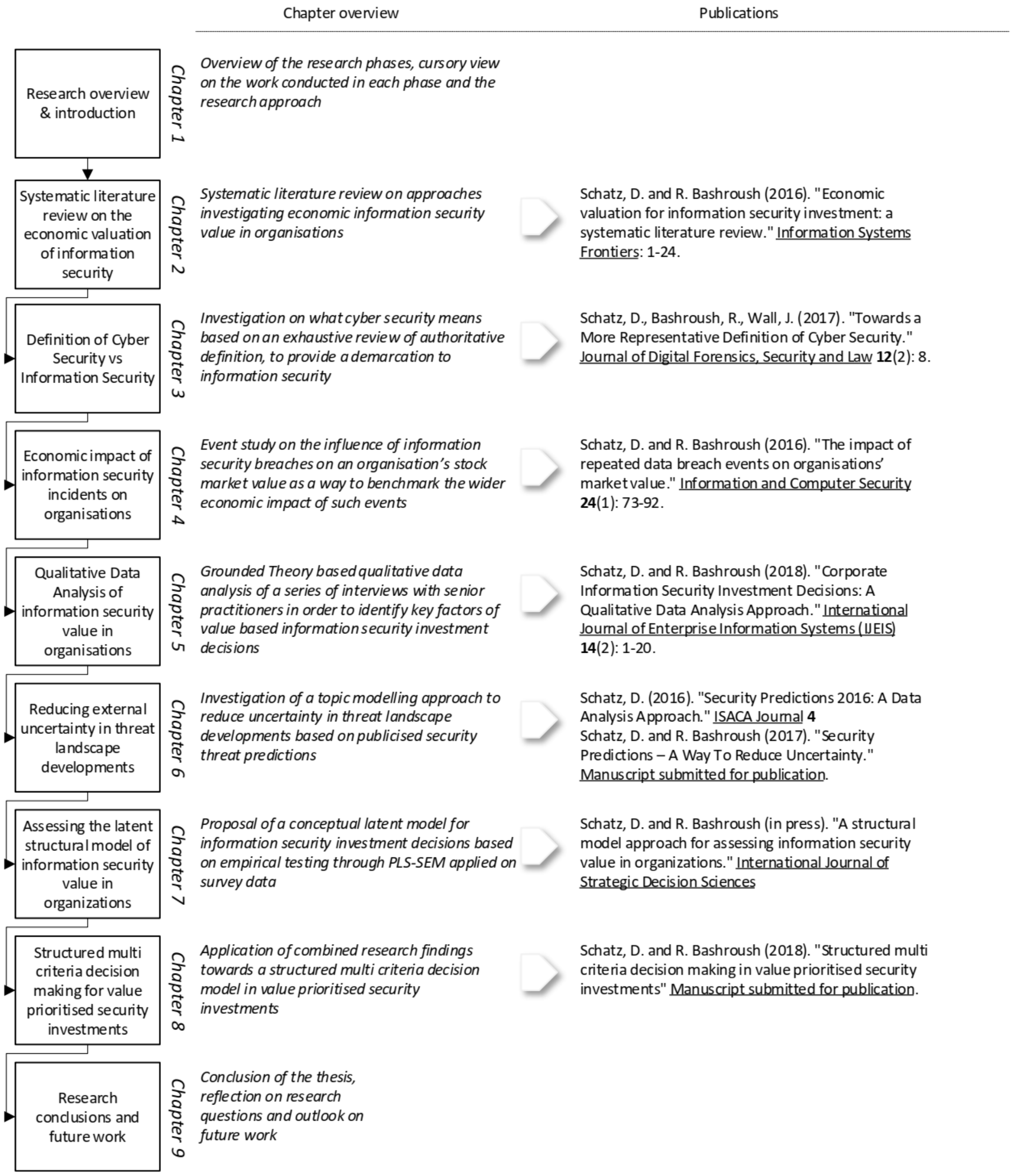
In **chapter 5**, we turn the focus of the research towards real-world experience in the context of information security value. Based on the Grounded Theory approach, we analyse the data gathered in a series of interviews with senior practitioners to identify the key factors behind value-based information security investment decisions. We discuss major drivers, challenges and other key factors and present the findings in a contextualised framework.

As the previous chapters found external uncertainty to be a key challenge to practitioners, **chapter 6** investigates and proposes an approach to reduce such uncertainty in threat landscape developments. Based on a substantial number of published security predictions for a defined time window, we use a topic modelling approach to identify the underlying predicted threat developments. We then verify post hoc to what extent these predicted threat topics have been realised by surveying respondents with varying experience.

Chapter 7 presents a conceptual model of information security investment decisions based on five crucial latent variables (LVs) as well as their measurement variables and significant relationships. It applies the results of our literature review and qualitative interview analysis to a survey with the goal of collecting expert data for analysis by using the PLS-SEM approach.

Chapter 8 examines how the research findings can be combined to enable structured multicriteria decision making in the context of value-prioritised information security investments. It extensively discusses our problem structuring approach as well as the identified measurement criteria and preferences and describes our use of stochastic multicriteria acceptability analysis (SMAA). We provide a discussion and two brief case studies to illustrate the application of the presented model.

Chapter 9 revisits the research questions and provides concluding thoughts on the research presented in this thesis. In addition, future work and forward-looking research opportunities are briefly discussed.



		Chapter overview	Publications
Research overview & introduction	Chapter 1	*Overview of the research phases, cursory view on the work conducted in each phase and the research approach*	
Systematic literature review on the economic valuation of information security	Chapter 2	*Systematic literature review on approaches investigating economic information security value in organisations*	Schatz, D. and R. Bashroush (2016). "Economic valuation for information security investment: a systematic literature review." Information Systems Frontiers: 1-24.
Definition of Cyber Security vs Information Security	Chapter 3	*Investigation on what cyber security means based on an exhaustive review of authoritative definition, to provide a demarcation to information security*	Schatz, D., Bashroush, R., Wall, J. (2017). "Towards a More Representative Definition of Cyber Security." Journal of Digital Forensics, Security and Law **12**(2): 8.
Economic impact of information security incidents on organisations	Chapter 4	*Event study on the influence of information security breaches on an organisation's stock market value as a way to benchmark the wider economic impact of such events*	Schatz, D. and R. Bashroush (2016). "The impact of repeated data breach events on organisations' market value." Information and Computer Security **24**(1): 73-92.
Qualitative Data Analysis of information security value in organisations	Chapter 5	*Grounded Theory based qualitative data analysis of a series of interviews with senior practitioners in order to identify key factors of value based information security investment decisions*	Schatz, D. and R. Bashroush (2018). "Corporate Information Security Investment Decisions: A Qualitative Data Analysis Approach." International Journal of Enterprise Information Systems (IJEIS) **14**(2): 1-20.
Reducing external uncertainty in threat landscape developments	Chapter 6	*Investigation of a topic modelling approach to reduce uncertainty in threat landscape developments based on publicised security threat predictions*	Schatz, D. (2016). "Security Predictions 2016: A Data Analysis Approach." ISACA Journal **4** Schatz, D. and R. Bashroush (2017). "Security Predictions – A Way To Reduce Uncertainty." Manuscript submitted for publication.
Assessing the latent structural model of information security value in organizations	Chapter 7	*Proposal of a conceptual latent model for information security investment decisions based on empirical testing through PLS-SEM applied on survey data*	Schatz, D. and R. Bashroush (in press). "A structural model approach for assessing information security value in organizations." International Journal of Strategic Decision Sciences
Structured multi criteria decision making for value prioritised security investments	Chapter 8	*Application of combined research findings towards a structured multi criteria decision model in value prioritised security investments*	Schatz, D. and R. Bashroush (2018). "Structured multi criteria decision making in value prioritised security investments" Manuscript submitted for publication.
Research conclusions and future work	Chapter 9	*Conclusion of the thesis, reflection on research questions and outlook on future work*	

Figure 2 - Overview and flow of the thesis

2 SYSTEMATIC LITERATURE REVIEW ON THE ECONOMIC VALUATION OF INFORMATION SECURITY

In this chapter, we systematically review the literature on approaches to economic valuation of information security in organisations. Its aims are to guide practitioners looking to understand the current state of research, provide researchers in the field with an overview of the directions previous work has taken and offer newcomers to this area an understanding of the economic assessment of information security investments in organisations. While there is an emerging research base investigating suitable approaches measuring the value of investments in information security, it remains difficult for practitioners to identify key approaches in current research. To address this issue, we conducted a systematic literature review on approaches used to evaluate investments in information security within organisations. Following a defined review protocol, we searched several databases for relevant primary studies and extracted key details from the identified studies to answer our research questions. The contributions of this work include a catalogue of existing approaches and trends that would help researchers and practitioners navigate existing work; categorisation and mapping of approaches according to their key elements and components; and a summary of key challenges and benefits of existing work, which should help focus future research efforts.

As mentioned previously, research on the security of information assets in organisations has largely focused on technology and technological risks. While early research on the economic impact of information security risks was conducted (Ekenberg et al., 1995), academic research was rather limited until the turn of the millennium when the studies by Anderson (2001) and Gordon and Loeb (2002a) raised interest in this topic. This effort is closely aligned with research in the fast-moving area of information security risks in general, which represents a challenging problem in its own right (Hoo, 2000). The present situation shows a dilemma, as understanding the risks involved in an investment is a key requirement to assessing the expected benefits of the investment; as Hertz (1979) states, *“the courage to act* *boldly in the face of apparent uncertainty can be greatly bolstered by the clarity of portrayal of the risks and possible rewards".*

This has led to a situation in which security professionals tasked with the protection of information assets have to justify security investments with little access to widely adopted financial methods given the lack of a tangible return on investment (ROI) since security measures aim to reduce loss as opposed to generate revenue. The result is a battle on various fronts. It involves the challenge of understanding the current and future threats to organisations' information assets, prioritising those with the highest probability to be realised on the highest valued assets and investigating appropriate countermeasures. Not only is this a highly complex undertaking based on estimates and assumptions; it is merely the preamble to a budget approval process. The security professional is faced with the challenge of transforming the identified risks into financial formulas to justify investment in controls by showing value and priority compared with other projects within the organisation competing for the same pot of money.

2.1 Related work

Gordon and Loeb (2006) find limited evidence of the effectiveness of an information security cost/benefit approach in organisations, concluding, *"However, on the open-ended questions, a few respondents noted the budgeted expenditure level on information security for their firms is largely driven by such items as the past year's budget, best practices in the industry, or a mustdo approach".* Along similar lines, Hoo (2000) argues that decisions favour security only when the security advocate (i.e. the security practitioner) commands significant respect from senior management. Likewise, Moore, Dynes, and Chang (2015) find that while calculating ROI is feasible, even helpful, in certain situations, it is unsuitable in many cases. Wood and Parker (2004) go a step further by advising against using traditional financial analysis at all, arguing that it is difficult and counterproductive to try to apply these tools in the context of information security. On the contrary, investment decisions in security based on anecdotal evidence tend to backfire, as security measures tend to look like redundant outlay regardless of whether they work (the lack of loss events impacts the value perception of the protective measure) or not (loss occurs despite the investment). This is clearly not an ideal situation for a maturing information security profession. It may even raise questions about the ability of the Chief Information

Security Officer to do his/her job properly or, in the worst case, calls for an audit to verify whether security budgets may have been misappropriated (Gordon, Loeb, Sohail, Tseng, & Zhou, 2008). Even in the absence of malice or incompetence, budget allocation is a cause of tension. Srinidhi, Yan, and Tayi (2015) find that managers overinvest in specific security-enhancing assets to reduce security breaches during their tenure as this is in their best interest. H. S. B. Herath and Herath (2014) discuss this classical agency issue in more detail and provide guidance allowing firms to decide whether conducting an IT security audit is worthwhile.

An ever-increasing amount of research activity in the information security field at large makes it difficult to identify relevant research addressing the value challenge. Although various works have provided preliminary views of the topic (Eisenga, Jones, & Rodriguez, 2012; European Network and Information Security Agency, 2012; Kesswani & Kumar, 2015; Neubauer & Hartl, 2009), with some detailed analysis (Demetz & Bachlechner, 2013; Huang & Behara, 2013), they tend to fall short of offering a comprehensive view of the literature.

The rest of the chapter is structured as follows. In section 2.2, the research methodology is discussed. This includes the study's research questions, search protocol and inclusion and exclusion criteria. Section 2.3 provides the data extraction and synthesis process of the primary studies identifying trends and developments in the field. Based on the data collected, the research questions are then addressed in detail in the remainder of section 2.3. Section 2.4 examines work in related areas and we discuss possible study limitations and threats to validity in section 2.5. In the last section, we round off the chapter with a summary and conclusions.

2.2 SLR research method

SLRs provide a structured method for critically examining, interpreting and evaluating the entirety of current research evidence in a certain field or area, leveraging a strict framework and predefined questions. As described by Cook, Mulrow, and Haynes (1997) a systematic literature review involves the application of scientific strategies, in ways that limit bias, to the assembly, critical appraisal, and synthesis of all relevant studies that address a specific question. Due to its defined protocol and structured approach this type of review is well suited for the task and has several benefits over other types of literature reviews as described in (Budgen & Brereton, 2006). For this thesis, we followed the guidance provided by Kitchenham and Charters (2007), Brereton, Kitchenham, Budgen, Turner, and Khalil (2007), Biolchini, Mian, Ana, and Travassos (2005) as well as Cronin, Ryan, and Coughlan (2008) and note its challenges and limitations. A multiple step approach that resembles the phases described by Kitchenham and Charters (2007) was then followed to conduct the SLR.

To aid the process, a high-level flowchart was created during the protocol definition phase (Figure 3).

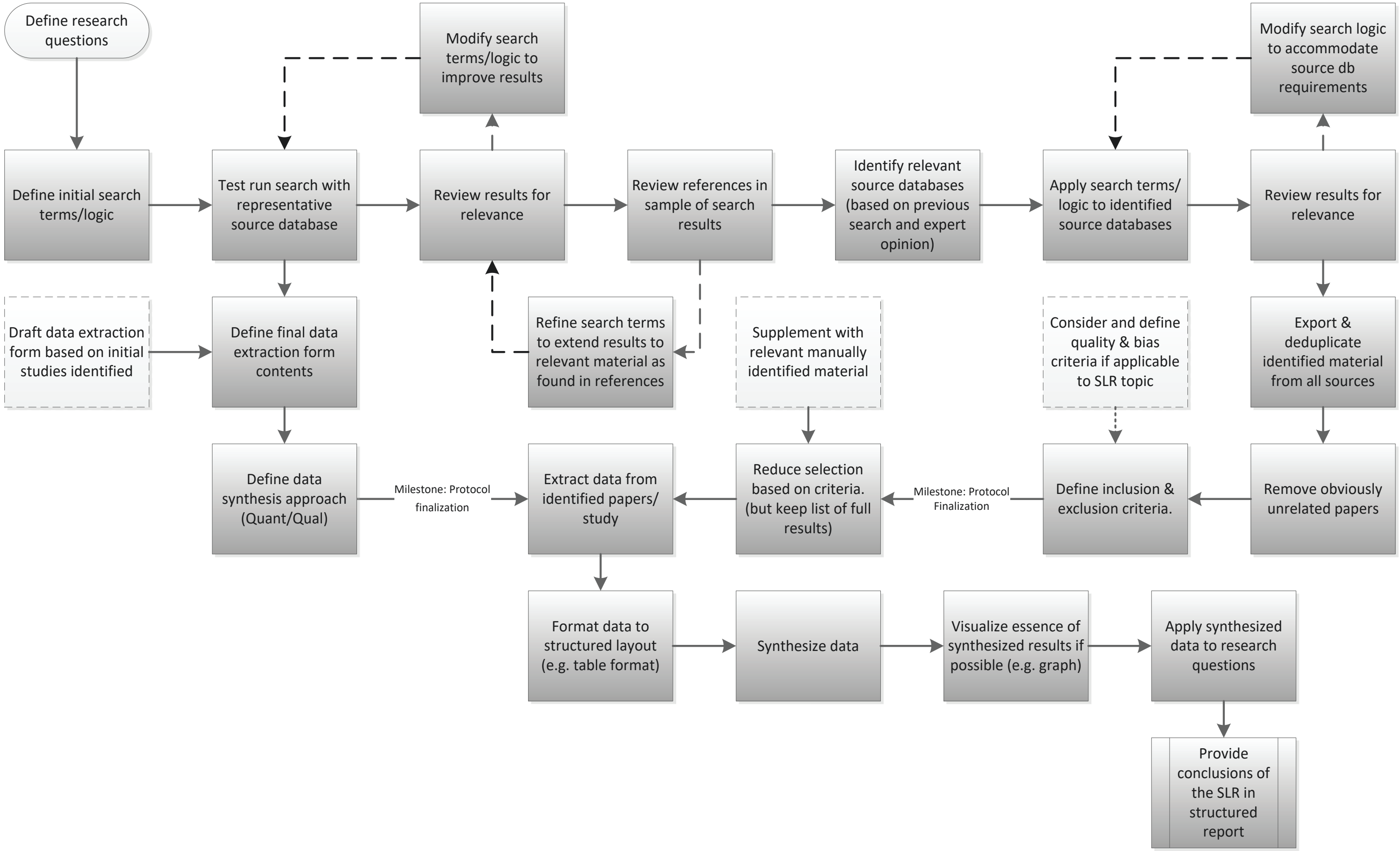

Define research questions
Define initial search terms/logic
Test run search with representative source database
Modify search terms/logic to improve results
Review results for relevance
Review references in sample of search results
Identify relevant source databases (based on previous search and expert opinion)
Apply search terms/ logic to identified source databases
Modify search logic to accommodate source db requirements
Review results for relevance
Draft data extraction form based on initial studies identified
Define final data extraction form contents
Refine search terms to extend results to relevant material as found in references
Supplement with relevant manually identified material
Consider and define quality & bias criteria if applicable to SLR topic
Export & deduplicate identified material from all sources
Define data synthesis approach (Quant/Qual)
Milestone: Protocol finalization
Extract data from identified papers/ study
Reduce selection based on criteria. (but keep list of full results)
Milestone: Protocol Finalization
Define inclusion & exclusion criteria.
Remove obviously unrelated papers
Format data to structured layout (e.g. table format)
Synthesize data
Visualize essence of synthesized results if possible (e.g. graph)
Apply synthesized data to research questions
Provide conclusions of the SLR in structured report

Figure 3 - SLR workflow

2.2.1 Chapter Research questions

As shown in Figure 3, the SLR process starts with the definition of the research questions the study is aiming to answer. For this study, five research questions were identified, as shown in Table 1.

RQ1	What approaches are described in the literature to support decision processes for information security investments (in organisations) taking economic factors into consideration?
	The intention is to understand which approaches are proposed to value information security investments inside organisations.
RQ2	Are there any common key elements across the identified approaches?
	The intention is to understand whether any common elements or factors are covered by the identified approaches.
RQ3	What are the main issues faced by these approaches as reported in the literature?
	The assumption is that no approach is perfect; hence, under this question, we try to capture the issues and limitations reported by authors.
RQ4	Who is publishing on this topic?
	The intention is to understand the size and distribution of the research community.
RQ5	Is there any tendency towards the use of a specific approach?
	The aim is to find out whether there are any favoured approaches when it comes to economically valuing information security investments in organisations.

Table 1 - Research questions

2.2.2 Search construction

To capture relevant material, the search was inspired by the work of Beecham, Baddoo, Hall, Robinson, and Sharp (2006), albeit modified to accommodate the requirements of this particular SLR. The selection of keywords was based on a review of relevant studies in the field and the authors' experience. During the protocol development phase, these keywords were refined based on the preliminary search results. Test searches conducted led to the identification of more potential keywords such as ROI and net present value (NPV). However, these were not used to avoid potential bias based on too narrow search terms in an already sparsely researched field. Additionally, the preliminary search results with these keywords did not noticeably improve or return further relevant material. The search was thus constructed based on the keywords in Table 2.

Keyword list
Information Security, IT Security, InfoSec, investment, investing, economy, cost, benefit, finance, spending, analysis, analyse, analyze, framework, model, decision, justification

Table 2 - Keyword list

These keywords were relationally grouped and each group linked by using Boolean logic. Terms were clustered into groups to reduce search strings, as groups form relevant compound nouns (e.g. InfoSec investment framework). Search terms were shortened by using wildcards (asterisks) where possible and sensible. For example, the use of an asterisk search with ‘invest*’ did not just return ‘investment’ and ‘investing’ but also ‘investigation’ and ‘investigating’, which are commonly used in relation to computer science but less useful in this context (Table 3).

Group 1	“Information Security” OR “IT Security” OR InfoSec
Group 2	Investment OR investing OR econom* OR (cost AND benefit) OR finance* OR spend*
Group 3	Analy* OR framework OR model OR decision OR justification

Table 3 - Search groups

The search construct was then tailored to suit each of the source databases following the specific search requirements/syntax of the database provider.

2.2.3 Search scope

The search mainly utilised electronic databases to identify the relevant literature. Source databases were considered based on their relevance to the field of computer science and information security. To return results from the databases in Table 4, the search function provided by each website was used.

Source	**Description**
EBSCOhost	http://www.ebscohost.com
Web of Knowledge	http://apps.webofknowledge.com/
ScienceDirect	http://www.sciencedirect.com
IEEE_Xplore	http://ieeexplore.ieee.org/Xplore/

Table 4 - Source databases

2.2.4 Inclusion and exclusion criteria

The initial results obtained through the search process were further filtered based on the inclusion and exclusion criteria below.

Inclusion criteria:

- **IC1**: Papers and studies investigating approaches and metrics supporting economic decision processes pertaining to information security investments in organisations
- **IC2**: Papers and studies available in English or German

Exclusion criteria:

- **EC1**: Papers and studies investigating largely or exclusively non-economic approaches of information security (e.g. purely risk- or technology-based)
- **EC2**: Short papers, articles or studies that do not provide sufficient new insights or ideas
- **EC3**: Papers, articles or studies that are not peer-reviewed (e.g. white papers)

Where multiple papers were identified by utilising the same or a similar approach, the most representative paper (favouring more detailed and more recent publications) was selected unless other major contributions reported in other papers warranted inclusion (e.g. additional arguments supporting an approach). All search terms were designed to capture papers and studies published in English; however, publications in German were considered and included if returned as a search result or found to be a relevant reference in a paper. The selection process entailed applying the inclusion and exclusion criteria to the title and abstract of the paper. When this proved inconclusive, the paper was retrieved in full and reviewed.

2.2.5 Search process implementation

Following the SLR framework in Figure 3, the search and extraction process was conducted as below:

- Define the search terms and logic appropriate for the individual databases
- Review the raw results and reduce by removing obviously unrelated material
- Export the search results to a management solution (Thomson Reuters Endnote)
- Create subfolders for each database searched and move imported references accordingly
- Remove duplicate papers based on author(s), year, title and reference type ignoring spacing and punctuation (Endnote functionality)
- Apply selection criteria and move selected papers into a new subfolder
- Retrieve full paper for data extraction
- Review the references in the selected studies for further relevant material

2.2.6 Search results

The search for papers was conducted in 2014 following the protocol defined earlier. Owing to the differences between databases, some modifications to the search string were necessary to optimise the search results. Table 5 shows the search construct unique to each database. Some databases provided additional refinement options that were leveraged as described in the comments section.

Source	**Search details**	**Comments**	**#**
EBSCOhost	("information security" OR "IT Security" OR InfoSec) N90 (investment OR investing OR econom* OR cost OR benefit OR spend*) AND (analysis OR analyse OR analyze OR model OR framework OR decision OR justification)	(Business Source Complete, Communication & Mass Media Complete, Library, Information Science & Technology Abstracts with limiters applied - Scholarly (Peer Reviewed) Journals)	143
Web of Knowledge	(("information security" OR "IT Security" OR InfoSec) NEAR ((investment OR investing OR econom* OR (cost NEAR benefit) OR spend*) NEAR (analysis OR analyse OR analyze OR model OR framework OR decision OR justification)))	Refined by: Research Areas=(COMPUTER SCIENCE OR BUSINESS ECONOMICS OR INFORMATION SCIENCE LIBRARY SCIENCE OR OPERATIONS RESEARCH MANAGEMENT SCIENCE) Timespan=All Years. Search language=English, German Search scope was set to ‘Topic’ which includes Title, Abstract, Author Keywords and Keywords Plus®	263

ScienceDirect	("information security" OR "IT Security" OR InfoSec) W/10((investment OR investing OR econom* OR cost OR benefit OR spend*) W/10(analysis OR analyse OR analyze OR model OR framework OR decision OR justification))	[Journals(Business, Management and Accounting, Computer Science, Economics, Econometrics and Finance)]	281
IEEE_Xplore	("Abstract":(Security OR InfoSec) NEAR (investment OR economic OR cost OR benefit OR spend) AND (analysis OR analyse OR analyze OR model OR framework OR decision OR justification))	Metadata	92

Table 5 - Search constructs and results

After removing obviously unrelated papers by conducting a one-pass review of the raw search results as seen in Table 5, the count of papers reduced from 779 results to 270 papers of potential relevance. These were distributed across the databases (Table 6).

Source	**Initial paper selection**
EBSCOhost	105
Web of Knowledge	139
ScienceDirect	25
IEEE_Xplore	1

Table 6 - Overview of the initial paper selection

Having only one paper attributed to the IEEE_Xplore database does not necessarily mean that no other IEEE published papers on the topic existed; it only indicates that only one study was not returned by the other sources. In the next step, the results across all four databases were further consolidated and duplicate references manually checked and removed, which reduced the reference count to 261.

The selection process of the papers to be considered for data extraction included a manual step exporting the initial selection to Microsoft Excel for easier handling. Each paper was listed with a unique ID and its reference information exported from EndNote. According to the defined inclusion criteria in section 3.4, a ‘single reviewer/two-pass’ review was conducted to decide whether to include a paper in the review (Yes), exclude it (No) or review it in more detail (additional research required [ARR]) before making the decision. Further information was added to the ‘Duplicate’ (if the paper is a duplicate that was not identified as such by EndNote) and ‘Comment’ fields where required. The ‘Included’ field is defined as Boolean and identifies the paper as either included (Y) or not included (N) in the data extraction phase. After the completion of this process, 22 papers were selected for data extraction. The examination of the references listed in the selected papers resulted in an additional five papers identified to be relevant. Three of these were selected for data extraction, bringing the total number of primary studies to 25.

2.3 Data extraction and synthesis

The data extraction process was conducted on 25 papers as described. This section lists all the extracted details under various headings, as follows:

- ‘ID’ represents the unique numeric identifier assigned to each primary study
- ‘Reference’ provides the citation of the paper
- ‘Publication outlet’ provides information on the publication outlet in which the primary study was published
- ‘Approach’ provides a short description of the area of research as reported in the primary study
- ‘Approach details’ provide a short description of the approach itself, as highlighted in the primary study
- ‘Key elements’ list the key elements of the approach as reported in the primary study
- ‘Reported benefits’ list the advantages of the approach as reported in the primary study
- ‘Reported challenges’ list the challenges of the approach as reported in the primary study

ID	Reference	Publication outlet	Approach	Approach details	Key elements	Reported benefits	Reported challenges
13	Arora, Hall, Piato, Ramsey, and Telang (2004)	IT Professional	Risk-based return on investment	RROI measures how effectively resources are used to avoid or reduce risk	Net bypass rate for all security solutions Incident risk, residual risk and baseline scenario	Easier to use than Net Present Value (NPV) Appropriate for identifying the amount of investment	Not appropriate for comparing the value of alternative solutions Obtaining true cost (observed damage) Estimating bypass rates Interaction impact between deployed solutions Representing catastrophic losses

ID	Reference	Publication outlet	Approach	Approach details	Key elements	Reported benefits	Reported challenges
23	Bistarelli, Dall'Aglio, and Peretti (2007)	Formal Aspects in Security and Trust	Strategic games on defence trees	Game theory strategies based on defence trees enriched with economic indexes as payoffs (utility)	Return on security investment (ROSI) Return on attack (ROA) Defence trees	Identification of security countermeasure investment level up to marginal returns boundary	Lack of reliable statistical data to use in a quantitative analysis Ambiguity around the calculation of the risk-mitigated attribute
28	Bodin, Gordon, and Loeb (2005)	Communications of the ACM	Analytic Hierarchy Process (AHP)	Using the ratings method variant of the AHP to determine the optimal budget allocation for	AHP criteria tree Fixed budget	Supports multicriteria decision problems involving both quantitative and qualitative criteria	Does not consider quantitative concerns Strong dependency on proper criteria definition and

ID	Reference	Publication outlet	Approach	Approach details	Key elements	Reported benefits	Reported challenges
				maintaining and enhancing security		Valuable tool for decision making and option ranking	weighting
31	Bojanc and Jerman-Blažič (2008)	International Journal of Information Management	Combined use of multiple indexes	Calculating multiple indexes for each investment option and consolidating the results for decision support	Risk metrics ROI/ROSI NPV Internal rate of return (IRR)	IRR is particularly useful for multi-year investments NPV describes the cash value of expected returns	Each index used individually does not present an appropriate solution ROI and IRR are not project magnitude indicators ROI does not consider the time value of money

ID	Reference	Publication outlet	Approach	Approach details	Key elements	Reported benefits	Reported challenges
41	Huseyin Cavusoglu, Birendra Mishra, and Srinivasan Raghunathan (2004).	Communications of the ACM	Game tree based on solution quality parameters	Game theory strategies based on security solution quality parameters in terms of risk mitigation	Damage cost estimate Mitigation quality parameters Threat parameter estimates	Understand how the parameters affect the optimal investment/cost Assess the marginal effect of a decrease or increase in one parameter on total cost	Uncertainty about the parameter estimates used for the model

ID	Reference	Publication outlet	Approach	Approach details	Key elements	Reported benefits	Reported challenges
43	Cavusoglu, Raghunathan, and Yue (2008)	Journal of Management Information Systems	Decision-theoretic and game-theoretic	Comparing the results of sequential and simultaneous game-theoretic and decision-theoretic approaches	Threat parameter estimates Vulnerability parameter estimates Sequential games Simultaneous games Strategy decisions	Game-theoretic approach achieves a superior result over decision theory in most cases	Uncertainty about the parameter estimates used for the model, particularly for the game-theoretic approach The game-theoretic approach is assumed to be more complex High levels of uncertainty reduce the payoffs under the

ID	Reference	Publication outlet	Approach	Approach details	Key elements	Reported benefits	Reported challenges
							game-theoretic approach Only relevant for targeted attack scenarios
54	A. Davis (2005)	Network Security	Practical Return on Security Investment	Set a policy defining the use of ROSI and adopt a consistent approach to calculating it	Cost of controls Cost of incidents Financial benefits Definition/policy when to use ROSI	Clear view of the value and benefits of security initiatives Making information security more accountable and transparent	Quality of the data estimates used for the model Calculations can be too complex ROSI is not well understood in businesses

ID	Reference	Publication outlet	Approach	Approach details	Key elements	Reported benefits	Reported challenges
80	Gordon and Loeb (2002a)	ACM Transactions on Information and Systems Security	Optimal investment amount to protect a given set of information	Leveraging information sets with security breach probability functions to calculate the optimal investments in information security	Breach loss Threat probability Vulnerability probability Cost of control	Considers how vulnerability and loss affect optimal security investment Supports the decision on what vulnerability level to focus investments Provides an upper limit for the optimal investment	Not intended to cover catastrophic events/loss Uncertainty about the threat, vulnerability and loss estimates Agency cost not considered

ID	Reference	Publication outlet	Approach	Approach details	Key elements	Reported benefits	Reported challenges
95	Hausken (2006a)	Journal of Accounting and Public Policy	Income, interdependence and substitution effects affecting incentives for security investment	Optimal strategies regarding security investment, taking account of the income effect, interdependence and substitution between attacker and defender as well as among defenders	Asset value Inefficiency factor Attackers' resources Average levels of attack Multistage games	Rate of return from security investment (marginal rate of substitution) Appropriate investment based on the identified attacker Appropriate investment based on the substitution and interdependence effects among firms	Time factors not considered Assumptions made on key parameters

ID	Reference	Publication outlet	Approach	Approach details	Key elements	Reported benefits	Reported challenges
99	H. S. B. Herath and Herath (2008)	Journal of Management Information Systems.	Real Options Analysis with Bayesian post-audit	Real options model for information security investments, using Bayesian inferences for valuation and post-auditing	Total cost Expected benefits Volatility parameters	(Bayesian) Revised parameter estimates lead to a reduction in upward bias and the incorporation of up-to-date information Reduces the possibility of a biased forecast Shows how to integrate security-specific features	Focused decision-theoretic approaches/situations Focuses on technical dependence, not market dependence Difficult to obtain prior estimates of the mean and standard deviation from the sample data

ID	Reference	Publication outlet	Approach	Approach details	Key elements	Reported benefits	Reported challenges
						properly in the valuation Incorporates available information into the decision making process in a systematic manner	
107	Iheagwara, Blyth, Kevin, and Kinn (2004)	Information and Software Technology	Cascading Threat Multiplier tied into ROSI	Use a standard risk analysis framework and extend it by introducing the cascading threat multiplier to	Asset value Exposure factor Rate of occurrence Underlying exposed assets	Assists in formulating the analytical framework for asset valuation and risk calculation A more	Cascading threat multiplier is somewhat subjective

ID	Reference	Publication outlet	Approach	Approach details	Key elements	Reported benefits	Reported challenges
				arrive at accurate ROI calculations	Secondary exposure factor	comprehensive valuation methodology that includes intangible factors into the asset valuation variable calculation	
114	Jingyue and Xiaomeng (2007)	2007 International Conference on Software Engineering Advances	Real options theory (ROT)	Apply ROT to make the right security investment decisions	Binomial options pricing model Underlying volatility	Comprehends uncertainty and responds to the dynamics of business needs When and how to implement to maximise the likelihood	Assumes profit-maximising decisions Key parameters need to be estimated or simulated based on historical data

ID	Reference	Publication outlet	Approach	Approach details	Key elements	Reported benefits	Reported challenges
						of desirable outcomes Determines the most value-adding strategy	
123	Khansa and Liginlal (2009)	European Journal of Operational Research	Security process innovation incorporating ROT	Model of invest-to-learn and switching options generated upon early investment in flexible security process innovation	Volatility estimate Intensity of malicious attacks Switching cost Binomial lattice	Value definition of switching solutions decision Invest-to-learn option	Considers switching between only two solutions Competitor impact not included in the model

ID	Reference	Publication outlet	Approach	Approach details	Key elements	Reported benefits	Reported challenges
165	Purser (2004)	Computers & Security	Total ROI	Risk mitigation is included as a factor in the ROI calculation	Revenue Cost saving Value of change in risk	Includes the financial impact of the change in risk	Requires a strategic approach and careful planning Must be business-driven
186	Sheen (2010)	Proceedings of the 9th WSEAS International Conference on Instrumentation Measurement Circuits and Systems (IMCAS 2010). Instrumentatio	Fuzzy economic decision models	NPV and discounted ROI models leveraging fuzzy values for cost/benefit analysis	Triangular fuzzy numbers NPV Discounted ROI Interest rate Inflation rate Operating cost/revenue	Considers the opportunity cost of capital Eliminates the need for complicated sensitivity analysis studies associated with input parameter variations	None reported

ID	Reference	Publication outlet	Approach	Approach details	Key elements	Reported benefits	Reported challenges
		n, Measurement, Circuits and Systems				Takes the degree of confidence of decision makers' opinions into consideration	
191	Shirtz and Elovici (2011)	Information Management & Computer Security	Decision support methodology for allocating information security remedies based on the end-effect perspective	Calculate the optimal subset of remedies for a given budget and the most cost-effective subset of remedies that comply with the	List of end-effects Potential damage Protection level for each end-effect Cost and performance of remedies	Does not use probabilities of undesired information security events Complies with the set budget constraints and desired security level for each end-	Only mutually exclusive end-effects considered

ID	Reference	Publication outlet	Approach	Approach details	Key elements	Reported benefits	Reported challenges
				organisation's policy		effect	
213	Tatsumi and Goto (2010)	Economics of Information Security and Privacy	ROT	Analytically modelling continuous real options applied to information security	Volatility estimate Drift factor Total expected benefits Intensity threat	Guidance on investment timing	Difficulties predicting threat timing/occurrence Difficult to formulate an attacker's objective function
237	Willemson (2010)	Proceedings of the Fifth International Conference on Availability, Reliability, and	Extending Gordon and Loeb	Restricting the class of possible remaining vulnerability functions and	Gordon and Loeb model	New family of remaining vulnerability functions satisfying all conditions	None reported

ID	Reference	Publication outlet	Approach	Approach details	Key elements	Reported benefits	Reported challenges
		Security (ARES 2010)		generalising by stating simple functional constraints		Generalising all the currently known example function families	
244	Yong Jick, Kauffman, and Sougstad (2011)	Decision Support Systems	Financial economics-based value-at-risk methods and operational risk modelling	Profit optimisation model for customer information security investments based on value-at-risk methods and	Value at risk Profit at risk Revenue Total costs Loss estimates	Decision making process using operational risk management and value-at-risk methods in financial economics Risk/return trade-offs for	Classes of risks that cannot be estimated (Black Swan) Considers only quantity of added services, not cost Uncertainty about the estimates of the frequency and

ID	Reference	Publication outlet	Approach	Approach details	Key elements	Reported benefits	Reported challenges
				operational risk modelling from financial economics		information security enhancement investments	magnitude of future losses
252	Zikai and Haitao (2008)	2008 IEEE International Conference on Networking, Sensing and Control (ICNSC '08)	Flexible optimal information security investment strategy	Information security risks are transformed into an opportunity cost and then a multi-object optimisation model is built based on the opportunity cost and direct information	Opportunity cost loss of CIA Direct cost Impact factor	Helps make more confident justifications for security spend	Data loss is hard to estimate by using equations How to combine uncertainty in this model

ID	Reference	Publication outlet	Approach	Approach details	Key elements	Reported benefits	Reported challenges
				security investment			
254	Huang and Behara (2013)	International Journal of Production Economics	Information security fixed budget investment allocation	Investment model defending against concurrent heterogeneous attacks taking budget constraints into consideration	Breach probability based on the scale-free networks concept Potential loss of class Cross-over coefficient	Considers budget constraints Incorporates concurrent attacks Adopts the concept of scale-free networks Considers the cross-over effects of investments	Uncertainty about the assumptions for variables and functions Attack category classification can be imperfect Total budget consumption

ID	Reference	Publication outlet	Approach	Approach details	Key elements	Reported benefits	Reported challenges
257	Capko, Aksentijevic, and Tijan (2014)	2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)	Cash flow analysis and IRR	Practical application of cash flow analysis for information security solutions	Initial investment Opportunity cost of capital end-of-life value and depreciation method Tax considerations Working capital considerations	Cash flow analysis model used to calculate NPV, IRR and RoC	Determining the input parameters, especially avoided cost/damage Cannot be used to analyse investment in multiple solutions
M1	Cremonini (2005).	n/a	Return-On-Attack (ROA)	Improve ROI-based evaluations by	Attackers' gain Attackers'	Identify the solution that mostly	None reported

ID	Reference	Publication outlet	Approach	Approach details	Key elements	Reported benefits	Reported challenges
				integrating them with an ROA index to measure the convenience of attacks	efficiency (or EFF) Cost of attack	discourages attackers in their intrusion attempts Able to consider the time factor	
M2	Faisst, Prokein, and Wegmann (2007)	Zeitschrift für Betriebswirtschaft	Dynamic security investment calculation	Model offering decision support for dynamic security investment calculations based on NPV considerations	Reduction in expected damage Reduction in opportunity cost Operating cost Interest rates	Despite the uncertainty of key factors, a statement on investment benefits can be arrived at Optimal time of investment Takes budget and equity	Interdependency between security controls and assets not considered Difficult to estimate the frequency and scale of malicious events Operational

ID	**Reference**	**Publication outlet**	**Approach**	**Approach details**	**Key elements**	**Reported benefits**	**Reported challenges**
						capital constraints into consideration	budget/cost not sufficiently considered
M4	Matsuura (2009)	Managing Information Risk and the Economics of Security	Extending Gordon and Loeb by productivity spaces	Optimal security investment considering Gordon and Loeb and productivity spaces (vulnerability and threat reduction)	Gordon and Loeb model components Security threat probability function	Identify security investment based on the value of productivities	Failure to assess the threat productivity can lead to the wrong choice Uncertainty about the estimates of the key variables

Table 7 - Extracted data of the selected papers

2.3.1 Results for RQ1

In the items listed under ‘Key elements’ in Table 7 are those considered to be the important elements the primary study is highlighting, relying on or proposing as novel, crucial or providing key contributions to the respective approach. Likewise, the items listed under ‘Reported Benefits’ are those that the primary study is listing as the particular benefits of the proposed approach. Following the data extraction process, we aligned each approach described in the primary study with nine high-level approach categories. We summarised both elements and benefits into a wider elements category and repeated the same with the reported challenges. The categories were then used as the basis to answer the research questions in Table 1. Figure 4 shows the simple relationships.

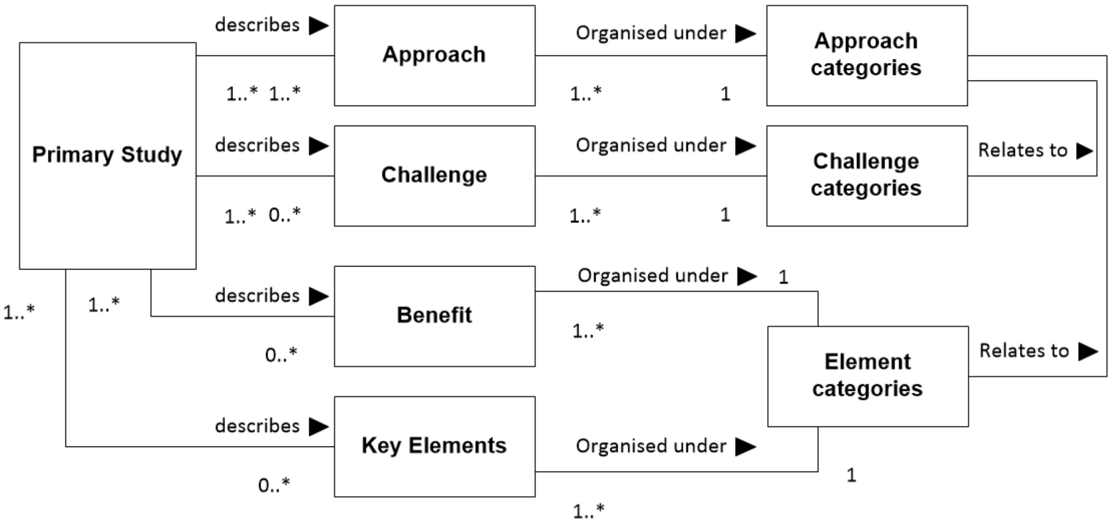


Figure 4 - Overview of the extracted data and relations

The extracted data showed that a number of approaches were discussed in the research. Although fewer primary studies were identified than initially expected, the breadth of approaches covered was noteworthy. An attempt was made to categorise each paper according to its approach to construct a simplified overview. After careful consideration, as noted earlier, nine high-level approach categories were identified that accommodate the individual approaches described in the primary studies. These categories were assumed to strike a balance between being too constraining on the variety of approaches described in the primary studies and avoiding too many approach categories that would hinder a meaningful summarisation. Table 8 describes the nine approach categories.

Approach category	**Description with reference**
AHP	The Analytic Hierarchy Process is a structured method of breaking down complex problems to aggregate sub-problem solutions into a conclusion (Saaty, 1994)
DSS	Decision support systems (DSSs) present a structured method to understand and improve decision processes and support the decision maker to make decisions more effectively (Alavi & Henderson, 1981; Keen, 1980)
Game Theory	Game theory describes the study of strategic decision making in situations of competition or conflict, leveraging mathematical models (Neumann & Morgenstern, 1964)
NPV	Net Present Value is a valuation formula that calculates the present value of the future cash flows of an investment (Ross, 1995)
ROA	Return On Attack is an extension of ROI where an attacker's gain as well its cost (losses) are considered in the model (Cremonini, 2005)
ROI	Return On Investment is a valuation formula that evaluates the efficiency of an investment based on cost and expected benefit (Phillips & Phillips, 2010)
ROI, NPV	Papers that utilise a balanced mix of ROI and NPV to provide guidance on economic information security decisions
ROT	Real Options Theory describes a quantitative means to evaluate the flexibility inherent in the decision making process (L. T. Miller & Park, 2002)
UM	Utility maximization describes a concept in which a subject attempts to derive the greatest possible value from an investment (Strotz, 1955)

Table 8 - Explanation of the categories

Table 9 provides an overview of the categorisation of each primary study.

ID	**Author(s)**	**Year**	**Approach category**
13	Arora, A., Hall, D., Piato, C. A., Ramsey, D., Telang, R.	2004	ROI
23	Bistarelli, S., Dall'Aglio, M., Peretti, P.	2007	Game Theory
28	Bodin, L. D., Gordon, L. A., Loeb, M. P.	2005	AHP
31	Bojanc, R., Jerman-Blažič, B.	2008	ROI, NPV
41	Cavusoglu, H., Mishra, B., Raghunathan, S.	2004	Game Theory
43	Cavusoglu, H., Raghunathan, S., Yue, W. T.	2008	Game Theory
54	Davis, A.	2005	ROI
80	Gordon, L. A., Loeb, M. P.	2002	UM
95	Hausken, K.	2006	UM
99	Herath, H. S. B., Herath, T. C.	2008	ROT
107	Iheagwara, C., Blyth, A., Kevin, T., Kinn, D.	2004	ROI
114	Jingyue, L., Xiaomeng, S.	2007	ROT
123	Khansa, L., Liginlal, D.	2009	ROT
165	Purser, S.A.	2004	ROI
186	Sheen, J.N.	2010	ROI, NPV
191	Shirtz, D., Elovici, Y.	2011	DSS
213	Tatsumi, K.-i., Goto, M.	2010	ROT
237	Willemson, J.	2010	UM
244	Yong Jick, L., Kauffman, R. J., Sougstad, R.	2011	DSS
252	Zikai, W., Haitao, S.	2008	DSS
254	Huang, C. Derrick, Behara, Ravi S	2013	UM
257	Capko, Z., Aksentijevic, S., Tijan, E.	2014	NPV
M1	Cremonini, M.	2005	ROA
M2	Faisst, U., Prokein, O., Wegmann, N.	2007	NPV
M4	Matsuura, K.	2009	UM

Table 9 - Category mapping by paper

Figure 5 shows how the approaches discussed in the 25 primary studies were mapped to the nine approach categories.

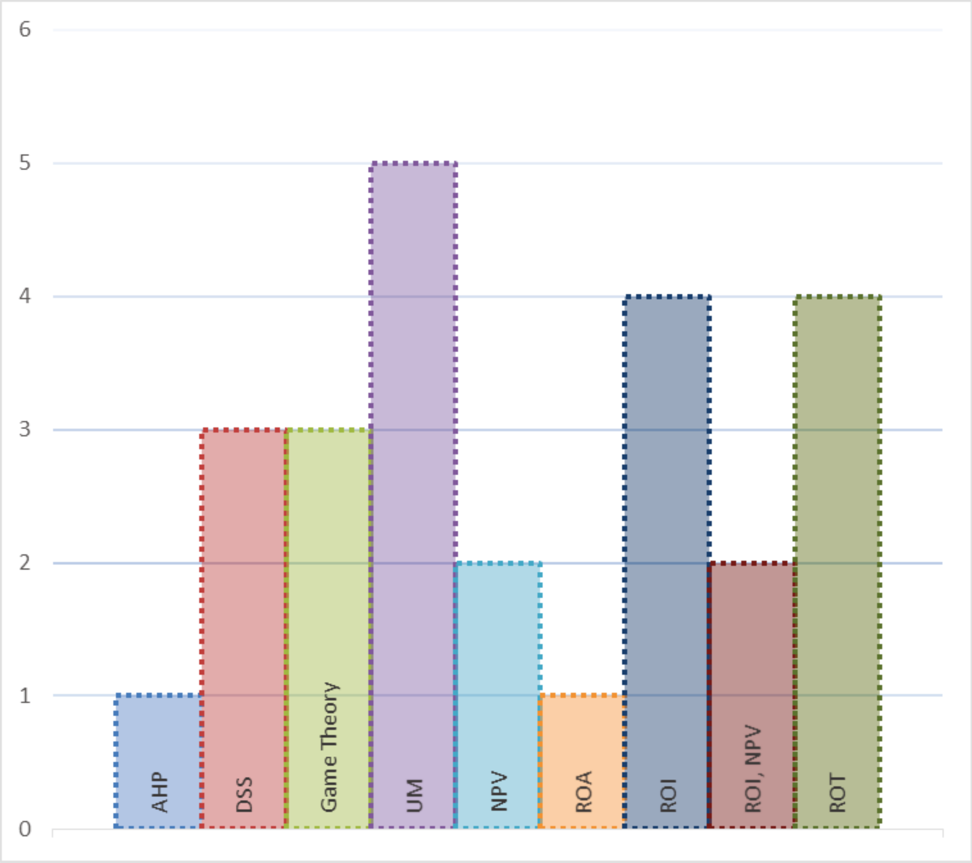


Figure 5 - Primary studies by category

These results allow us to conclude that the sampled approaches focus on three main categories, namely ROI, ROT and UM. While the solid representation of ROI and UM was no surprise, the strong presence of ROT research was unexpected, as we had considered this approach to be rather niche and more focused on financial market valuation rather than corporate investment decisions. Further, the majority of primary studies have approached the problem from an academic perspective with a focus on fundamental theories such as UM, game theory and ROT, perhaps because of the selection criteria of SLRs, which tend to exclude grey or non-refereed literature (e.g. white papers). Yet, several studies discuss the practical implementation and extensions of the primary approaches. For example, Hausken (2006b) analyses different classes of information security breach functions to examine the robustness of the Gordon–Loeb model, which is recognised in this paper as a type of UM approach. Gordon, Loeb, Lucyshyn, and Zhou (2015) extend the ROT approach by assessing the impact of information sharing when a firm is deciding on its security investment timing. The authors find that sharing reduces a firm's uncertainty about cyber security investment and decreases the value of the deferment option associated with such investment.

2.3.2 Results for RQ2

Overall, 90 key elements were extracted from the primary studies with several elements mentioned across multiple works. To better understand which elements are considered to be crucial to this research topic, we attempted to collate the individual elements into topical element categories. Table 10 describes the element alignment in each category.

Element category	**Description**
Benefit	Elements that have direct beneficial attributes such as cost reduction/revenue or are explicitly described as benefits in the primary study
Cost	Elements that are a direct or indirect cost such as operating cost, opportunity cost and switching cost
Function	Elements that are constructs such as decision trees, mitigation quality parameters and fuzzy numbers
Impact	Elements that describe impact in the context of the approach, such as potential damage and the list of end-effects
Resource	Elements considered to be resources such as fixed budgets, asset values and attackers' resources
Threat	Elements that describe or measure threats in the context of the approach, such as threat probability, attackers' efficiency and the rate of occurrence
Volatility	Elements that are specifically described as volatility elements in the primary study
Vulnerability	Elements that describe vulnerability in the context of the approach, such as the exposure factor, vulnerability parameter estimate and bypass rate

Table 10 - Element category details

Table 11 describes more in detail how the extracted elements for all papers aligned with these element categories.

Element category	**Elements**
Benefit	Cost saving (ROI), Expected benefits (ROT), Financial benefits (ROI), Interest rates (NPV, ROI), Reduction in expected damage (NPV), Reduction in opportunity cost (NPV), Revenue (DSS, ROI), Total expected benefits (ROT), Value of change in risk (ROI)
Cost	Cost and performance of remedies (DSS), Cost of attack (ROA), Cost of control (ROI, UM), Cost of incidents (ROI), Damage cost estimate (GT), Direct cost (DSS), Inflation rate (ROI, NPV), Operating cost (NPV), Operating cost/revenue (NPV), Opportunity cost loss of CIA (DSS), Opportunity cost of capital (NPV), Potential loss of class (UM), Residual risk (ROI), Switching cost (ROT), Total cost (DSS, ROT)
Function	AHP criteria tree (AHP), Baseline scenario (ROI), Binomial options pricing model (ROT), Binomial lattice (ROT), Cross-over coefficient (UM), Defence trees (GT), Definition/policy when to use ROSI (ROI), Depreciation method (NPV), Discounted ROI (ROI/NPV), Drift factor (ROT), Inefficiency factor (GT), IRR (ROI/NPV), Mitigation quality parameters (GT), Multistage games (GT), NPV (ROI/NPV), Protection level for each end-effect (DSS), ROI/ROSI (ROI/NPV), ROA (GT), Risk metrics (ROI/NPV), Security threat probability function (UM), Sequential games (GT), Simultaneous games (GT), Strategy decisions (GT), Tax considerations (NPV), Triangular fuzzy numbers (ROI/NPV), Working capital considerations (NPV)
Impact	Attackers' gain (ROA), Breach loss (UM), Impact factor (DSS), List of end-effects (DSS), Loss estimates (DSS), Potential damage (DSS), Profit at risk (DSS), Value at risk (DSS)

Resource	Asset value (GT, ROI), Attackers’ resources (GT), End-of-life value (NPV), Fixed budget (AHP), Initial investment (NPV)
Threat	Attackers’ efficiency (ROA), Average levels of attack (GT), Breach probability based on the scale-free networks concept (UM), Incident risk (ROI), Intensity of malicious attacks (ROT), Intensity threat (ROT), Rate of occurrence (ROI), Threat parameter estimates (GT), Threat probability (UM)
Volatility	Underlying volatility (ROT), Volatility estimate (ROT), Volatility parameter (ROT)
Vulnerability	Exposure factor (ROI), Net bypass rate for all security solutions (ROI), Secondary exposure factor (ROI), Underlying exposed assets (ROI), Vulnerability parameter estimates (GT), Vulnerability probability (UM)

Table 11 - Overview of the elements and their use across approaches

Roughly one-third of the elements are abstract constructs such as decision trees, mitigation quality parameters and fuzzy numbers and these were included in the ‘Function’ element category representing the largest section. Looking at the other categories, cost, benefit and threat are the main contributing factors as per our primary studies. This is not surprising as these are inherently linked to risk and value considerations in information security. Mapping these element categories to the reported approaches reveals an even more interesting picture, as Figure 6 shows.

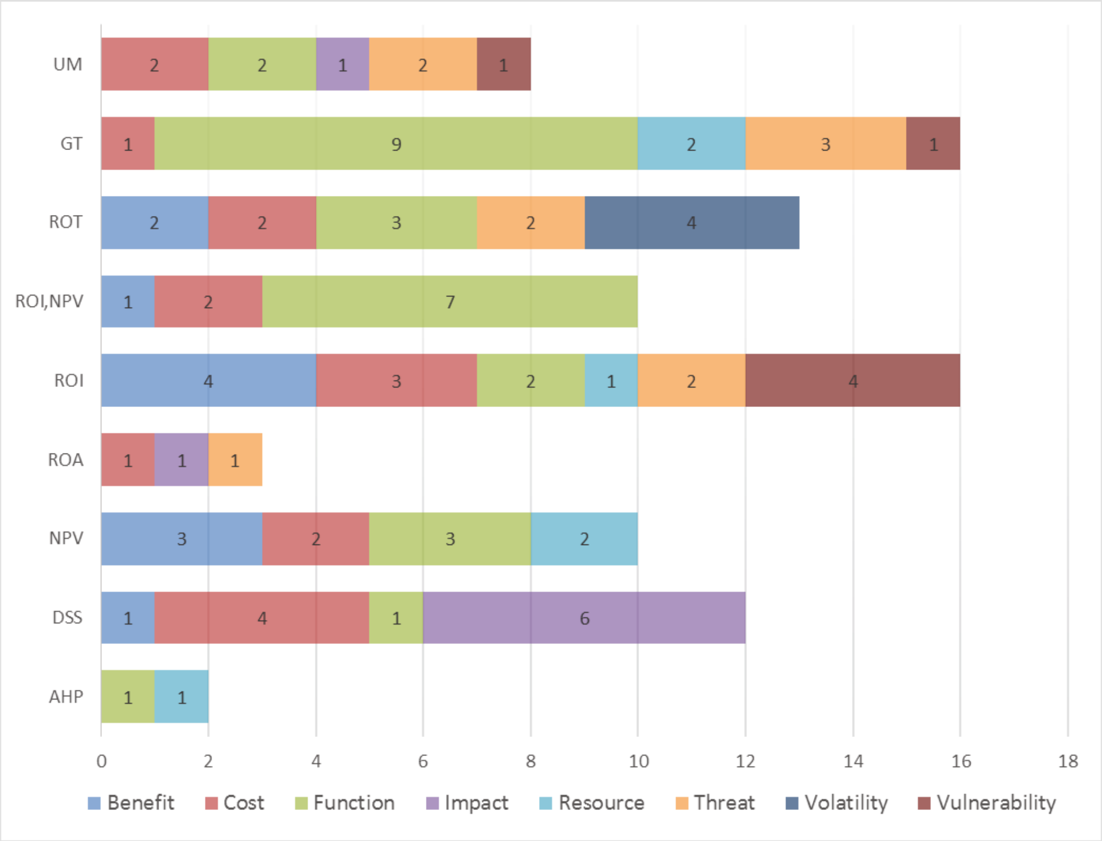


Figure 6 - Elements to approach category mapping

While any conclusion drawn here hinges on the chain of assumptions made until this point (aligning primary studies with approach categories, extracting elements from the papers and aligning elements into element categories), the displayed breakdown intuitively makes sense. Both ROI and NPV show a strong reliance on benefit and cost factors, whereas ROI/NPV and game theory have a high function element as they heavily focus on sub-functions (ROI/NPV) and game strategies. Interestingly, DSS studies are driven by reasonably measurable factors (cost and impact), which would appear to make a good candidate for real-world implementation. We further note that 'Impact' has little mention as a key element in the primary studies other than in DSS- and UM-focused papers. The UM approach stands out because of its balanced distribution of elements, which confirms its usefulness for assessing the true economic value of investments in this context but implicitly also carries all the complexities.

2.3.3 Results for RQ3

We noted 51 challenges reported by the authors in their papers. Similar to the key elements, these challenges were consolidated into five areas. Table 12 describes how the reported challenges were mapped to these challenge categories.

Challenge category	**Description**
Accurate estimates	Challenges related to the estimates of the key parameters or inputs for the described method, such as the frequency of malicious events, loss magnitude and quality of the estimates in general
Complex to apply	Challenges related to the complexity of the method, such as complex calculations, subjectivity and attacker function modelling
Constraint not considered	Challenges related to items specifically mentioned in the primary study as not being considered by the respective approach, such as catastrophic loss and time factors
Limited scenarios	Challenges related to limits in applicability as reported in the primary study, such as limited to targeted attacks and unsuitable for comparing more than two solutions
Real benefit	Challenges related to the identification of the real benefit of the approach

Table 12 - Challenge category details

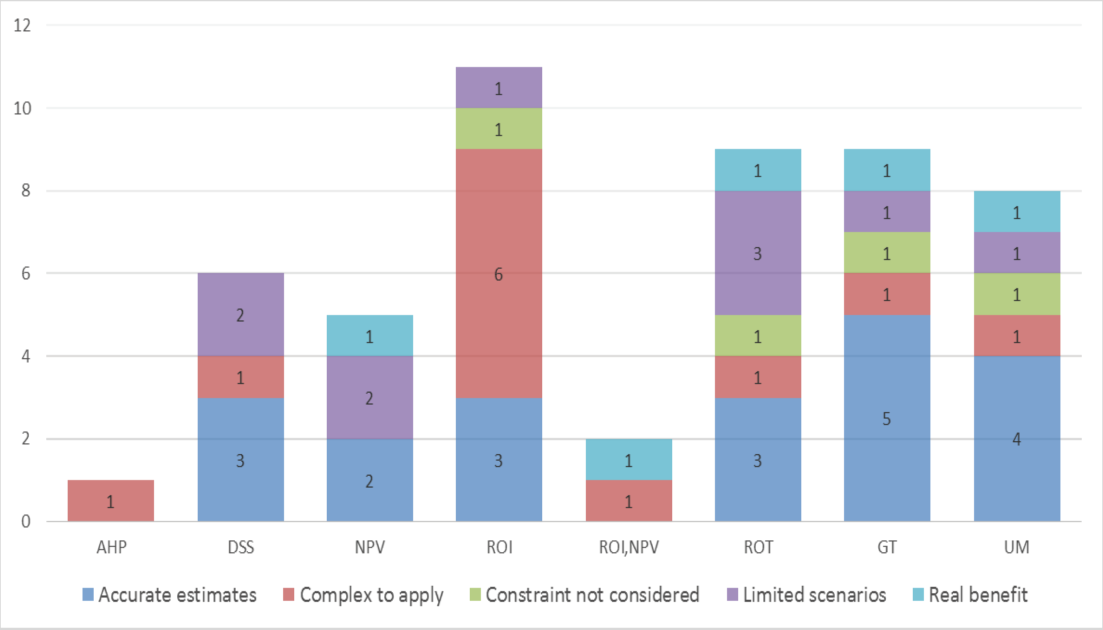


Figure 7 - Challenges to category mapping

Figure 7 illustrates that ‘Accurate estimates’ and ‘Complexity to apply’ are the key challenges across most approaches. When interpreting these data, however, it is important to note that a higher count of primary studies for a given approach is likely to produce an increased count of challenges for that approach. This reason may be why AHP, for example, shows a low amount of challenges compared with GT and ROI. ROI lists complexity as key challenge, which could be interpreted that this approach may not scale well; alternatively, it could be argued that it is one of the most researched approaches and thus better understood in terms of challenges.

2.3.4 Results for RQ4 and RQ5

To understand whether research in this area is progressed by only a particular institution or region, or whether there is a wider research community, we examined the authors of the primary studies (i.e. all authors and co-authors affiliations as well as their geographic locations). As shown in Figure 8, there is a strong research base in the United States (particularly Maryland and Texas) with notable contributions from Croatia, Italy, Norway, Japan, Germany and China. The strong presence of primary studies by US researchers is not a surprise, as according to the inclusion/exclusion criteria for this SLR, our results are biased by language. We cannot comment on whether there is a strong research community covering this topic publishing in languages other than English or German. Further, these data only answer the specific question set for our SLR and only consider primary studies fitting the strict criteria described in section 2.2.4. They do not consider supplemental or tangential papers published on this topic.

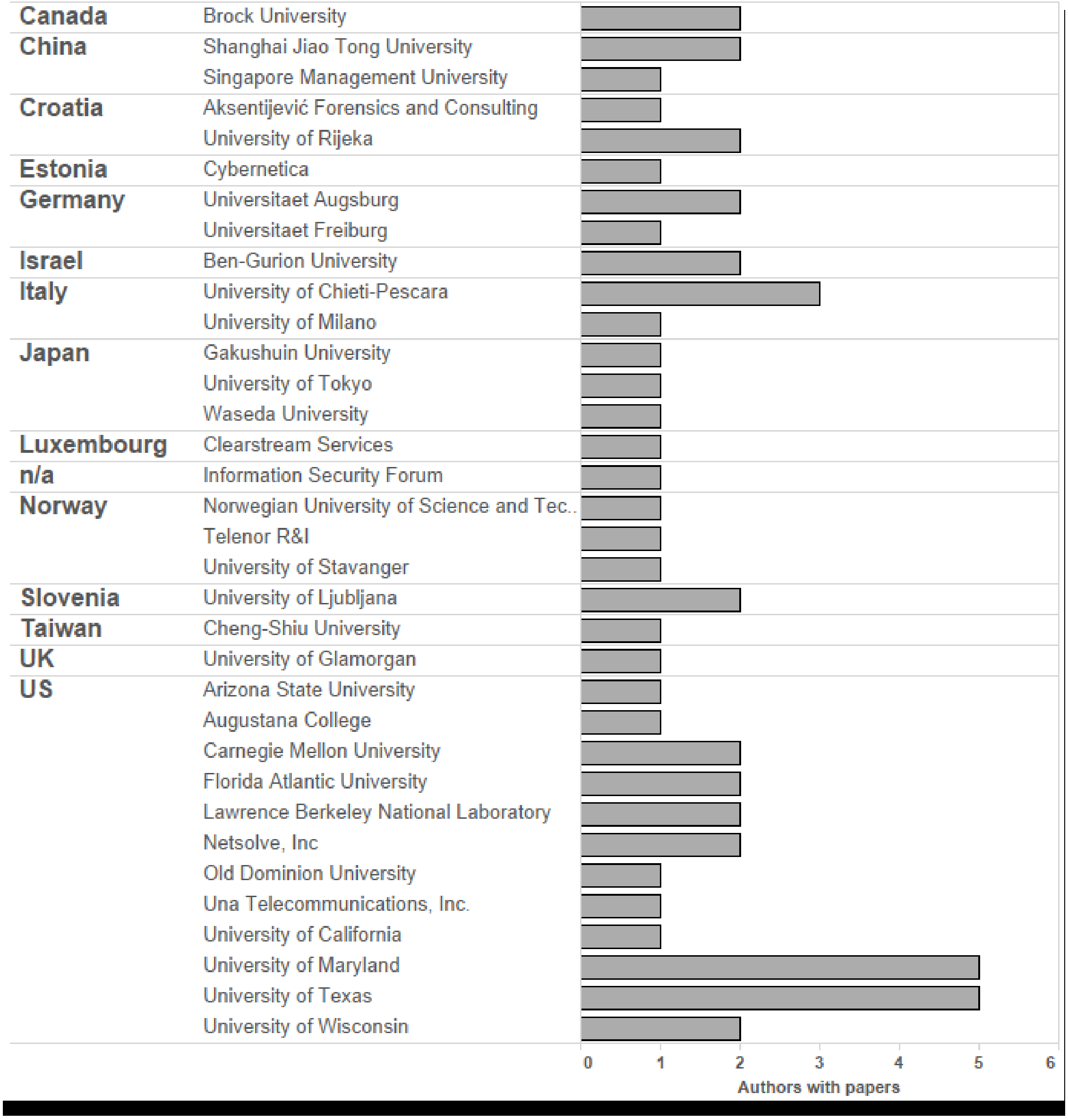


Figure 8 - Geographical distribution of the primary studies

Lastly, to answer RQ5, our assessment of the primary studies did not identify a clear research trend (Figure 9). While UM leads in publications on this topic, it does not dominate the domain. The lack of novel ROI-focused publications after 2005 is something of interest, as this suggests a decline in original contributions to this research approach. Publications on ROT are mainly observed between 2007 and 2010 but we continue to see research activity in this area. Notably, Gordon et al. (2015) extend the ROT approach from the aspect of sharing cyber security-related information among firms, thus addressing some of the reported challenges on this approach (e.g. difficulties predicting threat timing/occurrence and key parameters needing to be estimated or simulated based on historical data).

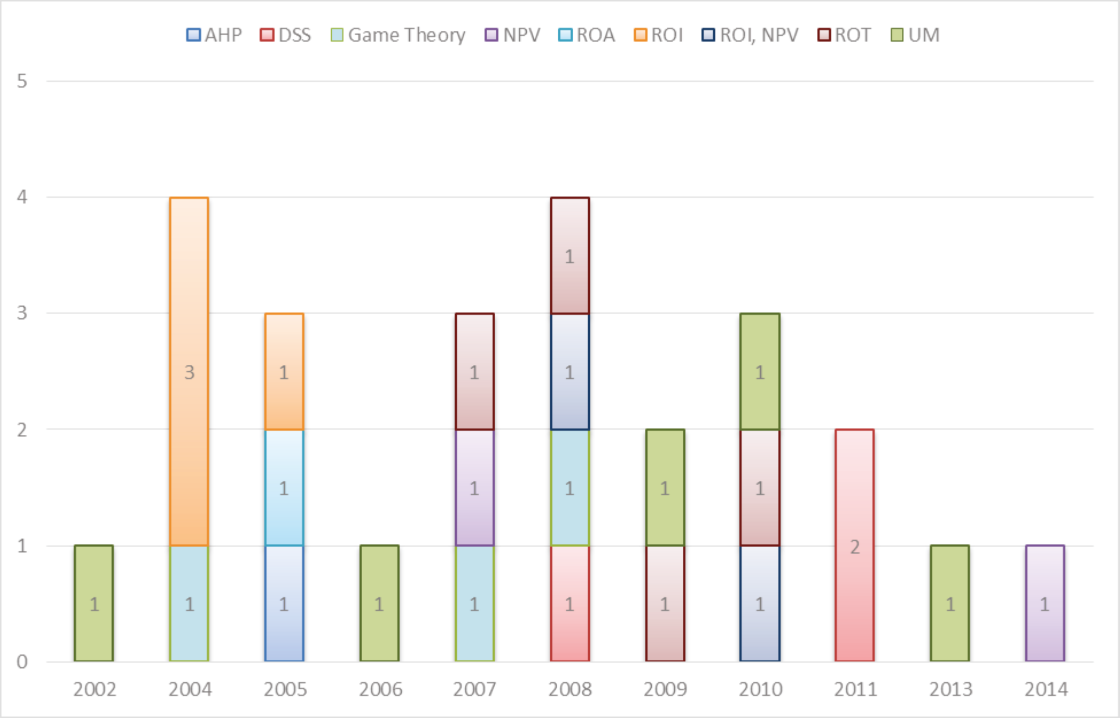


Figure 9 - Primary studies by year of publication

As the simple timeline of primary studies by approach did not provide a satisfactory answer to RQ5, we retrieved additional metadata to better indicate the research trends. The intention was to understand the impact of the primary studies and their approaches on other studies over time. We thus examined the citation count of each primary study based on data provided through Google Scholar because of its comprehensive citation coverage (Meho & Yang, 2006). To support the collection of citation data and calculation of metrics (citations/year), we utilised the ‘Publish or Perish’ tool (Harzing, 2007).

Somewhat as expected, the citation count (absolute and average) is higher for papers published earlier, particularly for the seminal paper by Gordon and Loeb (2002a) [ID 80]. We generally observe that research on game theory and UM provides a constant stream of cited papers over the years with a noticeable spike in 2008. Primary studies of other approaches appear to have a limited reach based on citation count, which may indicate opportunities for further research or simply point to a lack of interest in these areas. Again, no clear trend is observed; however, publication frequency and citation metrics point towards ongoing interest in game-theoretic approaches as well as general UM research.

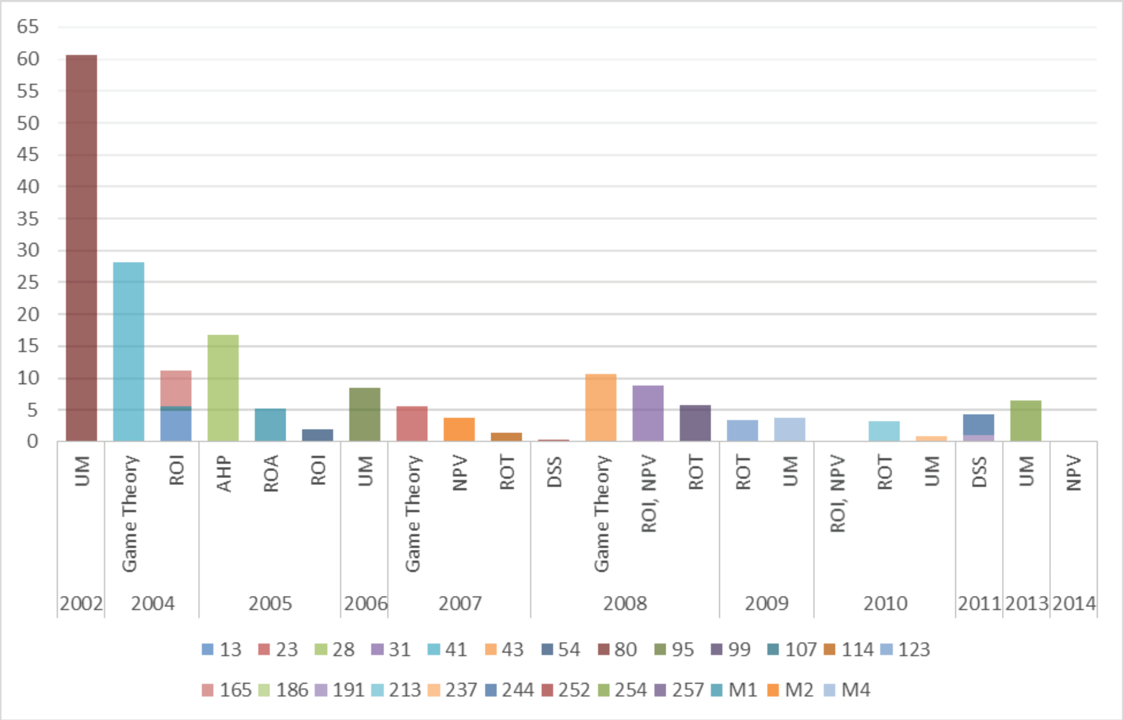


Figure 10 - Primary studies by publication year with average citations per year

2.4 Wider perspective

One of the advantages of the SLR process is that it helps focus the search process and ensures that the relevant literature is captured in an unbiased way and using a repeatable process. However, it also means that some relevant wider literature is missed, as it does not meet the inclusion/exclusion criteria. In this section, we complement the SLR results above by capturing the wider perspective to provide a more comprehensive view of the topic.

Gordon et al. (2015) emphasise the importance of firms understanding the process by which they can derive the most efficient allocation of their cyber security-related resources. This is now a widely accepted challenge and research on options to understand and address this gap is well underway (Dengpan, Yonghua, & Mookerjee, 2011; Lawrence A. Gordon, Martin P. Loeb, & William Lucyshyn, 2003; Hausken, 2007). Recent efforts in knowledge and information sharing, as it pertains to cyber security, try to improve the defender's position by enhancing the collective knowledge on the tools, techniques and procedures (TTP) of threat actors. Despite the collective benefits of moving towards a complete information game from a defender's perspective, however, firms are slow to adopt. Some antitrust concerns aside (Department of Justice, 2014), the main challenge to overcome is that of free-riding, which is akin to the tragedy of the cyber sharing commons. It is in the best interest of firms to consume, but not necessarily share, cyber intelligence to improve their security position. This potentially redirects attackers to other firms and therefore reduces the other firm's contest success (Hausken, 2007). With little market incentive to move away from such practices, governments are starting to encourage organisations to do 'the right thing' by applying a Thaler and Sunstein (2003) libertarian paternalism approach as evidenced in the US Cybersecurity Information Sharing Act of 2015 (The White House, 2015).

The question of the working approaches and strategies for information security investments remains, however. In their empirical study, Rowe and Gallaher (2006) introduce a conceptual approach to consider the trade-offs between various investment and implementation strategies. Their conclusion provides a macroeconomic view stating that policymakers and organisations would benefit from a robust analysis of the differences between the social and private costs of cyber security. Although not an empirical study, the model proposed by Bojanc and Jerman-Blažič (2012) provides an interesting approach for the evaluation of investments in security based on the quantitative analysis of security risks. The authors evaluate the profitability of security measures based on ROI, NPV and IRR and use the output to compare individual measures with each other. Based on an empirical study of S&P 500 firms, Gordon and Loeb (2006) conclude that there seems to be a movement towards using more economic analysis to evaluate information security activities. Although a particular interest in NPV can be seen, they also note that the budgeted expenditure level on information security is largely driven by such items as the past year's budget, best practices in the industry and a must-do approach. Wei, Tanaka, and Matsuura (2007) conduct an empirical analysis of information security investments by surveying the vulnerability of Japanese enterprises to computer viruses. By taking the number of security measures as a proxy variable of security investment, they confirm that the effects of information security investment help reduce vulnerability.

An alternative approach would be to consider risk transfer options, such as those provided by cyber insurance. Miaoui, Boudriga, and Abaoub (2015) propose an approach to distribute investments between controls to protect against security attacks, insurance to transfer the residual risk of loss and forensic readiness to maximise capability to collect digital evidence. The authors consider the interdependence of the investment strategies of their model when computing the optimal total investment. Mukhopadhyay, Chatterjee, Saha, Mahanti, and Sadhukhan (2013) propose a way in which to help firms decide on the utility of cyber insurance products and to what extent they can use them. The authors discuss using copula-based Bayesian belief networks to assess and quantify cyber risk as decision support for using cyber insurance products as a risk management tool. This is related to the previous work by H. S. B. Herath and Herath (2011), who describe a copula-based simulation for determining the annual net premiums of cyber insurance policies by adopting an empirical approach using Archimedean copulas.

2.5 Study limitations and threats to validity

This study suffers from the limitations inherent to SLRs as described by Kitchenham and Charters (2007). This includes limitations on search comprehensiveness and material selection. Owing to the volume of papers returned and analysed, the study might have missed a relevant paper (because of an error or oversight) at any stage of the search process. However, given the way in which the research questions were designed, and as the analysis was based on a set of papers, the impact of any potential omissions on the study’s findings and conclusions should be limited.

While the search terms were carefully crafted, search term definition is a potential limitation as relevant papers might have been missed. This is particularly true for papers not published in English. To mitigate this shortcoming, forward and backward reference checking was conducted on the key publications to identify any potentially missed studies. As is customary with SLRs, for papers to be considered to be primary studies, they have to be published in a peer-reviewed outlet. This placed further restrictions on the selection process, as material published, for example, as white papers (which is common in industry) could not be selected.

2.6 Chapter summary

This SLR aimed to examine economic information security decision making processes. Following standard SLR processes, we identified 25 highly relevant papers describing approaches supporting decision processes for information security investments taking economic factors into consideration. We aligned the reported approaches into nine categories and identified research in UM, game theory and ROT to be areas in which novel ideas are prevalent. We extracted the key elements for each primary study as mentioned by the authors and collated the individual elements into categories. Based on these element categories, we analysed which elements authors consider to be the most relevant for their approaches, finding that both ROI and NPV show strong reliance on 'Benefit' and 'Cost' elements, whereas game theory has high reliance on 'Function' elements because of its focused game strategies. We further noted that DSS studies are driven by measurable elements, namely 'Cost' and 'Impact'. Many of these primary studies discuss the challenges pertaining to their approaches, which we also extracted and summarised; 'Accurate estimates' and 'Complexity to apply' the approach were key challenges across most studies. Looking at the sources of research, a considerable number of our primary studies are accredited to researchers affiliated with US-based institutions. By contrast, representation of the APAC region is limited but this could be due to the language restrictions applied (IC2) for this SLR. Lastly, we analysed the publication timeline for the selected primary studies and found no clear trend towards one particular information security investment valuation approach. We did observe a decline in ROI and ROT publications, whereas UM publications are notably present across the timeline. This finding is supported by our analysis of citation counts: studies of UM and GT are visibly more influential than other approaches.

Taking the findings of this SLR into consideration, a reasonable assumption can be made, namely that challenges originating from uncertainty about the estimates of key variables is a problem that requires a prior solution. The increase in research into impact of information sharing seems to support this. With this in mind, we extended our research into one of the most challenging areas of information security uncertainty, namely developments in the global threat landscape (see chapter 6).

In the next chapter, we assess another area of security that regularly attracts the attention of researchers, practitioners and the media alike: the impact on organisations if a compromise of information processing systems or data occurs. In particular, we analyse the impact of data breach events on stock prices and extend the research into the impact of repeated data breach events.

3 Analysis of Cyber security definitions

Cyber Security has emerged in recent years as a widely used term, with increased adoption by practitioners and politicians alike. However, as with many fashionable jargon, there seems to be very little understanding of what the term really entails. Although this is not an issue when the term is used in an informal context, it can potentially cause serious problems when used as part of a new organizational strategy or business objective. In this chapter, we study the existing literature to identify the main definitions provided for the term cyber security by authoritative sources. We then conduct various lexical and semantic analysis techniques to better understand the scope and context of these definitions, along with their relevance. Based on the analysis conducted, we propose a new improved definition that we prove is most representative of the term. Lastly, we draw comparison to work by von Solms and van Niekerk (2013) who investigated the meaning of information security and highlight key differences between the topical areas.

During our research discussions, we quickly realised the ambiguity of the fundamental term and context when practitioners talk about the value aspects of information security. We found that some practitioners use the term 'cyber security' instead of 'information security', some use the terms in an analogous manner and others see a distinct difference in what these terms represent. Given the considerable overlap, we investigated the definition of cyber security to avoid ambiguity being carried forward into our later work. The terminology used to discuss the security aspects of digital devices and information has changed considerably in recent years. At the beginning of the century, terms such as computer security, IT security and information security were regularly used in this context. While these terms have nuanced differences understood by professionals working in this space, they were tangible enough to be meaningful to the wider populace. General conversations could take place and plans could be made based on a common understanding of what these terms imply. However, towards the end of the first decade, the popularity of the use of the term cyber security gained considerably when U.S. President Barack Obama proclaimed, *"I call upon the people of the United States to recognize the importance of cybersecurity and to observe this month with appropriate activities, events, and trainings to enhance our national security and resilience"* (The White House, 2009). The immediate impact of this press release on the terminology can be illustrated with the help of Google's search trends over time (Choi & Varian, 2012). Figure 11 shows the steady decline in the search terms 'computer security' and 'information security', with variants of 'cyber security' converging and surpassing them, with a notable spike in 2009.

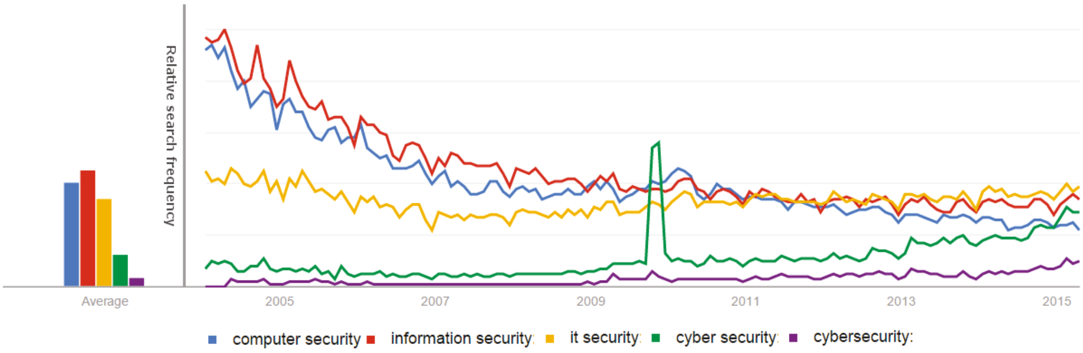


Figure 11 - Google search trends for security, 2004–2015

This development has caused some issues, as the term cyber security lacks the clarity of, for example, computer security, which can lead to confusion and misunderstanding if parties have different assumptions about what the term represents. Quoting Sowell (2014) on the importance of clarity,

> *"What may seem like small steps in logic, after the fact, can be a long, time-consuming process of trial and error groping, while creating and refining concepts and definitions to express ideas in clear and unmistakable terms which allow substantive issues to be debated in terms that opposing parties can agree on, so that they can at least disagree on substance, rather than be frustrated by semantics".*

While it is unlikely to be a problem in private conversations between interested citizens, it becomes, at the very least, a nuisance at the organisational level and is a widely recognised issue among professionals in the field. These problems amplify if such ambiguity infiltrates national cyber security strategies and international treaties. An additional, although less worrisome, issue is the inconsistent use of syntax for cyber security. Across the literature, both versions, namely 'cybersecurity' and 'cyber security', are used. Indeed, Figure 11 shows that both terms are upward trending.

However, the separated version (i.e. ‘cyber security’) shows higher absolute numbers, and this is the spelling used throughout the remainder of the thesis unless referring to primary source material.

Recognising the lack of a consistent meaning of the term cyber security as a considerable issue (Baylon, 2014; Congressional Research Service, 2014; Creasey, 2013; Internet Society, 2012), we first review the professional, academic and governmental literature to identify the most prevalent definitions used, assess the key components of these definitions and review any contentious points that exist between the proposed definitions. In the second and third steps, we identify the best match definition and contribute an improved one.

The remainder of the chapter is structured as follows. In the next section, we examine existing research in this field and discuss the challenges of current definitions. Section 3.2 describes the approach followed for our SLR of the topic. We continue to analyse the definition set from a semantic perspective in sections 3.3 and 3.4 with a proposal for an improved definition in section 3.5. In sections 3.6 and 3.7, we review the limitations of our approach and provide concluding thoughts.

3.1 Related work

The lack of a uniformly accepted definition of cyber security has been recognised across professional (Barzilay, 2013; Stubley, 2013; Walls, Perkins, & Weiss, 2013), governmental (Falessi, Gavrila, Klejnstrup Ritter, & Moulinos, 2012; Government of Montenegro, 2013; Wamala, 2011) and academic (Baylon, 2014; Giles & Hagestad, 2013) work. Walls et al. (2013) approach the topic from the perspective of a professional services provider (Gartner Inc.) and thus focus on providing guidance for strategic decision makers. They highlight the key challenge of the ambiguity introduced by the thoughtless use of the term cyber security where nuanced definitions such as information security and IT security are more appropriate and descriptive. They suggest that the term cyber security only be used in the context of security practices related to the combination of offensive and defensive actions involving or relying upon information technology and/or operational technology environments and systems. The authors state that this marks a superset of security practices such as information security, IT security and other related practices.

Stubley (2013) takes a different view by simplifying cyber security to information security based on a short analysis of the ‘cyber’ component, which he defines as the use of IT and computers. On the contrary, Barzilay (2013) argues that cyber security must be defined through cyber risk, concluding that cyber security is a sub-discipline of information security. In official guidance, ISACA (2014) takes yet another position, stating that cyber security is emerging within the fields of information security and traditional security. Enterprises should thus distinguish between standard (lower-level) information security and cyber security; the difference is in the scope, motive, opportunity and method of the attack.

In their analysis of the national cyber security strategies of European Union (EU) member states, Falessi et al. (2012) explain that there is no universally accepted or straightforward definition of cyber security. They find that some people regard cyber security as overlapping with information security, but no definitive conclusion is provided. This view is shared by Wamala (2011), who claims that cyber security is a branch of information security. This paper highlights the risk of using uncertain terminology and aims to clarify the relative positions of cyber security and information security. It links cyber security with the global characteristic of the Internet, as such distinguishing it from information security that, according to the author, rarely traverses jurisdictions. Wamala goes further in this definition claiming that cyber security focuses more on integrity and availability, whereas information security is mainly concerned with confidentiality. He concludes that cyber security is information security with jurisdictional uncertainty and attribution issues.

The Government of Montenegro (2013) agrees that clear definitions in this area are lacking and dedicates a full section in its cyber security strategy to this topic. While it presents definitions that comply with the basic meanings as understood in EU countries, it unfortunately does not actually provide a conclusion on the term cyber security, but rather cites various definitions from other sources.

Baylon (2014) discusses the topic from a multinational cooperation perspective, highlighting that the lack of consensus on the definition of key terminology in the cyber and space security domains poses a major challenge to international treaties and arms control agreements. In particular, the different interpretations of cyber security between western countries and both Russia and China cause complications in this context. Baylon states that the term cyber security as such does not exist in Russian legislation or official doctrines. Instead, the concept of information security is prevalent. However, in this context, information represents a meaning extending outside the digital space that widens conversations into the information space in general. The author categorises this into the Eastern approach, looking at cyber security emphasising ‘social cohesion’, and the Western approach, perceiving cyber security through a ‘national security prism’. Godwin III, Kulpin, Rauscher, and Yaschenko (2014) concur with this challenge and provide binationally (United States/Russia) agreed terminology for key phrases pertaining to cyber space. Among these, the term cyber security is defined as having a considerably different interpretation to those found in the official cyber security strategies of most western countries. Giles and Hagestad (2013) extend this by contrasting the key terms and principles in this space as understood in the United States, China and Russia. They find a notably different understanding and approach among these countries and conclude that in the absence of a mutually agreed terminology, any potential for finding shared views on the nature and governance of cyber space remains distant.

Academic research has also noted the obvious challenges in this developing problem space. Luiijf, Besseling, and de Graaf (2013) study the cyber security strategies of 19 countries and discuss their differences in terminology in some detail. They find that only eight nations define the term cyber security in their national cyber security strategies, whereas six nations do not provide any such definition. The authors note that of the 10 cyber security strategies that have the term cyber security defined by implication, description or definition, the understanding of what it means varies greatly. This view is shared by Craigen, Diakun-Thibault, and Purse (2014), who find that the term is used broadly and that its definitions are highly variable, context-bound, often subjective and, at times, uninformative. Based on a shortlist of nine definitions and feedback from a multidisciplinary group, the authors work towards a unified definition by identifying the five dominant themes of cyber security.

3.2 Systematic Review Approach

To better understand the variety of relevant definitions of cyber security in use, we followed the semi-SLR approach described below (Mäntylä, Adams, Khomh, Engström, & Petersen, 2014). Following the collection of definitions, we applied text analysis methods on the resulting dataset - focusing on semantic similarity analysis - to identify harmonising definitions. This approach resulted in a ranking of definition similarity across the dataset; in other words, we established which definitions from the whole dataset most accurately represent the definition of cyber security. Based on the further analysis of the highest scoring definitions, we then created a new definition comprising the key terms identified. This new definition was then compared with the original dataset to verify its best match status across the dataset.

3.2.1 Chapter Research question

We started by defining our research questions at a high level.

RQ1	What definitions of cyber security are used by authoritative sources?
	The intention is to understand how cyber security is currently defined by sources of authority (academic, professional, government)
RQ2	Are there differences in the definitions?
	The intention is to understand whether the definitions are similar or considerably different
RQ3	Is there a best match definition of cyber security?
	The assumption is that various definitions have been proposed; hence, we are trying to identify the best match definition across the dataset
RQ4	Are we able to contribute a new best match definition of cyber security?
	This is based on a text analysis approach

Table 13 - Research questions

To answer our research questions, we first needed to identify the relevant definitions. For this, we applied a set of inclusion and exclusion criteria to our literature search as follows.

Inclusion criteria:

- **IC1**: Sources with a clear intention of providing an explicit definition of cyber security
- **IC2**: Sources available in English or with a translation readily available

Exclusion criteria:

- **EC1**: Sources that provide no clear or only implicit definitions of cyber security
- **EC2**: Sources that lack the rigour (peer review) or authority (governmental or professional bodies) to define cyber security

These criteria, particularly EC2, were applied throughout the search process (Cornell University, 2016). In the first instance, Thomson Reuters' Web of Science database was used to identify the relevant academic sources. The search scope covered a timespan of 'All years' with a search construct of TOPIC: (('cyber security' OR Cybersecurity) NEAR definition). This produced merely 13 hits of which only one source met our criteria. Modifying the search query to include variations of the term 'definition' (meaning, interpretation) did not produce any additional relevant results. Our search efforts in other databases such as Science Direct (25 results) were met with similar challenges.

To capture a wider range of sources, we thus extended our search efforts to the general purpose search engine Google.com, limiting the search parameters as follows ([cybersecurity AROUND(3) definition] OR ["cyber security" AROUND(3) definition]). A manual review of the top search results returned by Google was then conducted to capture the most relevant sources. Based on the sources identified, further backward and forward reference crawling was conducted (using Google Scholar) to capture additional material relevant to our research question. In addition, source lists provided by ENISA[1] and NATO[2] were reviewed manually. Our literature review finally identified 28 sources that met our inclusion and exclusion criteria, as shown in Table 14 in no particular order.

#	Source	Title
1	Committee on National Security Systems	National Information Assurance (IA) Glossary
2	National Initiative for Cybersecurity Careers and Studies	Explore Terms: A Glossary of Common Cybersecurity Terminology
3	International Telecommunication	SERIES X: Data networks, open system communications and security

[1] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss.

[2] https://ccdcoe.org/strategies-policies.html.

	Union	
4	Gartner	Definition: Cybersecurity
5	The Institution of Engineering and Technology	Resilience and Cyber Security of Technology in the Built Environment
6	British Standards Institute	Guidelines for cybersecurity
7	Australian Government	Cyber Security Strategy
8	Federal Chancellery of the Republic of Austria	Austrian Cyber Security Strategy
9	Government of Belgium	Cyber Security Strategy
10	Government of Finland	Finland's Cyber Security Strategy
11	French Network and Information Security Agency	Information systems defence and security France's strategy
12	Federal Ministry of the Interior	Cyber Security Strategy for Germany
13	Government of Hungary	National Cyber Security Strategy of Hungary
14	The Netherlands, Ministry of Security and Justice	The National Cyber Security Strategy (NCSS) 2
15	New Zealand Government	New Zealand's Cyber Security Strategy
16	Norwegian Ministries	Cyber Security Strategy for Norway
17	Kingdom of Saudi Arabia	Developing National Information Security Strategy for the Kingdom of Saudi Arabia
18	Republic of South Africa	Cybersecurity Policy of South Africa

19	Republic of Turkey	National Cyber Security Strategy and 2013-2014 Action Plan
20	National Institute of Standards and Technology	Framework for Improving Critical Infrastructure Cybersecurity
21	Spanish Cyber Security Institute	National Cyber Security, a commitment for everybody
22	Republic of Poland	Cyberspace protection policy of the Republic of Poland
23	Government of Jamaica	National Cyber Security Strategy
24	Craigen, Dan Diakun-Thibault, Nadia Purse, Randy	Defining Cybersecurity
25	Merriam-Webster	Definition of Cybersecurity
26	Oxford Dictionary	Definition of Cybersecurity
27	Amoroso, Edward	Cyber Security
28	EastWest Institute	Critical Terminology Foundations 2

Table 14 - Definition of the sources

Of the 28 identified sources, one definition was considered to be from academia, five were contributed by industry and 22 definitions were from governments or government-aligned bodies. As expected, there is considerable overlap in their definitions used, with some including parts of definitions stated by another source (e.g. #3 and #18). The definition text was extracted from the source material in the context in which it was written. Details of the identified definitions are provided in the Appendices.

3.3 Basic definition analysis

To better understand the dataset, an initial exploratory text analysis (Hearst, 1999) was conducted to discover information inherent to the definitions. We started by applying basic information extraction procedures (Weiss, Indurkhya, Zhang, & Damerau, 2004) utilising the text mining framework *tm_map* (Meyer, Hornik, & Feinerer, 2008) in the software environment for statistical computing “R”. Before the definition data were loaded into “R”, minimal manual normalisation was applied to standardise the character encoding and remove unnecessary line breaks. The definition corpus was then prepared with the common preprocessing functions provided by *tm_map* to convert content into lower case, strip whitespaces and remove punctuation and stop words (English). In addition, stemming was applied (Porter, 1997) to reduce the number of distinct word types in the text corpus and increase the frequency of the occurrence of some individual types (Weiss et al., 2004).

With the corpus prepared, we then created a simple document-term matrix (Salton, 1963) that allowed us to gain basic insights into how our sources define cyber security. As illustrated in Figure 12, the root form of security, cyber security, cyber and cyber space is prevalent in the corpus as expected. However, we also gleaned an indication of related words fundamental to the definition pool.

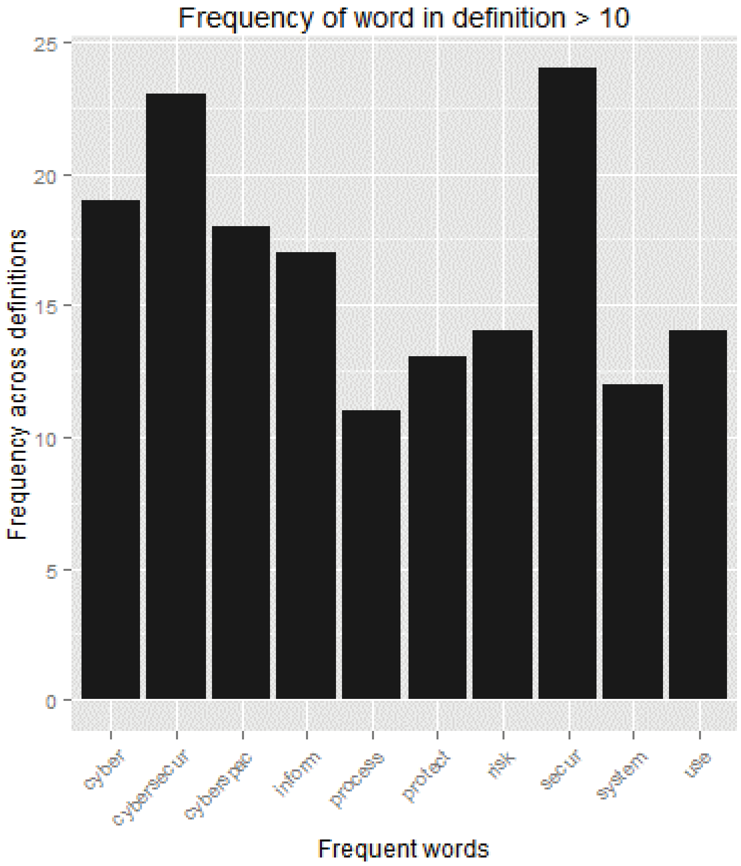
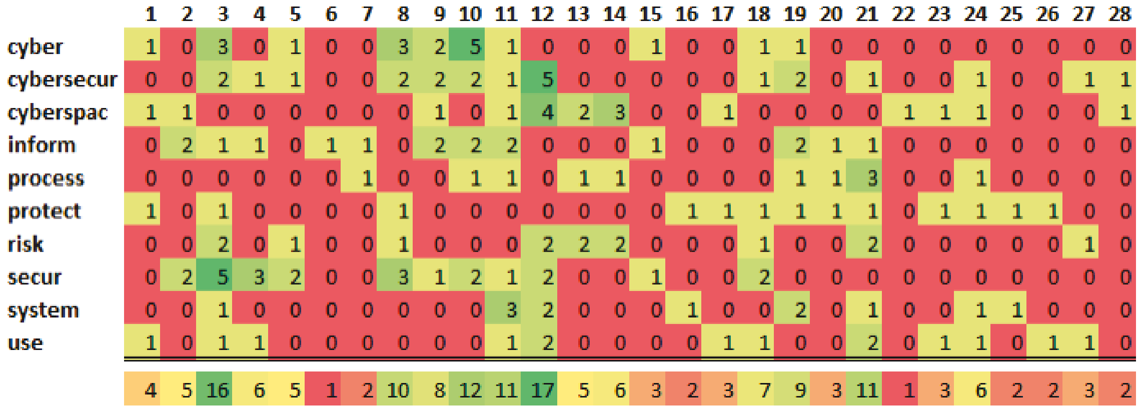


Figure 12 - Word frequency in the definition corpus for the top terms

The basic term frequency analysis provided an indication of the importance (by way of word count) of certain words in the dataset, most notably ‘risk’, ‘protect’, ‘use’, ‘process’ and ‘system’. By using this information, we analysed the definition sets. Lexical overlap analysis, the process of identifying the number of words that texts have in common, is one of the simplest methods of assessing the similarity between texts (Rus, 2014). We used this analysis to conduct a basic lexical token review of our definition set with the most frequent 10 unigrams in their stemmed form, as shown in Figure 13.



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
cyber	1	0	3	0	1	0	0	3	2	5	1	0	0	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0
cybersecur	0	0	2	1	1	0	0	2	2	2	1	5	0	0	0	0	0	1	2	0	1	0	0	1	0	0	1	1
cyberspac	1	1	0	0	0	0	0	0	1	0	1	4	2	3	0	0	1	0	0	0	0	1	1	1	0	0	0	1
inform	0	2	1	1	0	1	1	0	2	2	2	0	0	0	1	0	0	0	2	1	1	0	0	0	0	0	0	0
process	0	0	0	0	0	0	1	0	0	1	1	0	1	1	0	0	0	0	1	1	3	0	0	1	0	0	0	0
protect	1	0	1	0	0	0	0	1	0	0	0	0	0	0	0	1	1	1	1	1	1	0	1	1	1	1	0	0
risk	0	0	2	0	1	0	0	1	0	0	0	2	2	2	0	0	0	1	0	0	2	0	0	0	0	0	1	0
secur	0	2	5	3	2	0	0	3	1	2	1	2	0	0	1	0	0	2	0	0	0	0	0	0	0	0	0	0
system	0	0	1	0	0	0	0	0	0	0	3	2	0	0	0	1	0	0	2	0	1	0	0	1	1	0	0	0
use	1	0	1	1	0	0	0	0	0	0	1	2	0	0	0	0	1	1	0	0	2	0	1	1	0	1	1	0
	4	5	16	6	5	1	2	10	8	12	11	17	5	6	3	2	3	7	9	3	11	1	3	6	2	2	3	2

Figure 13 - Heat map showing the most frequent word stem analysis by definition

This heat map shows the 10 most frequent terms across all 28 definitions in the dataset with an individual and total term count per document. Based on this simple analysis, we gleaned that some definitions incorporate a wider spectrum of key terms than others (e.g. #3 or #11) and may better represent what the entire definition pool defines as cyber security. Such a simple analysis is skewed by term repetition, however; see, for example, definition #12 where 'cybersecur' and 'cyberspac' are used frequently.

Continuing with our basic analysis, we created a correlation matrix for a sparse DTM (sparsity at 0.85) to gain additional information on strongly correlated terms across the definition set. Figure 14 confirms our assumption that frequent terms such as 'cybersecur', 'cyberspac' and 'secur' are not highly correlated with other terms in this context. However, the correlation matrix shows that some correlated terms are worth further exploration.

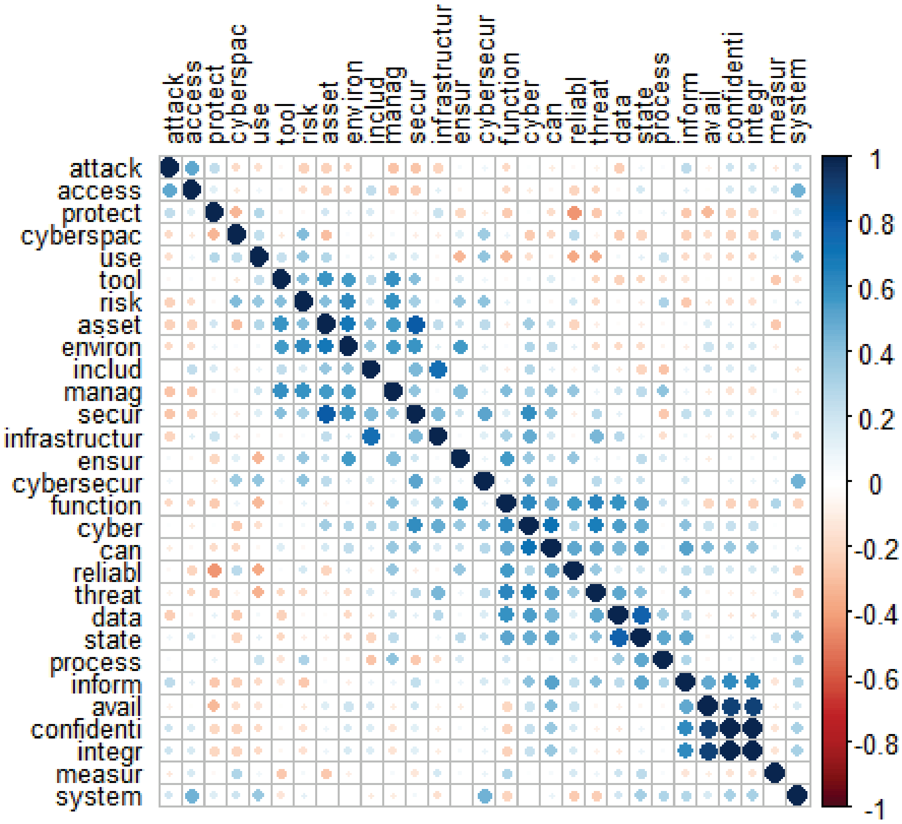


Figure 14 - Sparse DTM correlation matrix

We found a high correlation between the terms of the CIA triad (confidentiality, integrity, availability), which is intuitive as they tend to be used together when writing about topics such as cyber security. We also found a noteworthy correlation of ‘inform’ and ‘integr’ along with the CIA triad, as confirmed in a later section of this thesis. Moreover, the correlations among ‘secur’, ‘asset’ and ‘environ’ point towards a general agreement that those terms standing together are important for a harmonised definition of cyber security. This basic approach shows further interesting positive and negative correlations (e.g. ‘include’ and ‘infrastructur’, ‘realibl’ and ‘protect’) that help better understand the definition space. However, we still lack a way in which to identify the most representative definition of cyber security.

Following the maxim that *"a person without data is just another person with an opinion"*[3], we designed an approach that would allow us to identify the most representative definition within our pool. The assumption is that our dataset includes most of the authoritative definitions of cyber security and as such covers all the relevant aspects of the concept proposed by the sources (Ryan & Bernard, 2003). This means we can identify the definition encompassing the majority of the relevant components through lexical and semantic similarity analysis to ascertain the definition most alike to every other definition in the dataset. We used the range of advanced similarity measures described in the next section to achieve this.

3.4 Definition similarity analysis

Semantic similarity is a well-established area of research with a range of practical applications (Androutsopoulos & Malakasiotis, 2010; Couto, Silva, & Coutinho, 2007; Graesser, Olney, Haynes, & Chipman, 2005; Yuhua, Bandar, & McLean, 2003). For the purpose of this research, we investigated work on short text -and sentence-based similarity measures. We initially planned to use the best method for sentence-based similarity measures, as proposed by subject matter experts on this topic, but found that this is a developing area with various methods proposed. Hence, instead of choosing one method to calculate similarity, we used a variety of methods to balance their advantages and disadvantages. The result is the average similarity score described in this section. We found the SEMILAR toolkit (Rus, Lintean, Banjade, Niraula, & Stefanescu, 2013) to be ideal for this, as it vastly simplified the task of calculating similarity by using multiple algorithms and options. The authors describe the toolkit as *"a one-stop-shop for investigating, annotating, and authoring methods for the semantic similarity of texts of any level of granularity"*. We used the toolkit to conduct both the preprocessing phase and the similarity computing phase for our dataset.

As with our basic analysis, we conducted common preprocessing tasks on our dataset but with some notable differences. The first step was the tokenisation of the text to obtain the ordered set of lexical tokens. Based on our configuration, SEMILAR

[3] Attributed to Edward Deming.

calculated the initial lexical form of the token, lemma form of the word, part of speech, weighted specificity of the word, semantic representation (WordNet (G. A. Miller, 1995) or LSA (Martin & Berry, 2007)) and a list of syntactic dependencies with the other words in the same sentence (Lintean, 2011). To capture as much context as possible, we chose Stanford CoreNLP (De Marneffe et al., 2006) as the configuration option for tokenisation, part-of-speech tagging, lemmatiser and syntactic parsing. Figure 15 illustrates how this task processed one of the definitions in the set. The effect of lemmatisation (compared with stemming) and part-of-speech tagging is apparent. The function identified sentence tokens and categorised them accurately for further processing. In the selected sample, we see that the tagger associated words with their respective part of speech ("The" /Determiner, "ability" /Noun singular, "protect" /verb base, "or" /coordinating conjunction, etc.).

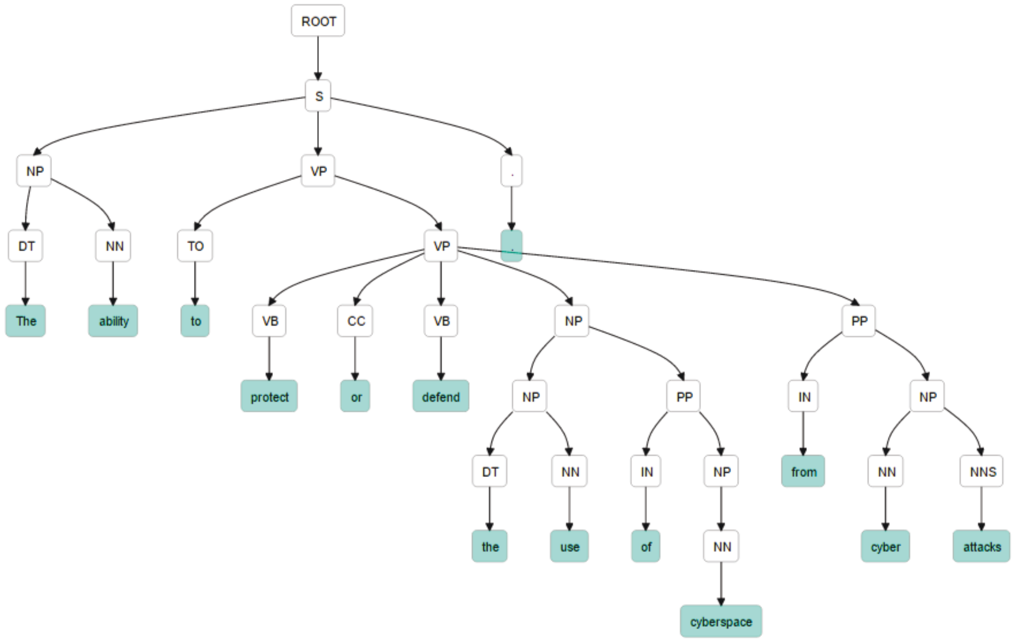
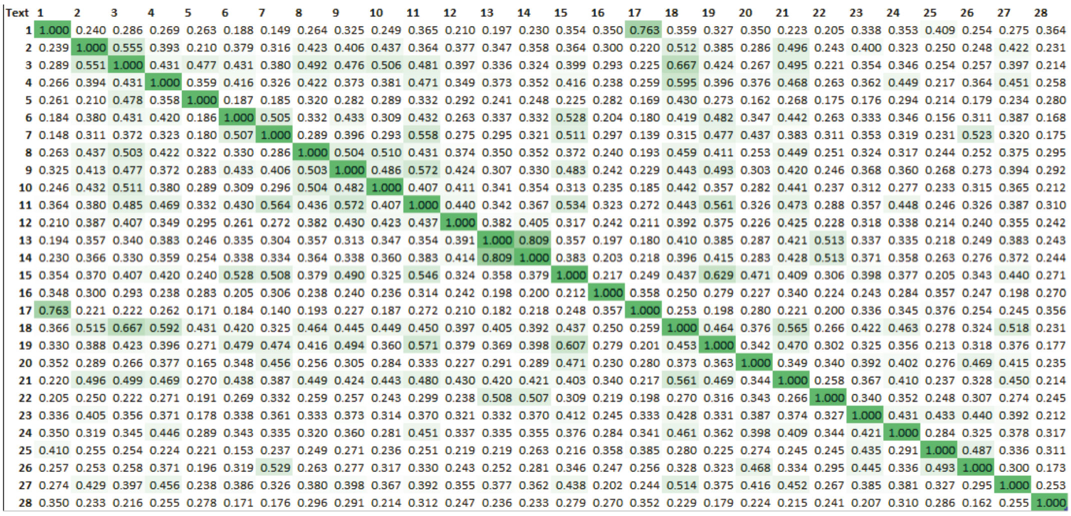


Figure 15 - Sample of preprocessing with StanfordNLP

With the definition set prepared this way, we calculated the similarity between all the definitions using nine methods, resulting in 7056 similarity scores. We selected the nine methods and their configuration options used to calculate the similarity scores based on recommendations and insights from the relevant literature (Corley & Mihalcea, 2005; Gomaa & Fahmy, 2013; M. C. Lee, 2011; Lintean, 2011; Nakov, Popova, & Mateev, 2001; Rus, 2014; Rus & Lintean, 2012; Yuhua, McLean, Bandar, O'Shea, & Crockett, 2006). The methods chosen were categorised and listed within the SEMILAR toolkit as follows: lexical methods (five), Corley–Mihalcea (three) and plain LSA vector similarity (one).

For the lexical similarity methods, we did not remove stop words, non-function words or punctuation following Lintean (2011) and Yuhua et al. (2006), who show the importance of these tokens for similarity calculations because of their structural information value. We did, however, convert all tokens into lower case. For lexical matching, we selected the optimal pairing (Rus et al., 2012) without enforcing part-of-speech matching. Further, the token weights were based on entropy (Martin & Berry, 2007) rather than inverted document frequency (IDF) (Sparck Jones, 1972) following Lintean (2011), who finds that entropy-based weighting leads to better results than inverted document frequency-based weighting.

With this configuration set as the baseline, we selected five token similarity metric methods: LSA, Jiang–Conrath (Jiang & Conrath, 1997), Leacock–Chodorow (Leacock, Miller, & Chodorow, 1998), Lin (Lin, 1998) and Wu–Palmer (Wu & Palmer, 1994). For the similarity calculations based on the 'class of method' proposed by Corley and Mihalcea (2005), we again chose the Jiang–Conrath, Leacock–Chodorow and Lin methods, each with the bidirectional scoring type. Touchstone Applied Science Associates' corpus derived inverted document frequency as the model. Finally, for plain LSA similarity scoring, we selected a frequency-based local weight as well as an entropy-based global weight. Further detail on each of these methods is beyond the scope of this thesis and can be found in the references list. We transformed the scores calculated into a matrix format (Figure 16) to calculate the final averages for each definition.



Text	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
1	1.000	0.240	0.286	0.269	0.263	0.188	0.149	0.264	0.325	0.249	0.365	0.210	0.197	0.230	0.354	0.350	0.763	0.359	0.327	0.350	0.223	0.205	0.338	0.353	0.409	0.254	0.275	0.364
2	0.239	1.000	0.555	0.393	0.210	0.379	0.316	0.423	0.406	0.437	0.364	0.377	0.347	0.358	0.364	0.300	0.220	0.512	0.385	0.286	0.496	0.243	0.400	0.323	0.250	0.248	0.422	0.231
3	0.289	0.551	1.000	0.431	0.477	0.431	0.380	0.492	0.476	0.506	0.481	0.397	0.336	0.324	0.399	0.293	0.225	0.667	0.424	0.267	0.495	0.221	0.354	0.346	0.254	0.257	0.397	0.214
4	0.266	0.394	0.431	1.000	0.359	0.416	0.326	0.422	0.373	0.381	0.471	0.349	0.373	0.352	0.416	0.238	0.259	0.595	0.396	0.376	0.468	0.263	0.362	0.449	0.217	0.364	0.451	0.258
5	0.261	0.210	0.478	0.358	1.000	0.187	0.185	0.320	0.282	0.289	0.332	0.292	0.241	0.248	0.225	0.282	0.169	0.430	0.273	0.162	0.268	0.175	0.176	0.294	0.214	0.179	0.234	0.280
6	0.184	0.380	0.431	0.420	0.186	1.000	0.505	0.332	0.433	0.309	0.432	0.263	0.337	0.332	0.528	0.204	0.180	0.419	0.482	0.347	0.442	0.263	0.333	0.346	0.156	0.311	0.387	0.168
7	0.148	0.311	0.372	0.323	0.180	0.507	1.000	0.289	0.396	0.293	0.558	0.275	0.295	0.321	0.511	0.297	0.139	0.315	0.477	0.437	0.383	0.311	0.353	0.319	0.231	0.523	0.320	0.175
8	0.263	0.437	0.503	0.422	0.322	0.330	0.286	1.000	0.504	0.510	0.431	0.374	0.350	0.352	0.372	0.240	0.193	0.459	0.411	0.253	0.449	0.251	0.324	0.317	0.244	0.252	0.375	0.295
9	0.325	0.413	0.477	0.372	0.283	0.433	0.406	0.503	1.000	0.486	0.572	0.424	0.307	0.330	0.483	0.242	0.229	0.443	0.493	0.303	0.420	0.246	0.368	0.360	0.268	0.273	0.394	0.292
10	0.246	0.432	0.511	0.380	0.289	0.309	0.296	0.504	0.482	1.000	0.407	0.411	0.341	0.354	0.313	0.235	0.185	0.442	0.357	0.282	0.441	0.237	0.312	0.277	0.233	0.315	0.365	0.212
11	0.364	0.380	0.485	0.469	0.332	0.430	0.564	0.436	0.572	0.407	1.000	0.440	0.342	0.367	0.534	0.323	0.272	0.443	0.561	0.326	0.473	0.288	0.357	0.448	0.246	0.326	0.387	0.310
12	0.210	0.387	0.407	0.349	0.295	0.261	0.272	0.382	0.430	0.423	0.437	1.000	0.382	0.405	0.317	0.242	0.211	0.392	0.375	0.226	0.425	0.228	0.318	0.338	0.214	0.240	0.355	0.242
13	0.194	0.357	0.340	0.383	0.246	0.335	0.304	0.357	0.313	0.347	0.354	0.391	1.000	0.809	0.357	0.197	0.180	0.410	0.385	0.287	0.421	0.513	0.337	0.335	0.218	0.249	0.383	0.243
14	0.230	0.366	0.330	0.359	0.254	0.338	0.334	0.364	0.338	0.360	0.383	0.414	0.809	1.000	0.383	0.203	0.218	0.396	0.415	0.283	0.428	0.513	0.371	0.358	0.263	0.276	0.372	0.244
15	0.354	0.370	0.407	0.420	0.240	0.528	0.508	0.379	0.490	0.325	0.546	0.324	0.358	0.379	1.000	0.217	0.249	0.437	0.629	0.471	0.409	0.306	0.398	0.377	0.205	0.343	0.440	0.271
16	0.348	0.300	0.293	0.238	0.283	0.205	0.306	0.238	0.240	0.236	0.314	0.242	0.198	0.200	0.212	1.000	0.358	0.250	0.279	0.227	0.340	0.224	0.243	0.284	0.357	0.247	0.198	0.270
17	0.763	0.221	0.222	0.262	0.171	0.184	0.140	0.193	0.227	0.187	0.272	0.210	0.182	0.218	0.248	0.357	1.000	0.253	0.198	0.280	0.221	0.200	0.336	0.345	0.376	0.254	0.245	0.356
18	0.366	0.515	0.667	0.592	0.431	0.420	0.325	0.464	0.445	0.449	0.450	0.397	0.405	0.392	0.437	0.250	0.259	1.000	0.464	0.376	0.565	0.266	0.422	0.463	0.278	0.324	0.518	0.231
19	0.330	0.388	0.423	0.396	0.271	0.479	0.474	0.416	0.494	0.360	0.571	0.379	0.369	0.398	0.607	0.279	0.201	0.453	1.000	0.342	0.470	0.302	0.325	0.356	0.213	0.318	0.376	0.177
20	0.352	0.289	0.266	0.377	0.165	0.348	0.456	0.256	0.305	0.284	0.333	0.227	0.291	0.289	0.471	0.230	0.280	0.373	0.363	1.000	0.349	0.340	0.392	0.402	0.276	0.469	0.415	0.235
21	0.220	0.496	0.499	0.469	0.270	0.438	0.387	0.449	0.424	0.443	0.480	0.430	0.420	0.421	0.403	0.340	0.217	0.561	0.469	0.344	1.000	0.258	0.367	0.410	0.237	0.328	0.450	0.214
22	0.205	0.250	0.222	0.271	0.191	0.269	0.332	0.259	0.257	0.243	0.299	0.238	0.508	0.507	0.309	0.219	0.198	0.270	0.316	0.343	0.266	1.000	0.340	0.352	0.248	0.307	0.274	0.245
23	0.336	0.405	0.356	0.371	0.178	0.338	0.361	0.333	0.373	0.314	0.370	0.321	0.332	0.370	0.412	0.245	0.333	0.428	0.331	0.387	0.374	0.327	1.000	0.431	0.433	0.440	0.392	0.212
24	0.350	0.319	0.345	0.446	0.289	0.343	0.335	0.320	0.360	0.281	0.451	0.337	0.335	0.355	0.376	0.284	0.341	0.461	0.362	0.398	0.409	0.344	0.421	1.000	0.284	0.325	0.378	0.317
25	0.410	0.255	0.254	0.224	0.221	0.153	0.237	0.249	0.271	0.236	0.251	0.219	0.219	0.263	0.216	0.358	0.385	0.280	0.225	0.274	0.245	0.245	0.435	0.291	1.000	0.487	0.336	0.311
26	0.257	0.253	0.258	0.371	0.196	0.319	0.529	0.263	0.277	0.317	0.330	0.243	0.252	0.281	0.346	0.247	0.256	0.328	0.323	0.468	0.334	0.295	0.445	0.336	0.493	1.000	0.300	0.173
27	0.274	0.429	0.397	0.456	0.238	0.386	0.326	0.380	0.398	0.367	0.392	0.355	0.377	0.362	0.438	0.202	0.244	0.514	0.375	0.416	0.452	0.267	0.385	0.381	0.327	0.295	1.000	0.253
28	0.350	0.233	0.216	0.255	0.278	0.171	0.176	0.296	0.291	0.214	0.312	0.247	0.236	0.233	0.279	0.270	0.352	0.229	0.179	0.224	0.215	0.241	0.207	0.310	0.286	0.162	0.255	1.000

Figure 16 - Cyber security definitions: Average similarity score matrix

Since the similarity score is asymmetric (Lintean, 2011) for some of the methods (Text A → Text B ≠ Text B → Text A), as illustrated by the different values in the upper triangle compared with the lower triangle, we calculated all the row (r) and column (c) means. This combined mean provided the overall similarity score per definition. Figure 17 shows these average similarity scores.

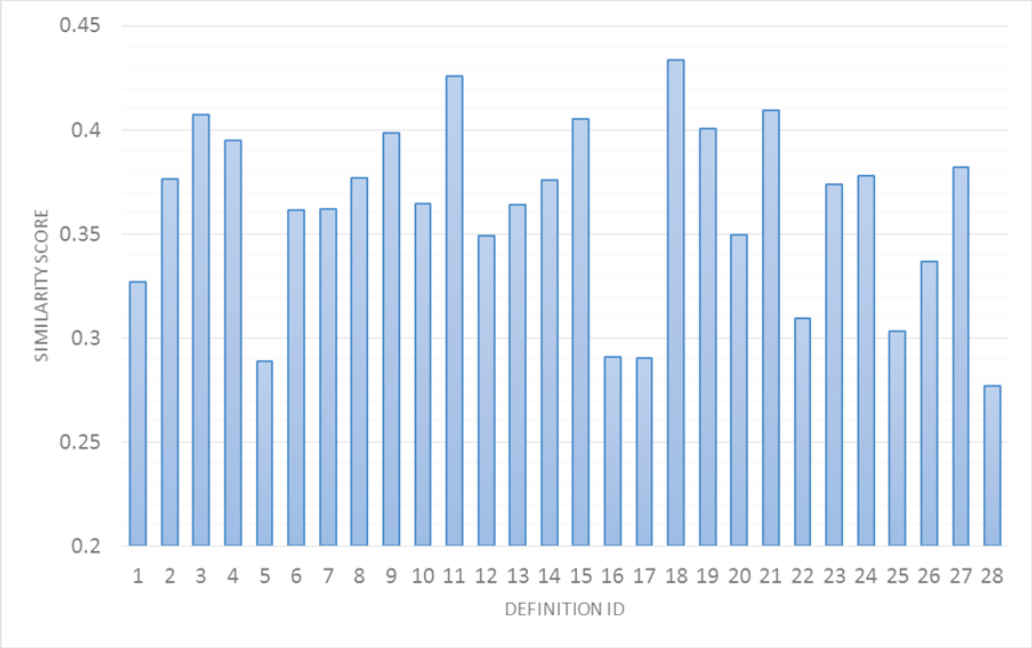


Figure 17 - Average similarity score per definition in the dataset

With this information, we produced a ranked order of the most representative definitions in the dataset. Table 15 shows an excerpt of the final list with the five most representative definitions of the definition pool ranked by similarity score across all nine methods and definitions.

Source	**Title**	**SimScore**
Republic of South Africa	Cybersecurity Policy of South Africa	0.434
French Network and Information Security Agency	Information systems defence and security France’s strategy	0.426
Spanish Cyber Security Institute	National Cyber Security, a commitment for everybody	0.409
International	SERIES X: Data networks, open	0.407

Telecommunication Union	system communications and security	
New Zealand Government	New Zealand's Cyber Security Strategy	0.405

Table 15 - Top five most representative definitions

According to our semantic similarity approach, the most representative definition in our dataset of authoritative definitions is the following part of the South African cyber security strategy: *"Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and assets"*.

Although definition #18 is part of a more exhaustive definition proposed by the International Telecommunication Union (2008), it comes out top because of its relative conciseness. On the flip side, brevity is not crucial to a representative definition (in the context of the pool of our authoritative definitions) as illustrated by definitions #16, #17 and #28. These are concise but lack sufficient descriptive depth to capture the meaning of cyber security, both objectively, as shown in the comparison, and subjectively (although this leaves plenty of room for argument). It is important to point out that we did not identify this to be the most relevant definition through expert opinion but rather through unbiased similarity analysis based on an authoritative set of definitions. This is important to distinguish as this approach rules out any bias introduced by subject matter expert view and opinions. The described analysis is not affected by potential agendas of individuals or recency bias, instead it presents an impartial view on the most relevant components of previously agreed authoritative definitions. It represents the unbiased essence of the worlds subject matter experts work on what defines cyber security. Definition #18 thus best captures the essence of all the authoritative definitions in the dataset.

3.5 Towards an improved definition

After identifying the most representative definitions of cyber security, the next step was to construct an improved definition to be measured under the same conditions to compare similarity scores. By using KH Coder (Higuchi, 2015), a computer-assisted qualitative analysis tool for content analysis and text mining, we investigated the previously mentioned top five definitions (#18, #11, #21, #3, #15) under the assumption that they contain the most relevant attributes. To establish the key underlying concepts needed to create an improved definition, we used co-occurrence network analysis (Rice & Danowski, 1993). In textual analysis, co-occurrence networks show words with similar appearance patterns and thus high degrees of co-occurrence. The approach is based on the idea that a word's meaning is related to the concepts to which it is connected. It also has the benefit that no coder bias is introduced other than to determine which words are examined (Ryan & Bernard, 2003). However, applying the function on our definition set produced a crowded output difficult to navigate even though it was already limited to five paragraphs and a minimum spanning tree had been applied. By filtering for term frequency (TF ≥ 2) when producing the co-occurrence network graph, we reduced the information presented to a (human) manageable level while preserving the important context.

Figure 18 shows the minimum spanning tree network graph model with 32 nodes and 25 edges extracted. The graph highlights the underlying concepts inherent to the words used in the definition set. In addition to the minimum spanning tree, we added community detection to further emphasise the connected components. The node size illustrates the term frequency and detected communities are highlighted in different colours. Based on the dataset, we found that the 'random walk' or 'walktrap' algorithm (Pons & Latapy, 2005) provided the subjectively best community detection approach. Combined with the minimum spanning tree, this explains not only the key concepts but also how words are grouped into communities and which communities are closer to each other (signified by the dotted lines).

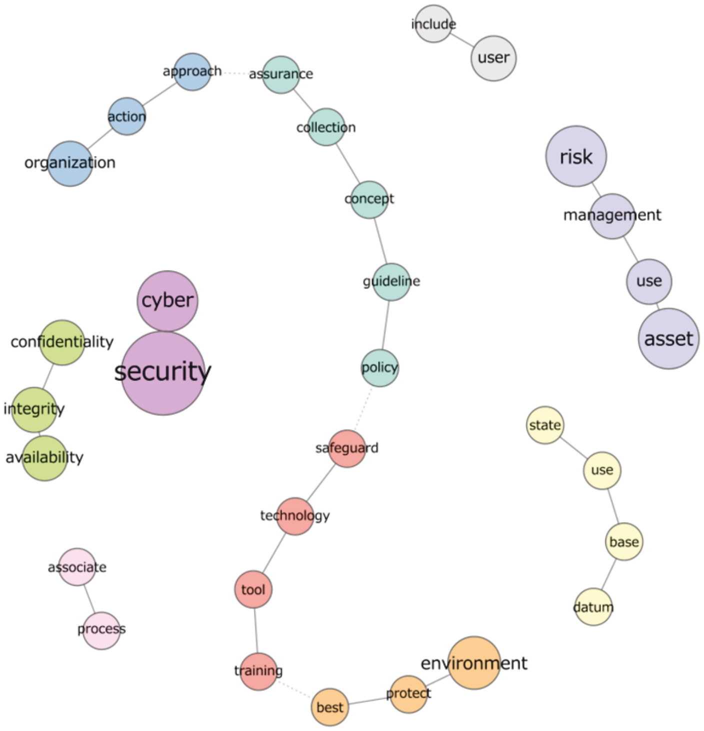


Figure 18 - Top five correspondence analysis (TF ≥ 2)

With the key components extracted, we were now able to propose an improved definition. Through several iterations of manual sentence construction by using words and communities, we arrived at a definition that captures the key components and respects community adhesion:

"The approach and actions associated with security risk management processes followed by organisations and states to protect the confidentiality, integrity and availability of data and assets used in cyber space. The concept includes the guidelines, policies and collections of safeguards, technologies, tools and training to provide the best protection for the state of the cyber environment and its users".

To verify that this definition is representative not only from a human reader perspective but also in terms of semantic similarity, we repeated our semantic analysis benchmarking work with our new definition included (#29), as shown in Figure 19.

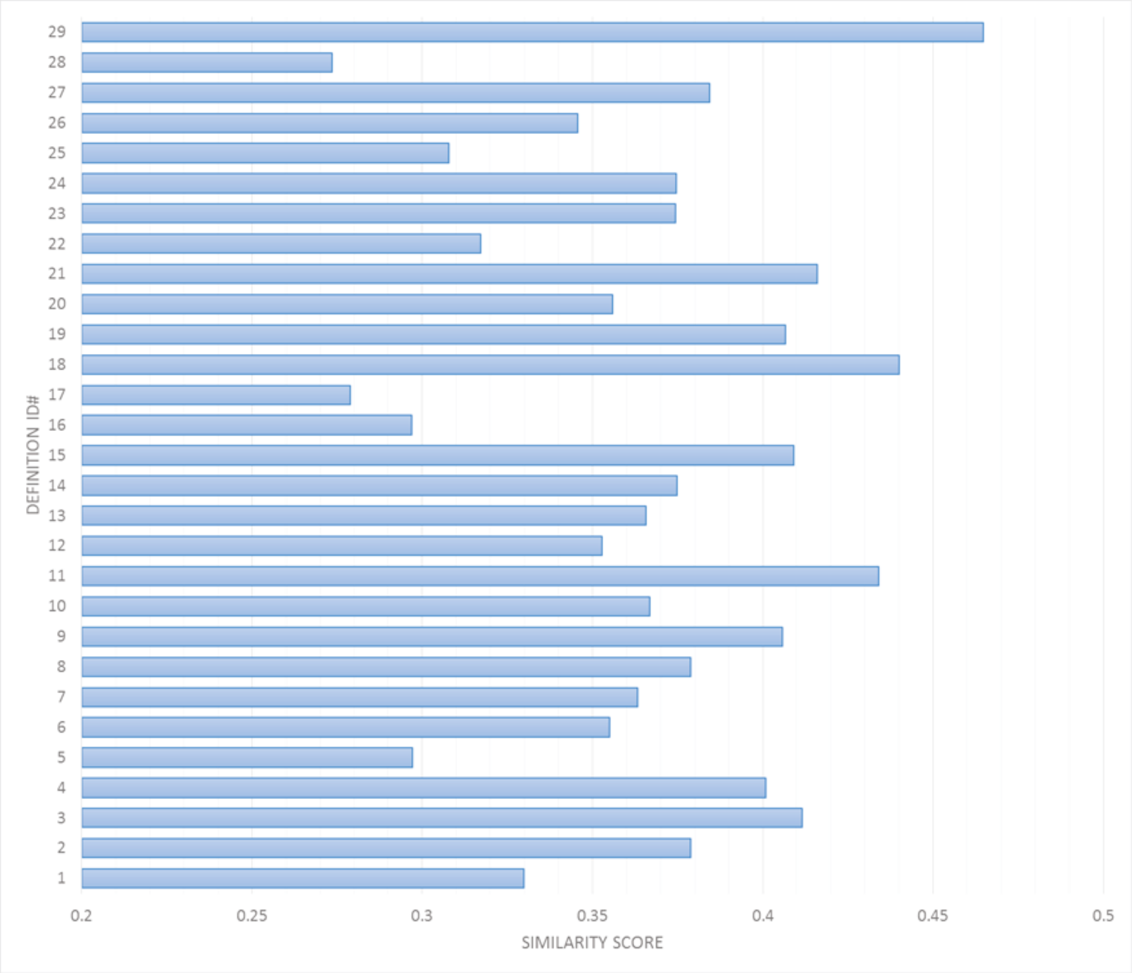


Figure 19 - Similarity scores including the improved definition (#29)

As expected, the overall results are nearly the same as those presented previously since the methodology and configuration of the benchmark are unchanged. While the individual scores have changed slightly because of the new addition to the corpus, the overall ranking remains the same, except for our proposed definition being included at the top, as shown in Table 16.

Source	Title	SimScore
New Definition	Towards a More Representative Definition of Cyber Security	0.465
Republic of South Africa	Cybersecurity Policy of South Africa	0.440
French Network and Information	Information systems defence and security France’s strategy	0.434

Security Agency		
Spanish Cyber Security Institute	National Cyber Security, a commitment for everybody	0.416
International Telecommunication Union	SERIES X: Data networks, open system communications and security	0.412
New Zealand Government	New Zealand’s Cyber Security Strategy	0.409

Table 16 - Top results for an improved definition

3.6 Study limitations and challenges to validity

In the previous section, we proposed a new definition for cyber security which tops the ranking of most relevant definitions among authoritative sources. However, as with many similar research exercises, there is no claim to completeness or infallibility of our work. Our study is affected by the limitations inherent to literature reviews described by Kitchenham and Charters (2007), such as those related to search comprehensiveness and material selection. To mitigate these shortcomings, forward and backward reference checking was conducted on the key publications to discover potentially relevant sources. Nonetheless, our efforts may have missed sources that we would have otherwise considered to be authoritative and relevant (although the number of definitions covered in this study should ensure relevance). The inclusion criteria may also lead to limited results from potentially relevant work towards a more comprehensive understanding of the cyber security space in general, or definitions still under development at the time of the research (CyBOK, 2018; Rashid et al., 2018). This is a limitation of the approach followed and should be addressed through a repeat study and extending the scope of such a study. Another inherent limitation to literature reviews is the language barrier, as this work only covered definitions provided in English.

Although we achieved our objective of creating a representative definition of cyber security, our approach was limited by manual sentence generation constraints. An automated approach, iterating all possible combinations of our nodes and communities leveraging natural language generation (Sauper & Barzilay, 2009), may have produced another, perhaps more relevant definition. This was beyond the scope of this thesis but will be considered for future work.

Lastly, considering the pace at which social communities create, adopt and modify their understanding of developing areas such as ‘cyber’ and ‘cyber space’, our definition is representative at the time of the research. It is expected that this definition will become less fitting or relevant as social, political and technological developments in this space progress. Nonetheless, our proposed model for evaluating definitions will prove useful and remain relevant in the future.

3.7 Chapter summary

For this research, we set out to analyse the landscape of authoritative sources defining the term cyber security. As part of this work, we conducted a semi structured literature review to identify relevant sources. Through our efforts outlined in section 3.2, we found 28 authoritative sources fulfilling our inclusion criteria and these were included for further analysis in the context of our research questions. This not only provided the platform to answer our research questions but also contributed an exhaustive set of authoritative sources for further research in this field. These sources represent the collection of the most informed definitions of the term at the current point in time. They are based on subject matter expert contributions from government officials, professionals and academics. Extensive efforts have gone into the creation of many of these definitions as described by Craigen et al. (2014). As described previously, the intention of this research is to present a condensed view of the relevant aspects across the definition pool towards a most representative definition. This approach also means that components of potentially incorrect definitions are included in the improved definition presented in this research. However, due to the large pool of authoritative sources, and the strict selection of authoritative definition sources as outlined in section 3.2, such issues are minimised.

We found the majority of the definition sources to be related to governmental institutions with several additional relevant sources from industry and academia (RQ1). Our review of the primary sources unveiled a clear lack of congruence as to the meaning and scope of the term. Even contradictory claims regarding scope were identified for several primary studies (RQ2). To better understand the differences in the definition set (RQ2) and identify the most relevant definition (RQ3), we applied basic (section 3.3) and advanced (section 3.4) semantic similarity analysis methods to the dataset. To our knowledge, this is the first endeavour to use this novel and non-biased approach to identify the most representative definition in a set (for cyber security). We showed that the South African definition achieved the highest similarity score and as such was the most representative definition of cyber security under the conditions of this work. To answer RQ4, we analysed the dataset further by using co-occurrence, semantic networks and community detection methods. By isolating the key components and communities in the definition set, we produced an improved definition of cyber security (section 3.5). Our new definition was shown to be the most representative definition according to the methodology used. This clarity on key aspects of the cyber security definition allows practitioners and other parties relying on unambiguous meaning of terms to confidently discuss the problem space. While we recognise the potential for the further improvement of this approach (section 3.6), we believe that the methodology and improved definition are noteworthy contributions to the field. The approach is useful to practitioners and researchers alike as it provides a way to quickly come to an unbiased agreed definition of the term in questions. Specific for cyber security, this exercise can be repeated with relative ease, including additional definitions. The improved definition as presented by this research is useful for practitioners who require a clear definition of what cyber security means, either for business, government or legal reasons. Our definition consists of the most relevant components across 28 authoritative definitions and is as such highly representative.

This brings us back to our original question of how information security and cyber security relate. Similarly to von Solms and van Niekerk (2013), we found confusion around the definitions of these terms. However, whereas those authors explore the definition of information security in depth, we focused our work on the definition of cyber security. In conclusion, both studies arrived at roughly the same point; information security and cyber security are related, but not analogous. Von Solms and van Niekerk see cyber security as a matter of interest to society at large, including critical national infrastructure. This description fits our proposed definition closely. It is also evident that the scope of cyber security resembles that of systemic or macroeconomic concerns. If we compare this with the assessment by von Solms and van Niekerk (2013) that *“the aim of information security is to ensure business continuity and minimise business damage by limiting the impact of security incidents”*, we note a much tighter focus on the organisational (microeconomic) level. This is an important distinction, as macroeconomic security aspects, including externalities and network effects, are not typically considered in a corporate security investments context. Consequently, our research is geared towards the information security value aspects within the organisational context and is not simply transferable to a systemic cyber security context as defined in the previous sections.

4 ECONOMIC IMPACT OF INFORMATION SECURITY BREACHES

To understand the value that information security can add to organisations, in this chapter we examine the impact of publicly reported information security incidents on the share prices of organisations. We used an event studies based approach where a measure of the event's economic impact can be constructed using security prices observed over a relatively short period of time. We use the source dataset available from the Privacy Rights Clearinghouse (PRC) to identify breached organisations in scope and retrieve their respective share prices from Thomson Reuters Datastream. Based on the results, we argue that although no strong conclusions could be made given the current data constraints, there was enough evidence to show that such correlation exists, especially for recurring security breaches. We envisage that as more breach event data become more widely available due to compliance and regulatory changes, this approach has the potential to emerge as an important tool for information security managers to help support investment decisions.

4.1 Related work

Organisations store an ever-increasing amount of information about their business partners, employees and customers and have a responsibility to protect this data. Thus, the protection of digital information has been and continues to be a growing concern across all areas of business. Related attacks are not only increasing in number and diversity, but also becoming more damaging and disruptive (National Institute of Standards and Technology, 2012). Despite increasing efforts to implement security controls to prevent information security breaches, we continue to see news of organisations suffering from such incidents (Passeri, 2013). As described by Cutler, Poterba, and Summers (1989), asset prices are generally attributable to changes in the fundamental value of the asset and as such react to announcements about corporate control, regulatory policy and market conditions that plausibly affect fundamentals. Under the assumption of an efficient market (Fama, 1970), and the rejection of the random walk hypothesis (Lo & MacKinlay, 1988), we assume that new information relevant to a traded equity becoming public knowledge has the potential to affect the market value of that equity (deBondt & Thaler, 1985; Fama, Fisher, Jensen, & Roll, 1969). This assumption has been the focus of various studies, as discussed below.

In all stages of the data lifecycle, namely data collection, data use, data storage, data retention and data destruction, sufficient protection must be provided against unauthorised use (Grama, 2010). Yet, we continue to see instances where this duty of care appears to fail as data is disclosed to unauthorised parties. While data breach is a widely discussed topic, there is little guidance in the literature on its definition. In this study, we follow the International Standards Organisation (2014), which defines a data breach as a compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to protected data transmitted, stored or otherwise processed. In their cost of data breach study, the Ponemon Institute (2014) finds that those breaches caused by malicious or criminal attacks incur a significantly high monetary cost. Consequently, in our research, we focus on information security breaches caused by malicious or criminal attacks. As it is notoriously difficult to obtain information on direct and indirect value loss resulting from an information security breach, a study of the market reaction to such an incident is the best proxy for the economic consequences. A common approach is the use of event studies, where a measure of the event's economic impact can be constructed by using the security prices observed over a relatively short period (MacKinlay, 1997). At the core of an event study is the measurement of an abnormal stock return during the observation window. The observation window typically includes the period leading up to the observed event, the event itself and the post-event period. The application of event studies in this form is well documented in academic research on corporate events such as earnings announcements, stock splits (Fama et al., 1969) and mergers and acquisitions (Duso, Gugler, & Yurtoglu, 2010).

Previous studies have adopted an event study methodology to investigate the effect of information security incidents on market value, including the works by Kannan, Rees, and Sridhar (2007), Yayla and Hu (2011), H. Cavusoglu, B. Mishra, and S. Raghunathan (2004), Campbell, Gordon, Loeb, and Lei (2003), Gatzlaff and McCullough (2010) and Garg, Curtis, and Halper (2003). On the contrary, T. Wang, Rees, and Kannan (2007) apply an event study methodology to financial reporting data rather than public breach announcements. Telang and Wattal (2007) apply the methodology to a precursory event (i.e. the announcement of software vulnerabilities) to observe the effect on stakeholders in this context. Andoh-Baidoo, Amoako-Gyampah, and Osei-Bryson (2010) extend previous event study results with decision tree induction to further examine the relationship between the independent variables.

The remainder of the chapter is organised as follows. The next section revisits the research methodology used. Sections 4.3 to 4.6 present the chapter research questions as well as the dataset used for the validation. In section 4.7, the experiment is described. The results are then discussed in section 4.8. The study limitations and potential threats to validity are covered in section 4.9. Finally, conclusions are drawn in section 4.9.

4.2 Event study methodology

Measuring, or even estimating, the true impact of information security breach events on the economic well-being of organisations is challenging. Industry reports such as the Ponemon study (Ponemon Institute, 2014) aim to approximate the value loss by considering various factors such as the expenditure on detection, escalation, notification, after-the-fact (ex-post) response, analysis of the economic impact of lost or diminished customer trust and confidence measured by customer turnover or churn. They also acknowledge the limitations of this approach. A possible alternative developed in the field of economics is the event study methodology. An event study is a statistical approach relying on the assumption of efficient markets to identify the abnormal returns resulting from an event. MacKinlay (1997) explains that the usefulness of such a study stems from the fact that the effects of an event will be reflected immediately in security prices given rationality in the market. Although this relies on the assumption of an efficient or rational market, which is not without its problems (Malkiel, 2003), the results produced are perceived to be a fair 'cause–effect' approximation.

At the core of an event study is an asset measurable over time (e.g. equity value) and an event suspected to affect the value of that asset. Practical issues such as data availability for a chosen asset should be considered early on. Obtaining the necessary dataset to complete the study may be difficult (where data are not publicly accessible) or infeasible because of cost and resource constraints. To conduct such a study, the time of the event must be defined and a time window constructed around it. This window includes the period leading up to the event (estimation window), a narrow event window and a post-event window to measure the impact. The selection of the event window needs to strike a balance between being too narrow, potentially missing leading or trailing reaction, and too broad, risking misleading results through confounding events and other long-term event study issues (Kothari & Warner, 2004). With these basic requirements in place, normal asset returns can be calculated throughout the estimation window as well as potential abnormal returns in the event window by using two common approaches: the constant mean return model and the market model. A detailed description of the intricacies and varieties of these models is outside the scope of this thesis. Further details can be found in Brown and Warner (1985) and Kothari and Warner (2004).

4.3 Chapter research questions and approach

Although the event study methodology has been applied to study the economic impact of information security events, research remains limited compared with other areas, particularly considering the increasing interest in and prevalence of publicly reported information security breaches. This study therefore aims to extend existing research by investigating the stock price reaction of organisations that have been affected by more than one information security event. The study seeks to answer two main research questions:

- RQ1: Do publicly reported information security breaches impact the stock prices of the affected organisations?
- RQ2: Is there a difference in stock price impact, compared with a previous breach in that organisation, if organisations experience a subsequent information security breach event?

These questions are formulated as the following two hypotheses:

- H_1 – Publicly reported information security breaches do not lead to abnormal returns for the stock price of the affected organisation.
- H_2 – There is no difference in the stock price reaction between the first measured breach event and a subsequent breach event for an organisation.

Through RQ2, we examine the reaction of market participants if the same organisation is breached repeatedly. We try to clarify whether investors penalise organisations in such cases (i.e. those that fail to provide tangible improvements in information security), show indifferent behaviour or even react positively. To answer these research questions, the study needs to meet several conditions. Figure 20 provides a high-level view of the approach and workflow followed.

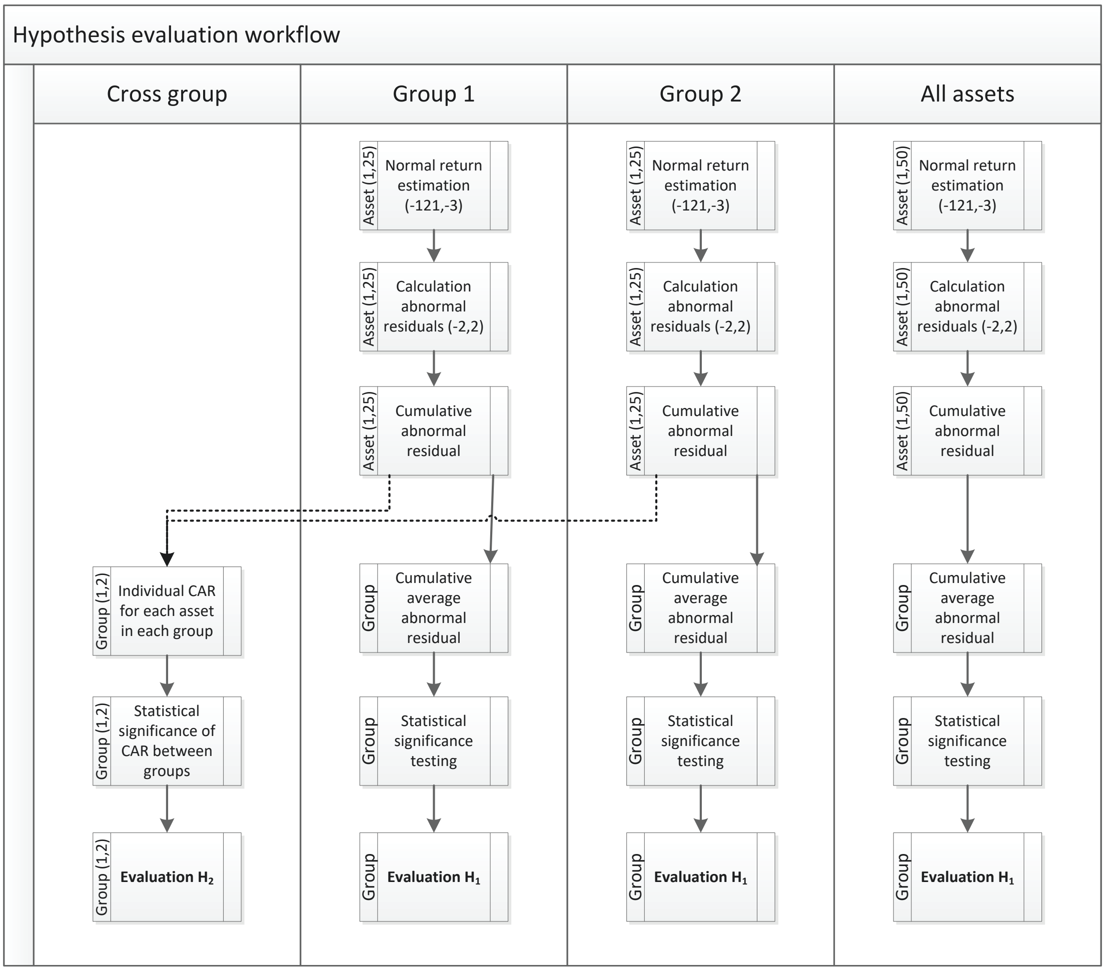

Hypothesis evaluation workflow
Cross group
Group 1
Group 2
All assets
Asset (1,25)
Normal return estimation (-121,-3)
Asset (1,25)
Calculation abnormal residuals (-2,2)
Asset (1,25)
Cumulative abnormal residual
Group
Cumulative average abnormal residual
Group
Statistical significance testing
Group
Evaluation H_1
Asset (1,50)
Normal return estimation (-121,-3)
Asset (1,50)
Calculation abnormal residuals (-2,2)
Asset (1,50)
Cumulative abnormal residual
Group (1,2)
Individual CAR for each asset in each group
Group (1,2)
Statistical significance of CAR between groups
Group (1,2)
Evaluation H_2

Figure 20 - Event study approach and workflow overview

As shown in Figure 20, the normal returns for each asset (stock) in each group are estimated based on the corresponding estimation window (-121 to -3 days). Then, abnormal returns are calculated based on the event window for each asset (-2 to +2 days). This approach results in a cumulative abnormal residual for each asset from which a cumulative average abnormal residual (CAAR) is calculated. Statistical significance tests are then applied to evaluate the results against the stated hypothesis in the workflow (Group 1, Group 2 and All assets). Cross-group calculations are also conducted based on the individual cumulative abnormal returns (CARs) for Group 1 and Group 2.

4.4 Event data sample selection

In this analysis, the requirements for the underlying event dataset are rather high, as the simple selection of organisations that suffered a security breach is insufficient to answer H_2. The datasets available from the Open Security Foundation's DatalossDB[4] and Privacy Rights Clearinghouse (PRC)[5] were considered. While the data available from DatalossDB are likely to be the most exhaustive repository available, their use for academic research is ambiguous because of copyright issues (Widup, 2012). On the contrary, the PRC data pose no such issue but are not as exhaustive and almost exclusively focus on US-based entities. However, this limitation was not an issue for our work and, accordingly, the PRC dataset was chosen for our experiment.

The PRC database provides information on data breaches reported since 2005 categorised as *Business, Educational, Government and Military, Healthcare* and *Non-profit Organisations*. Breach information is then categorised as *Unintended disclosure, Hacking or malware, Payment card fraud, Physical loss, Portable device, Stationary devices* and *Unknown or other*. For this study, the full dataset for the *Business* category (i.e. excluding EDU, GOV, MED and NGO) was retrieved. The dataset was reviewed for repeat breaches and filtered for events classified as 'HACK', 'DISC' or 'UNKN'. The other categories ('CARD', 'STAT' and 'PHYS') were not considered because this study focuses on information security breach events. The remaining 180 events were screened based on the following criteria:

- Public company listed on a stock exchange
- Price data available[6]
- Not acquired, merged or ceased trading
- No overlapping event windows for repeated breaches or duplicate events
- No notable confounding events close to the event window[7]

[4] http://datalossdb.org/.

[5] http://www.privacyrights.org/data-breach.

[6] Data source – Thomson Reuters Datastream.

[7] Data source – Recorded Future (https://www.recordedfuture.com/).

After applying the selection criteria, 25 organisations were filtered, each with two breach events. These breach events do not necessarily represent the first breach events for an organisation, or even the second or latest because of the limitations of the data available in the PRC database. The data sample for this study thus consists of a breach event that happened at an earlier stage and another that happened at a later stage in the trading history of an organisation (Table 17).

Selection steps	No. of records
Total events retrieved from the PRC data	1490
Events for organisations affected twice or more	409
Events categorised as DISC, HACK or UNKN	180
Events meeting the suitability criteria	50

Table 17 - PRC dataset

4.5 Price data selection

To calculate the potential abnormal returns, the stock price time series for each organisation in the event pool was required. Various sources for such information are available ranging from free services such as Google Finance and Yahoo! Finance to commercial providers such as Bloomberg, the Center for Research in Securities Prices and Thomson Reuters. Many previous studies prefer the data provided by the Center for Research in Securities Prices, whereas this study used Thomson Reuters DataStream, which has comparable quality (Ince & Porter, 2006). To retrieve the relevant time series data, we needed the correct identifier for the equities examined as well as an appropriate time window. The time window for the price data was defined as 121 days before the event date to 30 days after based on previous studies examining short horizon event effects utilising a similar estimation window (Dyckman, Philbrick, & Stephan, 1984; Patell, 1976). This approach maximises the estimation time window, while avoiding overlap with an information security breach event affecting the same asset earlier in time. The setup of this study prevented an extension of the pre-event time window without introducing overlapping estimation windows between events. To analyse the events following the market model time series, data from Standards & Poor's 500 Composite were retrieved. The S&P 500 was selected as this is listed as the local market index for the majority of the examined assets.

4.6 Data preparation and analysis method

Before conducting the analysis, sense checks and some formatting had to be conducted for the collected data. Two data issues were investigated: (i) when events fell on non-trading days and (ii) gaps (missing information) in the pricing data. Once checks were completed, the raw data were formatted as comma-separated values (CSV) following a predefined layout. To analyse the data, a standard market model methodology was chosen following Dyckman et al. (1984), who show that the market model offers more powerful tests than the mean-adjusted returns model and market-adjusted returns model for detecting abnormal performance. The market model is defined in equation (1):

$$R_{i,\tau} = \alpha_i + \beta_i \, R_{M,\tau} + \varepsilon_{i,\tau} \text{ with } E[\varepsilon_{i,\tau}] = 0 \text{ and } VAR[\varepsilon_{i,\tau}] = \sigma^2_{\varepsilon i} \qquad (1)$$

where $R_{i,\tau}$ and $R_{M,\tau}$ are the period returns for the asset and market, respectively. The alpha (α_i), beta (β_i), variance ($\sigma^2_{\varepsilon i}$) and prediction error ($\varepsilon_{i,\tau}$) values follow MacKinlay (1997).

For this study, ordinary least squares (OLS) was chosen as the estimation procedure over the procedure proposed by Scholes and Williams (1977). This is based on results from Dyckman et al. (1984) that showed that the Scholes–Williams method of estimating risk does not enhance the ability to detect abnormal performance when using daily data. Brown and Warner (1985) further comment that bias in beta events does not necessarily imply misspecification. All the calculations were carried out by using a simple return mode (versus continuously compounded - log return mode). The time windows of relevance were set as -121 to -3 days (estimation window) as explained in section 4.4 and -2 to 2 days (event window). We recognise that Dyckman et al. (1984) establish that the extension of the event window has a disproportionally negative effect on a model's ability to identify impact. However, an event window of 5 days (-2,-1,0,1,2) was chosen to account for any uncertainty around the event date. Uncertainty could emerge from many factors including the fact that security breach event dates are difficult to pinpoint because of factors such as news dispersion and the speed of adjustment to the information revealed. This type of information typically follows a dispersion process starting with limited coverage (e.g. information security-specific press) followed by wider coverage in technology outlets before it breaks to major news media outlets.

4.7 Experiment

As outlined in the previous section, the dataset covers 25 organisations with two security breach events each. The overall set of 50 events was separated into two groups, where Group 1 contained the earlier event of each pair and Group 2 the later event (Table 18, Table 19).

Symbol	**Organisation**	**Event date**	**Group**
@AAPL	Apple	9/4/2012	1
@CMCSA	Comcast	3/16/2009	1
@DRIV	Digital River Inc.	6/4/2010	1
@FOXA	Fox Entertainment Group	7/23/2007	1
@GOOG	Google	4/27/2007	1
@HKFI	Hancock Fabrics	11/23/2009	1
@SRCE	1st Source Bank	6/10/2008	1
EXPN	Experian	3/29/2007	1
H:ING	ING	2/12/2010	1
REL	LexisNexis	7/13/2009	1
U:C	Citigroup	9/21/2007	1
U:CFR	Frost Bank	5/19/2006	1
U:CVS	CVS	6/21/2005	1
U:EFX	Equifax	2/11/2010	1
U:HIG	Hartford	9/12/2007	1
U:JPM	JP Morgan	1/30/2011	1
U:LNC	Lincoln Financial Group	7/26/2011	1
U:MWW	Monster.com	8/23/2007	1
U:NYT	The New York Times	1/30/2013	1
U:ldos	Leidos	7/20/2007	1
U:T	AT&T	8/29/2006	1
U:TMUS	T-Mobile	6/7/2009	1
U:VZ	Verizon	8/12/2005	1

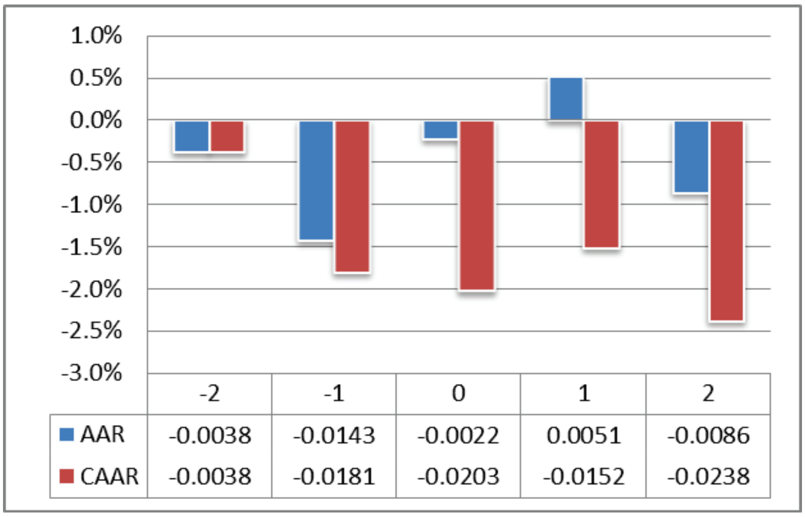
U:WFC	Wells Fargo	8/12/2008	1
U:WYN	Wyndham Hotels & Resorts	2/16/2009	1

Table 18 - Group overview - Group 1

Symbol	Organisation	Event date	Group
@AAPL	Apple	2/19/2013	2
@CMCSA	NBC Universal	2/22/2013	2
@DRIV	Digital River Inc.	12/22/2010	2
@FOXA	Fox Entertainment Group	5/10/2011	2
@GOOG	Google	3/7/2009	2
@HKFI	Hancock Fabrics	3/5/2010	2
@SRCE	1st Source Bank	11/19/2010	2
EXPN	Experian	4/5/2012	2
H:ING	ING	10/12/2010	2
REL	LexisNexis	6/8/2011	2
U:C	Citigroup	6/9/2011	2
U:CFR	Frost Bank	11/7/2007	2
U:CVS	CVS	3/24/2012	2
U:EFX	Equifax	10/10/2012	2
U:HIG	Hartford	4/6/2011	2
U:JPM	JP Morgan	3/28/2013	2
U:LNC	Lincoln Financial Group	9/16/2012	2
U:MWW	Monster.com	1/23/2009	2
U:NYT	The New York Times	8/27/2013	2
U:ldos	Leidos	1/18/2008	2
U:T	AT&T	6/9/2010	2
U:TMUS	T-Mobile	1/16/2012	2
U:VZ	Verizon	8/25/2006	2
U:WFC	Wells Fargo	10/20/2011	2
U:WYN	Wyndham Hotels & Resorts	2/28/2010	2

Table 19 - Group overview - Group 2

First, calculations were conducted for the events in Group 1 to obtain the results on the earlier breach data. As shown in Figure 21, the CAAR exhibits a decrease of 2.38% over the defined event window with a positive to negative ratio of 7:18.



	-2	-1	0	1	2
🟦 AAR	-0.0038	-0.0143	-0.0022	0.0051	-0.0086
🟥 CAAR	-0.0038	-0.0181	-0.0203	-0.0152	-0.0238

Figure 21 - Group 1 event impact

Based on the standardised cross-sectional test following the BMP approach (Boehmer, Masumeci, & Poulsen, 1991), with the adjustments proposed by Kolari and Pynnönen (2010), it was shown that the statistical significance is 1%. To verify the results of the parametric test, an additional non-parametric test was conducted. Following the observation by Cowan (1992) that the generalised sign (GSIGN) test becomes relatively more powerful as the length of the event window increases, the GSIGN test was selected over the rank approach proposed by Corrado (1989). For Group 1, the GSIGN test does not confirm the parametric test results and merely approaches the 5% significance level as shown in Table 20.

Event window	CAAR	Pos:Neg	BMP	BMP p	GSIGN	GSIGN p
(-2...2)	-0.0238	7:18	-2.9066	0.0037	-1.8993	0.0575

Table 20 - Test results for Group 1

To better understand the reason for this discrepancy, a manual review of the CARs of the individual assets was conducted. This was feasible as the sample size for this study was comparatively small. By plotting the results for Group 1 (Figure 22), it was found that the non-significant result in the GSIGN test is likely to be because of a strong outlier (U:WYN, -22%).

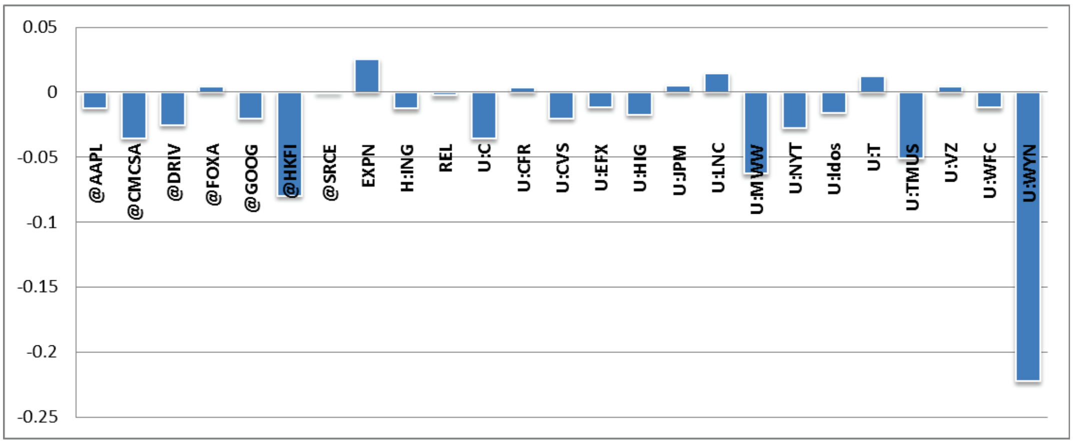
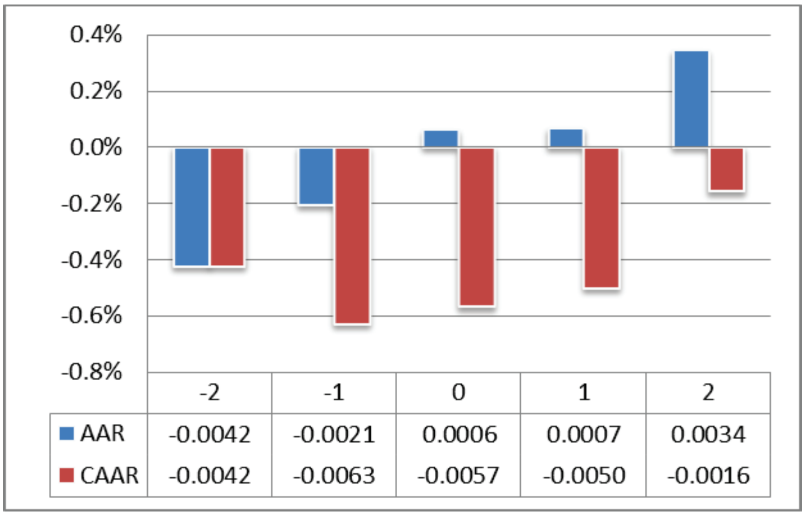


Figure 22 - Individual CARs for Group 1

As the data are non-normal, the strong significance level in the parametric test should be considered to be of limited relevance. Although non-parametric tests are not immune to outliers (Zimmerman, 1994), the rejection of H_1 seems to be likely given that the non-parametric tests approach significance. The calculations were repeated for the events in Group 2 by using the same approach as above. The results of Group 2 are noticeably different to the observations of Group 1, showing a CAAR of only -0.16% with a flat average abnormal residual distribution around the event date, as illustrated in Figure 23.



	-2	-1	0	1	2
🟦 AAR	-0.0042	-0.0021	0.0006	0.0007	0.0034
🟥 CAAR	-0.0042	-0.0063	-0.0057	-0.0050	-0.0016

Figure 23 - Group 2 event impact

Hence, the statistical tests provide no indication of significance for the results for Group 2, either for the parametric or for the non-parametric methods (Table 21).

Event window	CAAR	Pos:Neg	BMP	BMP p	GSIGN	GSIGN p
(-2...2)	-0.0016	9:16	0.0213	0.983	-1.1244	0.2608

Table 21 - Test results Group 2

As an additional verification, the individual CARs for each asset in the group were plotted. Figure 24 shows no outliers and exhibits a balanced dataset for Group 2.

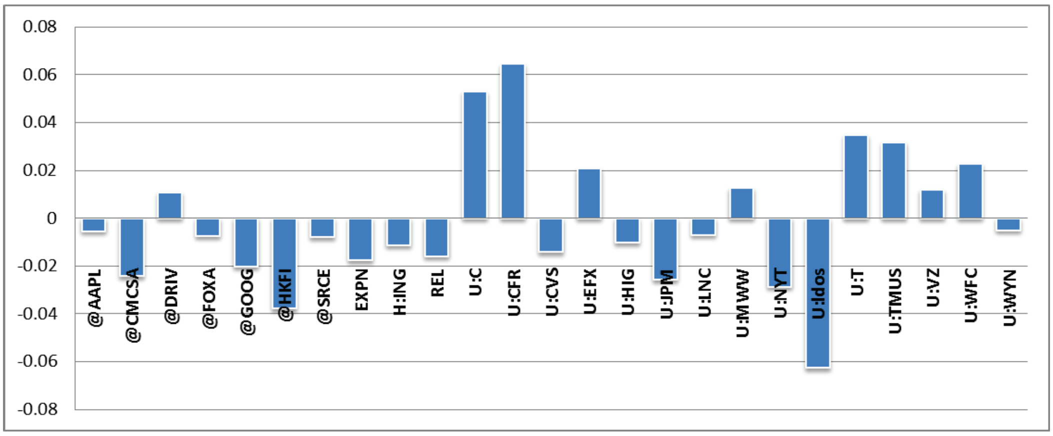
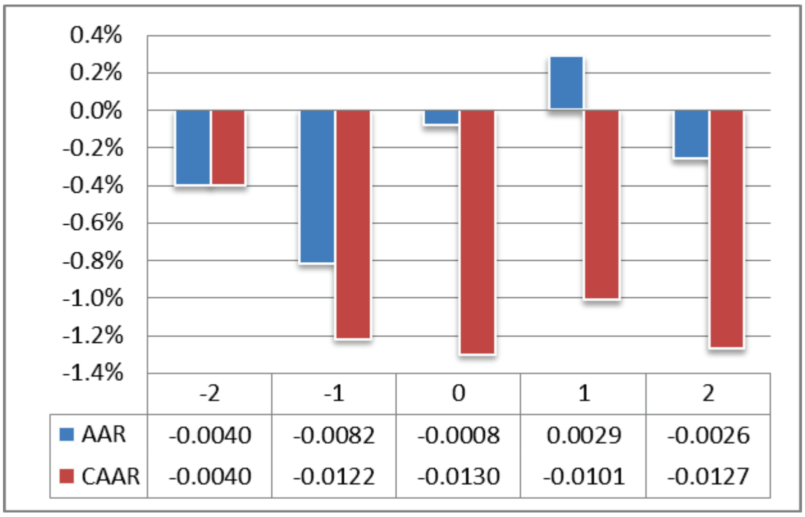


Figure 24 - Individual CARs for Group 2

The results for Group 2 show no statistical significance for any of the indicators; accordingly, H_1 for this group is not rejected. In addition to the calculations for each group, the combined event data were analysed and the CAAR showed a return of -1.27% carried by a 16:34 positive:negative ratio (Figure 25).



	-2	-1	0	1	2
🟦 AAR	-0.0040	-0.0082	-0.0008	0.0029	-0.0026
🟥 CAAR	-0.0040	-0.0122	-0.0130	-0.0101	-0.0127

Figure 25 - Event impact for the complete event pool

The parametric test showed low significance and suffered from non-normality in the dataset (as the Group 1 data are a subset and thus carry the same outlier issue). The GSIGN test results are well within the critical region, however.

Event window	CAAR	Pos:Neg	BMP	BMP p	GSIGN	GSIGN p
(-2…2)	-0.0127	16:34	-1.3943	0.1632	-2.138	0.0325

Table 22 - Test results for the complete event pool

Figure 26 plots the CARs for each individual asset in each group to illustrate the reaction of each organisation in the sample pool to both events.

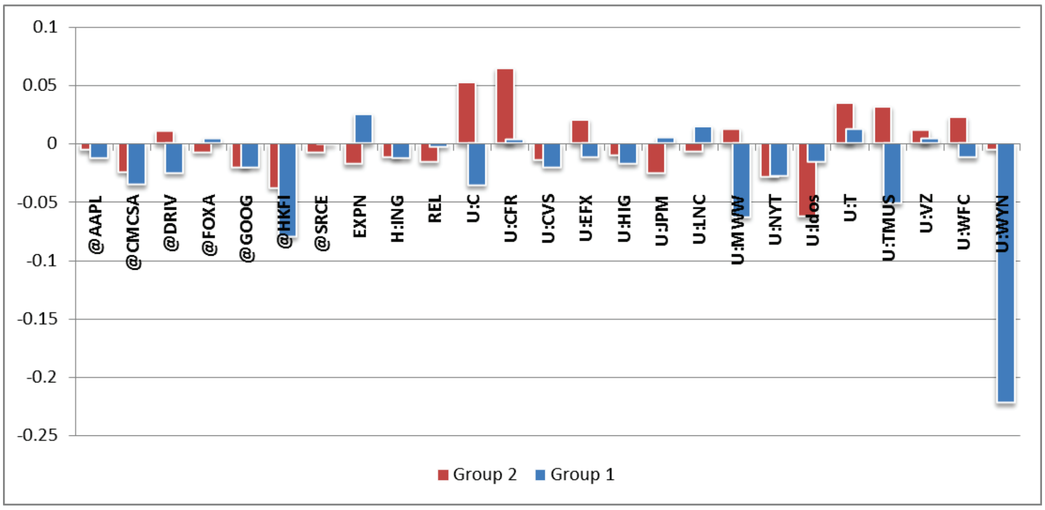


Figure 26 - Combined CARs for the event pool

Considering the outlier problem as well as the implications from the parametric testing, the results of the non-parametric tests are given priority for reaching a conclusion on $H_{1.}$ Taking all 50 events into consideration, we identified a significant negative effect (-1.27%) over the observed event window with a *p*-value < 0.05 (Pearson, 1900), as shown by the non-parametric test. To answer the question posed by H_2, the individual CARs for each asset in Group 1 were compared with those of Group 2 to understand if they are significantly different (Figure 27). A visual comparison of the individual CARs provided no clear indication, although Group 1 appeared to show a slightly stronger negative reaction.

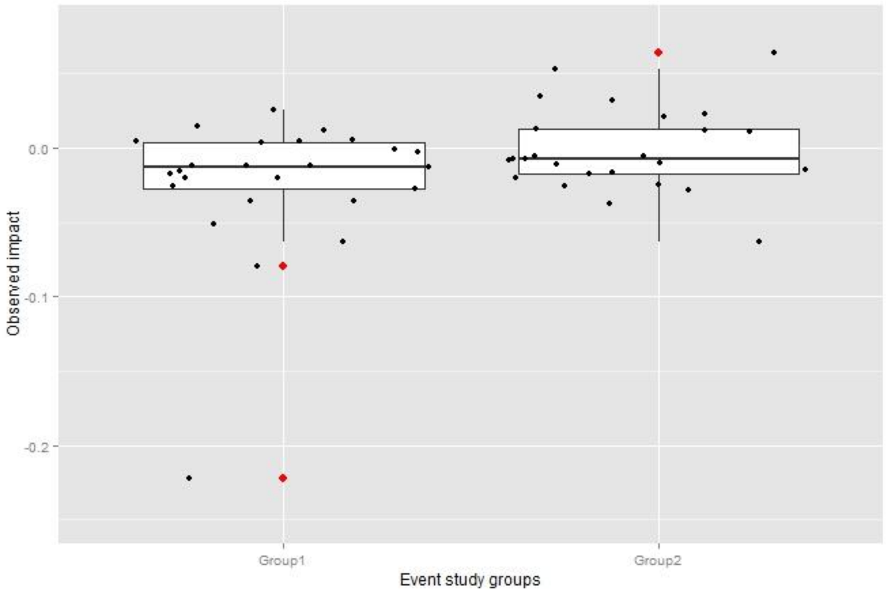


Figure 27 - Box plot of the individual CARs between the groups

By comparing the CAARs for each group calculated in the previous section, Group 1 showed a considerably stronger negative return (Group 1 -2.38%, Group 2 -0.16%). However, as noted earlier, this was driven by an outlier. To better understand the impact of the identified outlier, we temporarily removed the outlier in Group 1 from the dataset. This led to a move towards normality and resulted in a return of -1.55%; yet, a noticeably stronger negative reaction for Group 1 remained. As discussed earlier, the data in Group 1 are not normally distributed, which reduces the usefulness of parametric testing. To understand the extent to which the data are non-normal, a Shapiro–Wilk test (Shapiro & Wilk, 1965) was applied to both groups (Table 23).

Shapiro–Wilk test	**Group 1**	**Group 2**
W	0.671252696	0.963874
p-value	3.06201E-06	0.496879
alpha	0.05	0.05
normal	no	yes

Table 23 - Shapiro–Wilk test results

While a paired sample t-test was conducted, it was not taken into consideration. Instead, the non-parametric Wilcoxon signed-rank test for paired samples (Wilcoxon,

1945) was used to assess the significance of the differences in the dataset. The result showed a *p*-value of 0.074 for the two-tailed test, we thus could not reject H_2.

4.8 Results

For the CAARs in Group 1, we found a loss of 2.38% aligned with the event date (*p*=0.0037), using the standardised cross-sectional test proposed by Boehmer et al. (1991). This result in the parametric test is therefore likely to be driven by an outlier as described in the previous section. The non-parametric result under GSIGN testing, on the contrary, found significance approaching the 95% confidence level (*p*=0.0575). Considering the tendency of both test results, we thus reject H_1 for this group. For Group 2, we found a CAAR close to zero (-0.16%, not significant). Then, by applying the model to the whole event pool, we found a CAAR of -1.27% that showed significance for the non-parametric test (*p*=0.0325) but not the parametric test (*p*=0.1632), leading us towards rejecting H_1.

H_2 is addressed by comparing the cumulative abnormal residuals for Groups 1 and 2. The results of the Shapiro–Wilk test showed that the data in Group 1 are non-normal, suggesting the use of a non-parametric test such as the Wilcoxon signed-rank test to conduct the statistical evaluation. Although the difference in the absolute CAARs between Group 1 and Group 2 seemed to provide grounds to reject H_2, the statistical test did not support this initial notion. The Wilcoxon signed-rank test showed only marginal significance (*p*=0.074) for the two-tailed test, which is considered to be insufficient to reject H_2 in the context of this study. In other words, we found only weak statistical evidence that the market reacts differently to a subsequent breach event affecting the same organisation.

4.9 Threats to validity and study limitations

Based on the results of this analysis, we weakly conclude that there is an impact on the stock prices of organisations that suffer a publicly announced information security breach. The weakness in explanatory power is driven by several of the limitations inherent to event studies in general and this study in particular. The event study methodology relies on the assumption of an efficient market with rational players. In reality, this assumption does not necessarily hold in terms of either efficiency (Malkiel, 2003) or rationality (deBondt & Thaler, 1985; Dichev & Janes, 2003). Kothari and Warner (2004) caution that predictions about securities' unconditional expected returns are imprecise. Consequently, the greater the imprecision in the predicted returns (error factor), the lower is the explanatory power of the model on which it is based. In particular, for short-term event studies, knowing the precise event date is crucial. Uncertainty about the exact event date is an issue, and a compromise between data availability and dataset quality had to be made in this study. Yet, even if the precise date of the event is known, there is still uncertainty about the speed of information dissemination across market participants.

Further limitations stem from potentially unrelated events (confounding events) around the event dates, which are difficult to reliably identify ex post. In addition, challenges specific to RQ2 affected the time window between the first and second measured breach events. Following such an event, organisations not only work to mitigate the original breach cause but also invest in improvements and trust-building initiatives such as replacing key executive positions (e.g. Chief Executive Officer, Chief Technology Officer, Chief Security Officer). The potential influence of such activities on the subsequent breach event was not considered in this study. These potential issues as well as the outlier in the sample pool were magnified by the small sample size available for this study, thereby reducing the significance of the statistical tests. Hence, the presented results can be seen as an indication of impact tendency. Nonetheless, a tendency towards significance was identified and this could be emphasised if we only considered one-tailed test results.

4.10 Chapter summary

Understanding the role of information security in the context of the economic well-being of an organisation is a difficult yet important proposition (Anderson, 2001; Gordon & Loeb, 2002b). Research in this area has examined the approaches used by economists and applied promising methods to answer questions on the economic value of information security. One such approach, the event study methodology, was applied in this work. We relied on the assumption of an efficient market to measure the potential abnormal effects caused by an information security relevant event, using event data from the PRC database split into two groups. For the first group, consisting of each organisation's earlier breach event, we found an indication of a significant negative reaction (parametric *p*-value = 0.0037, non-parametric *p*-value = 0.0575). For the second group containing the latter breach events, there was no significant reaction (parametric *p*-value = 0.98, non-parametric *p*-value = 0.26). The combined event pool showed a tendency towards significance based on the parametric test (*p*-value = 0.1632) and non-parametric test (*p*-value = 0.0325) findings. Hence, we weakly concluded that information security events affect the economic well-being of organisations, as expressed by the corresponding stock prices based on the parameters of this study. For RQ2, we observed a difference in the reactions of the two study groups with a *p*-value approaching significance (*p*-value = 0.074 for the non-parametric test).

In summary, the selected methodology for evaluating the economic impact of information security breach events is promising. If some of the limitations discussed were addressed, such as the sample size and precise identification of event dates, the methodology could provide valuable input to support economic decision making within enterprise risk management programmes. This might become possible in the future if public information on data breaches becomes more widely available and more detailed, as laws and regulations become more explicit on the reporting of such incidents (Dipietro, 2013; Smedinghoff, 2006). This will provide a larger pool of useful data to which the methodology could be applied. A larger sample size would also allow more sophisticated analysis to be conducted and help draw more reliable conclusions.

Whereas this chapter provided an external view of the economic impact of information security breach events on organisations, the next chapter offers a broader insiders' view based on a qualitative analysis of senior security practitioner interviews. Building on the findings from the SLR (chapter 2) as well as the general questions on information security value and impact, we used a semi-structured interview to gather input from experienced practitioners.

5 QUALITATIVE ANALYSIS OF INFORMATION SECURITY VALUE IN ORGANISATIONS

Based on the Grounded Theory approach, in this chapter we analyse the data gathered in a series of interviews with senior professionals in order to identify key factors in the context of information security investment decisions. We present our findings condensed into a simplified but highly useful framework that security practitioners can utilise for critical review or improvements of investment decisions in their own environments. Extensive details for each category as extracted through a qualitative data analysis are provided along with a category network analysis that highlights strong relationships within the framework. Information security economics research, particularly earlier approaches, tends to be firmly rooted in the theoretical model space as we found in chapter 2, leaving the key challenges practitioners face unmentioned or unsolved. Although such models enhance approaches to examining information security investments, they often suffer from their overly theoretical methodology and, as such, are not well suited for real-world application. In this chapter, we identify how organisations prioritise and evaluate information security investment. Based on a series of semi-structured interviews, a qualitative analysis approach is adopted to understand the key factors, core challenges and common practices experienced by information security practitioners. In particular, we investigate the following questions:

- How are information security investments in organisations approached by practitioners?
- What key factors and challenges are considered by practitioners in relation to information security investments?
- How do information security management systems and information security governance models support practitioners in this regard?
- How are traditional accounting metrics such as NPV and ROI used?

The remainder of the chapter is structured as follows. In the next section, related work is presented. Section 5.2 discusses the research methodology and design as well as the interview framework including the sample strategy, data collection procedures, coding approach and analysis. Section 5.3 presents the results of the data analysis including participants' responses. Section 5.4 offers additional details on the relationships between the categories. Finally, in sections 5.5 and 5.6, the limitations of the approach presented in this study are thoroughly reviewed and concluding thoughts are provided.

5.1 Related work

Cyber crime-related loss is a serious issue threatening the economic well-being of most organisations (Anderson et al., 2013; Armin, Thompson, & Kijewski, 2016; Hyman, 2013). As such, organisations are either actively discussing how to deal with this situation or are already taking actions in the form of information security risk management programmes and aligned investments. In this context, Hoo (2000) quite rightly asked the difficult question as to how much is enough. As expected, there is no single right answer to this. Rather, Hoo stresses the need for quantitative computer security risk management to become more acute. Inevitably, the follow-up question will be how to sensibly allocate funds in order to maximise risk management benefits. Although this topic is still a relatively new field of research, a range of options for approaching the problem have been suggested over the past two decades (Eisenga et al., 2012; Kesswani & Kumar, 2015; Neubauer & Hartl, 2009; Sawik, 2013). Some solutions are more popular among researchers than others. For example, Cavusoglu et al. (2008) argue that investments in IT security should be managed differently from other investments by organisations. Their research proposes a game-theoretic approach that is illustrated to outperform an alternative decision theoretic-based approach. Bistarelli et al. (2007) discuss the use of defence trees to assess the effectiveness and economic profitability of countermeasures, leveraging economic indexes as a utility function. Furthermore, Garvey, Moynihan, and Servi (2013) refer to utility functions in their portfolio-based investigation that examines the delicate relationship of investments in countermeasures, the benefits provided to the organisation's security and their effects on its ability to achieve its mission. Srinidhi, Yan, and Tayi (2008), likewise, consider the ability of organisations to achieve their core mission in the context of information security investments. They analyse internal cash flows and the allocation of external funds to revenue-generating and security-assuring processes in the presence of security breaches, borrowing and financial distress costs over multiple periods. Similarly, Huang and Behara (2013) investigate the allocation of constrained information security budgets, finding that organisations with a limited security budget are better off allocating most or all of it towards measures to counter a certain class of attack.

To understand how practitioners in the field approach investment decisions, Moore et al. (2015) explore the ways in which organisations identify, prioritise and invest to manage risks in this context. Following a qualitative analysis approach, seven key points distilled from interviews with executives knowledgeable in this area are presented. The researchers conclude that a contradiction exists between high confidence in security frameworks guidance and the continued stream of breach reports. With regard to researching investment decisions in an IT governance context, Xue, Liang, and Boulton (2008) conduct a series of semi-structured interviews in an healthcare environment. The researchers highlight several findings and contextual factors relevant to IT governance processes in organisations, which play a key role in investment decisions. Rantapuska and Ihanainen (2008) follow a similar methodology to research how managers use knowledge when making investment decisions in this area. They report four contributing factors (problem, product, provider, solution) and conclude that investment decision making should reflect some of the features of organisational learning, where various forms of knowledge are used for a shared organisational purpose.

5.2 Research methodology and design

Understanding the way in which security investments are made in real work environments requires interaction and close cooperation with practitioners in the field. For this purpose, a qualitative research approach was chosen, as this allows for the collection of rich and vivid primary data from research subjects, which in turn emphasises the lived experience and is suitable for locating meaning and connecting such meaning to the social world (Miles & Huberman, 1994).

Grounded Theory (Glaser et al., 1968), in particular, is a suitable approach for this research. Based on a constructivist paradigm, this theory acknowledges that meaning is constructed by individuals and is not simply something merely waiting to be discovered. Whereas Glaser favours a ‘blank slate’ inductive approach under which the researcher has little or no knowledge of the topic, the Straussian (Strauss & Corbin, 1998) approach is better suited for the purpose of this paper, especially as Strauss advocates reviewing the relevant literature ahead of the study to stimulate theoretical sensitivity. To paraphrase Wolcott (1982), while there is benefit to being openminded and looking for questions as well as answers, it is impossible to conduct research without an understanding of what to look for. Specifically, semi-structured interviews were used to collect the primary data in this research. Interviews are typically an effective method of encouraging subject matter experts to talk about their experiences and opinions. They also provide an opportunity for the researcher to gain insights into the way in which people think about, feel about and relate to a topic.

This work adhered to ethical research standards and was approved by the University of East London under UREC 1516 128. All participants were issued with written information on the research project and research team. The purpose of the research was share with all participants describing the aim of the study being the analysis of current practices and approaches to information security investment evaluation in organisations to understand key factors and core challenges as experienced by information security professionals. It was explained that the results of the study will be analysed in conjunction with previous work (Systematic Literature Review, chapter 2) with the goal to create and verify an improved model assisting security practitioners in evaluating information security investments. In addition, guidance on confidentiality, data handling and storage as well as the voluntary nature of participation was provided in writing. Ahead of the interview, we addressed all concerns and emphasised participants' right to withdraw at any point in the interview process. Along with ethical research requirements, COREQ guidance (Tong, Sainsbury, & Craig, 2007) was followed when designing the research framework. Accordingly, information on the research team, affiliation and qualifications were made available to all participants. Furthermore, potential interviewees were chosen following a purposive approach (with a snowballing effect in some cases). Eighteen participants were interviewed as described below. One interview had to be removed from the dataset after completion, leaving a pool of 17 interviews for the analysis. Participants were mainly based in the United Kingdom (13), with five residing in the United States. All interview questions (Appendix 5-1) were developed by the research team and pretested in trial runs. In several instances, the research team followed up with participants to clarify or extend the responses given during the interviews; in all cases, the interviewees were willing to oblige.

Following the guidance presented by Miles and Huberman (1994), the research process was not strictly segregated into data collection and data analysis phases but rather took place as a parallel iterative process where possible. For each interview, the work cycle shown in Figure 28 was followed. In the first instance, an open-coding, sentence-by-sentence approach was followed, which led to an initial code list. As suggested by Miles and Huberman (1994), such an initial list may come from the conceptual framework, research questions, hypotheses, problem areas or key variables of the study. As the research process progressed, and as the researchers gained a better appreciation of the views and perceptions of the interviewees, 141 codes were refined through several iterations until a list of 79 codes remained. The coding and parts of the qualitative analysis process was completed using a web application for managing, analysing, and presenting qualitative and mixed method research data called Dedoose (SocioCultural Research Consultants LLC, 2016).

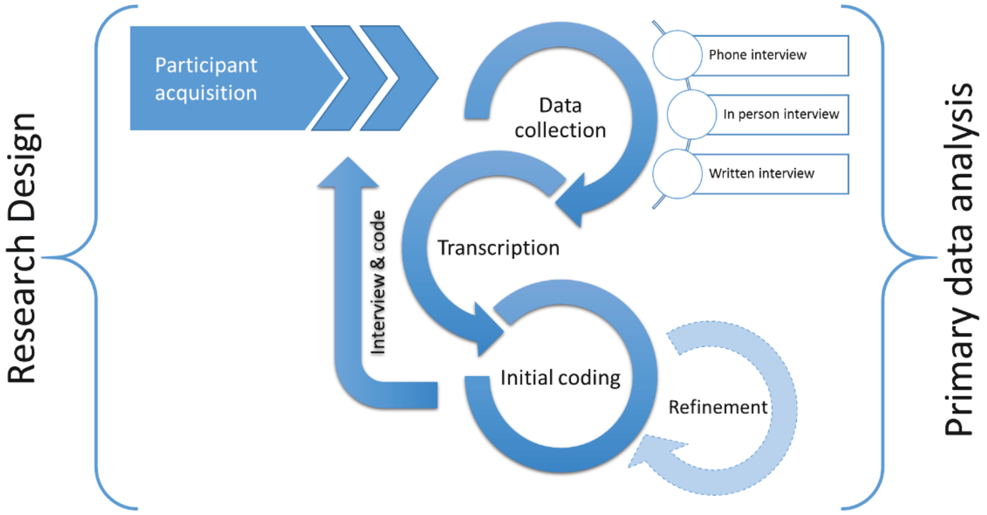


Figure 28 - Transition phases from design to analysis

Once open coding was done, the axial coding of the interviews was initiated. Axial coding reassembles the fragmented codes in which the data were broken down during the open coding to link these concepts to categories by comparing the properties, context and relations of the codes and inherent concepts. This comparison allowed us to see both patterns and variations in participants' statements and added dimensions to the categories that were not obvious previously. As is common for this research approach, the final step in the process is to integrate and organise categories around central explanatory categories or themes. Although this is considered to be the final phase, it is an evolving process, maturing throughout all phases of the research. It requires systematic examination, analysis and reflection on the data—tactics for generating meaning as described by Miles and Huberman (1994). Figure 29 presents a high-level overview of the journey of data coding and analysis.

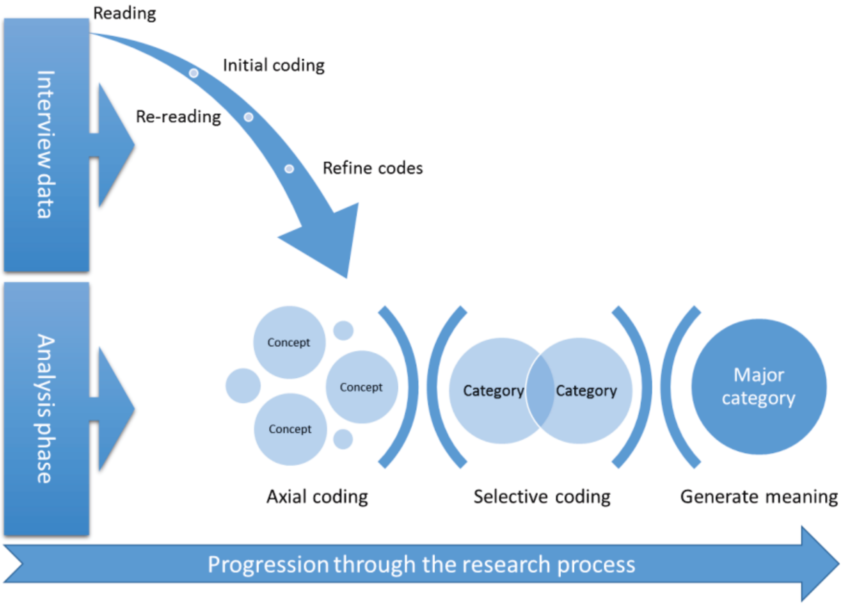


Figure 29 - Overview of the journey of data coding and analysis

5.3 Qualitative analysis

As participants described their views and experience, they frequently jumped between topics, pondered rival thoughts and ideas and generally blurred the boundaries between categories as they navigated their mental map. The research approach was designed to extract as much experience and knowledge as possible, but the richness of a single person's thoughts on this topic could not be fully captured or analysed as part of one paper, let alone all participants' thoughts. By examining, re-examining and reflecting on the views shared by participants, the relations and patterns used to generate meaning were thus identified. To make a useful contribution, complexity was stripped away and the simplicity of the key underlying components was presented. The condensed outcome in Figure 30 shows an overview of the information security investment framework as constructed by the participants.

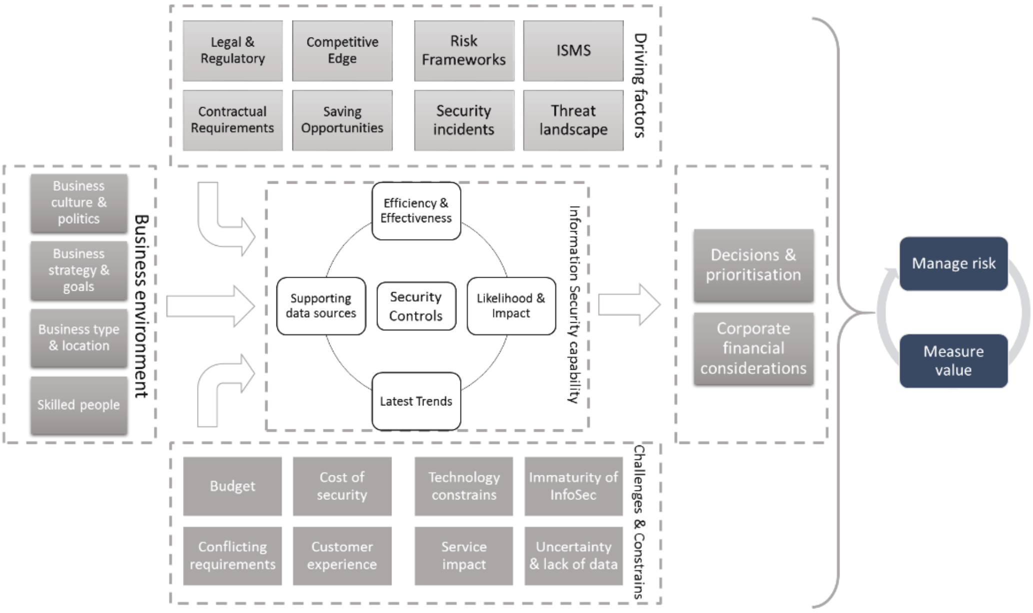


Figure 30 - Information security investment framework overview

This overview illustrates the key categories aligned with their theme. It provides a simplified framework of the context in which investment decisions for information security are made in an organisation's environment. Information security investments follow a decision support process initiated by 'driving factors' and adjusted by 'challenges and constraints'. Based on these driving factors and challenges, professionals select an appropriate security capability, which is then refined through corporate decision filters. Participants expressed that the main purpose of their programme is to add value to the organisation, commonly in the form of managed risk. This process is heavily influenced by the underlying business environment that defines what value means to a certain organisation. It was found that categories were commonly thought of in relation to other categories (i.e. within and across themes). Figure 31 illustrates this contextual relationship.

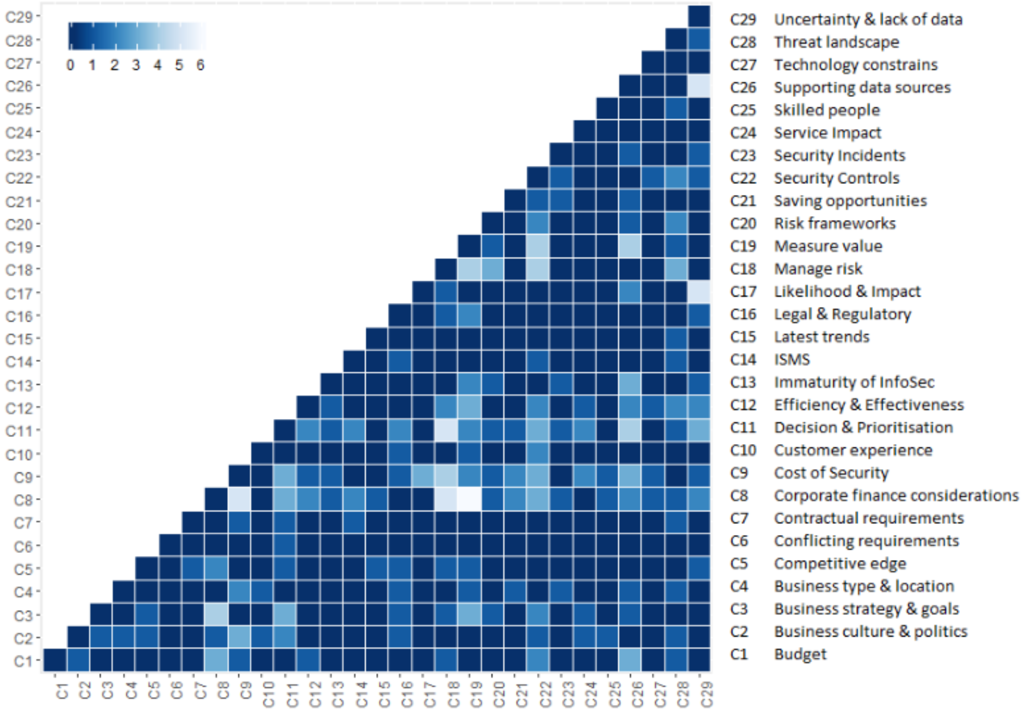


Figure 31 - Category co-occurrence matrix

5.3.1 Business environment

Businesses exist in a complex world with a multitude of factors influencing the plans and strategies of individual companies. Throughout the interview process, participants considered the business environment in which they are working to be a significant factor affecting their security investment approach. Their responses highlighted the importance of the industry and type of business to the information security strategy, with legal and regulatory requirements being an underlying theme. In general, business environments are used as a proxy for security-relevant factors. They explain the areas particularly important to the organisation. For example, an online retailer cares more about the availability of its web services than a bricks-and-mortar business would. Likewise, such a business would be more concerned about the potential reputational impact should a breach occur, which further impacts the way in which information security spending is prioritised.

Aligning security spending with business goals is a point that repeatedly came up during the interviews. We observed an inherent understanding that information security must form part of the value chain working towards the broader business goals while solving, often abstract, security-specific problems simultaneously. This comes with various challenges and has a strong impact on prioritisation, as discussed in a later section. Participants reported that business culture and politics influence their approach to information security. It is crucial to understand a company's risk tolerance levels and attitude towards security controls. Along similar lines, it was mentioned that it is worth paying attention to something that is best described as 'office politics'. When selecting technology and controls, careful consideration should be given to the preferences and expectations of key employees and departments (*"There's often a kind of acceptability to an organisation, so if network teams are completely fixated on CISCO, then proposing a CISCO project will go down well"*). An interesting development, especially in competitive sectors, was described where organisations strive to be on par or better in their security approaches than their competitors. In this type of organisational culture, investments in information security are not simply viewed as a cost factor. Similar to other areas that depend on highly skilled staff, information security departments rely on the right people to accomplish the job. Participants emphasised that one of the key components for delivering value is to have competent staff with the right skillset making the right decisions. Having a team of skilled professionals with backgrounds in various sectors has a positive impact on the performance of the information security programme. There was wide agreement that constant training and retaining skilled staff are important for success. At the same time, it was highlighted that the cost of finding and retaining skilled staff is a challenge.

> *Principle 1: The business environment provides the platform on which security investment value decisions are rooted. Without appropriately considering it, security programmes will fail to add value.*

5.3.2 Driving factors

As driving forces, legal and regulatory requirements were mentioned frequently across all sectors. Typically, these requirements define the minimum security stance in which an organisation invests. Organisations are growing conscious of cost implications, often in the form of fines if they are found to be in non-compliance of the regulations in their sector. However, such requirements are also used to simplify investment justification. Interviewees stated that security teams might use regulatory requirements to sidestep investment approval processes by linking their investment request to a 'must-do' requirement of a regulation. Although this may seem to be an insolent shortcut, it can be with the best intention to, say, get ahead of anticipated but not yet enforced regulatory changes. As described by one participant, it is hard to know all applicable regulations for a global organisation, let alone stay abreast of upcoming changes. Security teams who implement security controls that anticipate and prepare an organisation for upcoming requirements are seen as adding considerable value to the business. Legal and regulatory requirements also play a role when it comes to competitive advantage, especially in highly regulated sectors with strict mandates for security controls, where security is a key differentiator that can be used to gain competitive advantage. Regulations set the minimum security requirements, with all the inconvenience for customers that comes with it; thus, organisations try their best to make a user's experience as seamless as possible (*"Security is now probably one of the key differentiators within our sector … you know where customers will go, who they'll bank with and who they'll trust"*).

> *Principle 2: Legal and regulatory requirements are a key driver of information security investments. Such requirements are important investment justifications and provide an opportunity to positively differentiate an organisation from its competitors.*

Closely related to legal and regulatory requirements are risk framework requirements. For some sectors, these are externally imposed; however, many organisations voluntarily subscribe to information security-specific frameworks such as ISO/IEC 27001 (British Standards Institute, 2013) and the ISF Standard of Good Practice (Information Security Forum, 2016) to support their security programmes or achieve certification. As a consequence, these become a driver of investments. Participants described how information security management systems support their work in this context. These frameworks help identify gaps and weaknesses, provide a list of controls to consider and, to a certain extent, provide guidance on minimum investment levels. However, participants noted that these frameworks contribute little guidance on economically sensible investment in their environments. When asked if they thought that that should be the case, reserved responses were received. Many believe that it would be too difficult to include economic decision support as part of such a framework. Some expressed doubt that it would make any difference, as finance departments would not recognise information security frameworks as authoritative in the context of sensible investment guidance. Instead, larger organisations or regulated industries look to overarching operational risk or enterprise risk functions for this. One participant described how his information security management system was joined up with operational risk frameworks that factor in economic aspects. He explains that *"it's almost like security as a function has kind of mushroomed into these sub-functions with operational risk that contributes an economic view or financial driver"*. This was seen as beneficial since mature operational risk functions have established metrics and language that are well understood by finance departments and other non-technology stakeholders.

> *Principle 3: Security risk management frameworks drive information security investment decisions but provide little guidance on economically sensible investments. Integration or alignment with an operational or enterprise risk function helps add an economic dimension in this context.*

Information security is increasingly seen as a competitive advantage for both the business-to-consumer and business-to-business markets. Security in the former is a differentiator when paired with a seamless user experience and innovative solutions. Participants described their efforts to weave the required security controls into their services in a way that emphasised innovative approaches while enhancing customer experience. This is not done in isolation. Information security professionals collaborate closely with their business counterparts to seek feedback on what the market demands or favours. In the business-to-business space, the focus is on generating trust, with participants highlighting the importance of business relationships with partners, suppliers and business customers. Several high profile security breaches have been directly related to third-party service providers (Target Inc (2013) was a breach mentioned by several participants). Participants described how their area was becoming a key factor in supplier selection and consequently is perceived as a competitive advantage, even in sectors with limited regulatory oversight. Although security requirements are increasingly defined in contracts, surpassing expectations adds value, as it increases customer trust. Organisations are aware of the value of these investments in the continued success of their businesses (*"We are providing valued services and we are a trusted supplier. If you lose that trust, and that can happen in an instant, it takes a long time to build it up, so you never want to let it go"*).

Reducing the cost of operations or enabling an organisation to achieve savings on operations is another important aspect. Participants described a clear link between security controls and the quality of service improvements, which resulted in operational cost savings. An example was described where costly production line outages could be tied to security weaknesses in the delivery process. After implementing the appropriate security controls, outages declined considerably, resulting in improved availability and lower response costs. Some organisations take deferred costs into consideration; in this context, security controls enable an organisation to defer operational costs for a certain time so that they can focus resources on urgent opportunities. In many markets, it is important to be able to act swiftly to achieve or retain the first-mover advantage. If the resources of organisations are tied up with clearing technical debt or other legacy issues, momentum may be lost. By selecting appropriate controls, information security allows corporations to defer such operational costs to a later point while managing the risk accordingly.

Principle 4: Information security investments offer competitive advantage when they support businesses safely innovate, increase market agility and enhance customer trust.

Security incidents and developments in the threat landscape are common reasons for information security investments. In particular, security incidents appear to be a strong driver of investing in security, unfortunately after the horse has bolted. One participant commented on this rather cynically: *"The level of thinking on this topic is so immature that your best chance to be seen as a successful chief security officer is to have incidents and manage them well. There is no credit in avoiding them — if you have a clean sheet, nobody's interested"*. Post-incident reviews provide useful insights into the gaps and weaknesses in the current security stance and steer investment budgets towards the projects addressing these issues. Incident metrics play a key role in measuring the effectiveness of the programme as discussed later; they also help an organisation estimate the cost of the incident and, in turn, provide input to value discussions. Understanding the current threat landscape and ongoing developments is thus an essential aspect in a security management process. Knowing the relevant threats to their sector in general and to their organisation in particular, even down to the business unit level, enables security functions to direct their efforts (and as such investments) to where they add the most value. Participants try to keep pace with such a fast-changing threat landscape, often by proactively monitoring relevant threats and collaborating with other organisations. This includes not only exchanging information on threats and threat actors but also providing useful and effective security controls.

Principle 5: Security incidents have an immediate effect on security investments and the value perception of information security. Understanding threat trends is *crucial for the direction of security programmes and should steer investment accordingly.*

5.3.3 Challenges and constraints

Of the challenges and constraints faced by information security professionals, one of the most pressing is the budget allocated to the information security department. Some participants reported that their budgets do not increase as fast as compliance requirements demand. This prevents their security programme from covering as much compliance ground as required, let alone focusing on additional, real security threats. Responses indicated that simple financial models are occasionally used to prioritise security investments. However, most respondents are suspicious of the usefulness of such models. A general scepticism towards the way in which budgets are allocated in organisations was found. In most cases, organisations follow a conventional budgeting approach (Drury, 2013) where budgets are allocated annually based on a percentage of another budget, commonly IT. This traditional budgeting approach is viewed as problematic as it does not sufficiently account for the fast-paced changes in threat landscapes. In no case was an activity-based or zero-based budgeting approach reported.

Principle 6: Conventional budgeting approaches cause information security departments to direct their funds towards a 'minimum protection/maximum compliance' strategy rather than initiatives that contribute the most value to the organisation.

At the other end of the spectrum, participants reported that their challenge is not so much the available budget, but the capacity of organisations to absorb change. The main concern was negative user experience with a security control (*"If something is viewed as an obstructive control that will encourage people to work around it, then that is something that is likely to dissuade us more than any sort of economic or other consideration"*). Business stakeholders care about customer priorities, ease of use, product adoption rates and legal compliance; security must contribute value to these priorities. Security controls are not worth investing in if they are perceived to be cumbersome or obstructive. Participants commented that it is not always straightforward to anticipate the views of customers and thus they work closely with business stakeholders for better guidance. At times, this results in conflicting requirements. Customers, particularly in the business-to-business market, have high expectations of information security. This is a challenge for organisations trying to strike a balance between client requirements and the ‘right level’ of security costing. As aptly put by one of the participants, the business side always wants to have the new application faster, whereas the security side always wants it to be more secure. This leaves security teams with the challenge of proving that security controls add sufficient value to make it worthwhile implementing them. This point is discussed in more detail in a later section on security metrics.

> *Principle 7: Security controls must be accepted by users and customers to add value. For this, security teams must work with business stakeholders to understand what ‘acceptable’ means in a given context.*

Asking participants about security costs provided a range of views. A good understanding of financial aspects, mostly distinguishing between operating expenses (OpEx) and capital expenses (CapEx), was observed. Costs related to staffing were a concern, with the lack of affordable talent and resulting lengthy hiring processes being a common challenge. This has an immediate impact on solution selection as well as the cost structure of investments. Participants reported that they are unable to find skilled people to implement, support or use the preferred solution. Costs for the specialised training of security staff are factored into this as well. Generally speaking, solutions with lower staff and training costs were seen as more favourable. Similarly, external consultants are often hired to supplement staff to be able to add value more quickly. In some cases, consultants are used to achieve a more favourable cost structure (CapEx vs. OpEx), which serves the accounting preferences of the organisation better. The direct costs considered for security solutions are unsurprising. Participants mentioned the initial purchase price, license cost, implementation, configuration and ongoing maintenance costs, overhead cost for project management resources, customer or user communications, training cost, datacentre space, power and HVAC (heating, ventilation, air conditioning) cost as well as professional services cost. Some responses extended this by considering the integration cost with existing solutions and the sunk cost for non-performing controls. The majority of participants explained that they consider the potential impact of the control on the performance of existing systems, including the expected future downtime requirements for updates and maintenance. In a similar vein, it was mentioned that rewriting and testing ‘disaster recovery and business continuity’ plans may be an indirect cost. Several participants considered the opportunity cost in various forms including avoiding lost customer contract opportunities through proactive security investment, weighing the impact of a security solution implementation on other business resources (and thus tying up resources that would have contributed to revenue-generating projects) and calculating the value of temporarily supplementing the workforce to free up higher value resources to work on other business projects. It is assumed that this keen awareness of the opportunity cost is due to the unusually high amount of competing requirements and risks related to a firm's security stance.

As discussed previously, security incidents are a strong driver of investments in security. The potential cost of compromises plays a major part in the economic calculations in this context. Some of these costs are relatively straightforward to capture, such as the cost of legal counsel, cost of public relations damage control, cost of credit monitoring for affected customers, cost of specialised incident response and forensic consultants, regulatory fines, contractual fines, cost of lawsuits, staff overtime cost, direct losses due to service outage and insurance premium increases. The views on the loss of intellectual property were mixed; some responses suggested it to be a direct cost, while others saw it more on the indirect side as it is difficult to know what financial value a particular property would have had without the compromise occurring. Similarly, with regard to reputational loss, there were varying views. One participant argued that it could be approximated through metrics such as 'abnormal customer churn rate', whereas others recommended not using soft costs such as reputational loss at all. In general, there was a feeling that information security should seek help from other functions such as public relations, legal and operational risk to ascertain a better input on the economic impact of large events. Those who considered indirect costs in their calculations suggested looking at the loss of market share (e.g. abnormal churn rate), loss of prospective customers (e.g. abnormal customer conversion rates) and loss of trust by customers. A company's share price is a measure often mentioned in this regard and some responses suggested looking at share prices pre- and post-breach as a proxy for the cost of compromise. However, some suggested avoiding share prices as a metric. One particularly interesting point mentioned during the interviews was to consider the impact of security breaches on staff morale and the costs resulting from demotivation, distractions, distrust and private concerns seen with deeply intrusive compromises such as those faced by Sony Pictures Entertainment (Hess, 2015).

Principle 8: Human resources costs and incident-related costs are crucial to value equations for information security. Practitioners must consider a range of relevant cost factors, both direct and indirect, to approximate the incurred loss with a priority on realistic impact figures.

Participants explained that the immaturity of the information security profession is a challenge itself. Practitioners look to mature areas such as the operational risk and enterprise risk functions for guidance and note a lack of evidence-based decision making in their own space. This has a knock-on effect on the comparison and selection of controls and ultimately how the value of investments can be evaluated. In their view, this leads to information security being perceived as an opinion-based rather than evidence-based profession. One participant summarised it as follows: *"It is a very immature industry and there isn't really a proper understanding as to what should be done and how much it should cost. It's an area where there's lots of room for snake oil salesmen trying to tell you how to solve problems but in fact they themselves don't understand how"*.

Part of this is the omnipresence of uncertainty and lack of data in most areas of information security. Although risk management is expected to deal with uncertainty, the responses show that the lack of data permeates all aspects of the profession. There is uncertainty about the likelihood of an incident happening and the likely impact and resulting cost. Likewise, there is uncertainty about if, or to what extent, security controls would prevent, reduce or even notice an attack. As a consequence, security professionals are uncertain about whether their security controls work or are a sensible investment at all. Therefore, organisations resort to expert opinion. However, such expert estimations are often unreliable, either because they are biased or because they are simply too broad to provide meaningful input into decision making processes. To address this issue, participants noted that historical data might be useful to reduce uncertainty in some respects, whereas others cautioned that the fast changes in the threat landscape make historical data a poor indicator.

Principle 9: The lack of decision support processes and absence of evidence-based approaches are problematic. Uncertainty about key factors such as developments in the threat landscape, effectiveness of security controls and reliability of such data must be addressed as a priority.

5.3.4 Information security capability

This subsection discusses the core categories related to information security capabilities in organisations. Considering the environment, drivers and challenges, the information security function assesses the available inputs to create and implement risk management programmes (Mishra, 2015). Based on the interview responses, four categories related to the thought processes of practitioners when selecting a control were identified: Efficiency & Effectiveness, Likelihood & Impact, Latest Trends and Supporting Data Sources.

In section 5.3.3, the lack of data was found to be one of the major challenges. Information security practitioners reduce uncertainty by filling white spaces with data from a variety of supporting sources. At a governance level, organisations adopt benchmarks to assess gaps in their security stance, the current maturity level and the right amount of spending. Benchmarking against standards such as ISO/IEC 27001 allows them to identify areas where controls differ from the expectations of control frameworks. This provides authoritative guidance on the control areas where investments are likely to add value to an organisation. In a further step, benchmarking maturity levels across control areas provides similar guidance albeit more nuanced to adjust for sector- and organisation-specific risks.

An important part of many benchmarks is the comparison with peer organisations. Participants confirmed that peer comparison and industry best practice are vital to their investment approach. They look to peers to understand which controls contribute the most value for those environments, especially in cases of publicised breaches. The information shared by or about the impacted organisation is used as a valuable data point for risk and cost calculations. In addition, practitioners look to industry bodies, vendors, analysts and professional membership organisations for data to help them refine their programme and guide control selection towards the best value option. Cyber insurance might also be employed to estimate the value of controls, using the proxy of insurance premiums. Increasingly important components in this context are threat intelligence sharing and collaboration services (Serrano, Dandurand, & Brown, 2014; Vázquez, Acosta, Spirito, Brown, & Reid, 2012). Sources can be commercial (e.g. Digital Shadows[8]), open source (e.g. Alienvault OTX[9]), government-led (e.g. NCSC CISP[10]) and membership-based (e.g. FS-ISAC[11]) with varying goals and benefits. However, the underlying benefit is largely the same, namely to increase the visibility of security threats or trends and consequently reduce uncertainty. Practitioners use threat intelligence to evaluate the threat source, the likelihood and impact of attacks, the effectiveness of controls and future threat landscape developments.

The richest data sources may be internal security metrics. Participants frequently referred to the importance of metrics, including having defined metrics and aligning them with business goals, which is challenging in many cases. Information security professionals traditionally struggle to translate security metrics into business metrics. Interviewees suggested keeping it as simple as possible with a focus on repeatable and clear measurements. Business stakeholders are often familiar with metrics related to service availability, which makes these metrics good candidates for use. However, even simple project management metrics tracking the delivery of milestones are common. Furthermore, most of the metrics mentioned are related to security incidents or compromise scenarios. Participants discussed the absolute number of compromises/incidents, time to discovery, man-hours spent on incident resolution and the dwell time of adversaries following a breach. Other examples were related to the number of vulnerabilities in products, which can be tied to when market metrics interest business stakeholders. Participants also reported metrics to assess effectiveness, such as the percentage of prevented malware infection and proportion of blocked malware attacks.

Principle 10: Governance benchmarks, internal metrics and peer comparison data are key instruments for refining value-oriented security programmes. Collaborative threat intelligence is an increasingly important source to reduce uncertainty.

[8] https://www.digitalshadows.com/.

[9] https://www.alienvault.com/open-threat-exchange.

[10] https://www.ncsc.gov.uk/cisp.

[11] https://www.fsisac.com/.

Metrics on security control effectiveness are useful but not commonly available. Few organisations even carry out proof-of-concept or proof-of-value exercises before making an investment decision and these are often limited to assessing whether the solution is doing what the vendor claims or if it causes problems in the IT environment. This is more so a concern for organisations with a large amount of legacy technology in their environments, which may result in additional effectiveness challenges. Participants explained about the difficulty of defining meaningful key performance indicators to measure effectiveness, particularly for non-technical controls such as security awareness. Effectiveness describes how reliable the protection is, how a control works against threats and how completely it mitigates a risk or solves a problem. Considerations of efficiency focus on the service delivery of the control (i.e. how it compares with other controls in terms of the associated costs). In this context, the financial and operational preferences of the organisation play an important role. Trade-offs such as CapEx versus OpEx, buy versus build, on premises versus cloud and permanent staff versus outsourced are also considered.

Closely related to the discussion on the effectiveness of controls is the topic of the likelihood and potential impact of a successful attack. Participants pointed out the importance of understanding the likelihood and impact of an attack against organisational assets. Both factors provide valuable input into control selection from a risk management and economic perspective; however, respondents also cautioned that assessing either is difficult. In many cases, organisations use external information as described in the data sources section. However, some opinions were that such expert-driven data are too subjective, potentially biased and often too broad. Larger organisations rely on inputs from operational risk functions, which are more experienced in this space, particularly on impact figures. Smaller organisations reportedly prefer a simplified approach with the assumption that a control will effectively reduce both impact and likelihood to a negligible level upon deployment.

Principle 11: Security control effectiveness metrics are rarely available or independently gathered. Security programmes need to address this gap due to its importance for assessing the value of controls.

The purpose of controls in an information security programme is to support the wider risk management goal. Depending on the business environment, recommendations for controls range from focusing on known and proven solutions to following new and innovative approaches. In general, the control must solve the problem identified in the most effective and efficient way. Prioritising defective controls in the first instance to improve the visibility of the environment was agreed upon by participants. They also highlighted that controls with multiple benefits as well as those that provide a better experience for users are preferred. As mentioned in the challenges and constraints section, the seamless integration of security controls with user experience is a business advantage. Moreover, controls are preferred if they fit with the skillsets of current support staff. An interesting aspect is the role that trends in the security industry play. Controls that are attractive to support staff due to their innovative or novel character can have a higher priority than tried and tested controls. Highly skilled and talented employees enjoy working in a dynamic environment that provides opportunities to interact with innovative technologies. This increases work satisfaction and talent retention, thus adding value indirectly.

Principle 12: Controls that provide multiple benefits at a comparable cost enable seamless user experience, attract and retain talent and are preferred due to the value they add to an organisation overall.

5.3.5 Decisions and prioritisation

Prioritising investments is not a simple checklist exercise; it is intertwined with all the aspects and categories discussed. Information risk is not the only factor considered; business requirements weigh heavily in this decision. One of the first questions asked is how a control supports business goals. However, this is not an abstract question; it is directed to understand how suitable risk management controls affect the core assets and customer service. As discussed previously, investment drivers strongly influence this process. Legal and regulatory requirements, either current or anticipated future developments, serve as a strong prioritisation factor. Customer requirements and competitive advantage are also considered in the decision process. The weaknesses and gaps identified through benchmarking exercises, against frameworks or peers, provide further input into the process as well, while third-party involvement, through audits or penetration tests, serve as an additional input in the prioritisation process. Saving opportunities or synergies also play a role.

From a challenges perspective, practitioners look closely at the resources they have available to deliver their programme and consider what is realistically achievable. Insufficient human or financial resources may influence the controls deployed by the security function. The capacity of an organisation to absorb change influences its decisions on the timing and types of security controls. Security incidents have a special role in this context as stated by several participants. Major incidents have an immediate impact on the prioritisation of security investments. They trigger a review of previous prioritisation decisions, leading to adjustments as necessitated by the incident. In line with these prioritisation aspects, all participants described a more or less formalised decision process followed in their environment. Only one participant who followed a fully formal investment decision approach was found. This particular approach is based on the AHP technique (Saaty, 1994).

Principle 13: Security investment decisions and prioritisation are not a checklist exercise but rather a reflective cycle accounting for the weighed factors from drivers, challenges, the business environment and security capabilities to produce a value-prioritised control selection.

5.3.6 Corporate finance considerations

As with any other investment, information security investments must follow the rules of corporate finance. Information security practitioners are aware of the accounting preferences in their organisations and consider financial aspects (e.g. CapEx, OpEx, cash flow) in their decisions. However, financial formulas are rarely used to justify investment. In nearly all cases, participants reported that they were not expected to use valuation or performance models such as ROI, NPV and IRR, or any other similar model. In those cases where it was requested, the process tended to be sidestepped by relying on more mature risk departments to help with the expected justification. Indeed, the numbers might even be ‘massaged’ to meet an imposed hurdle rate. This is relatively easy as the translation of security metrics into financial variables leaves plenty of room for interpretation.

Practitioners do not feel that they have sufficient reliable data to make formal investment calculations and finance departments have little incentive to question such numbers based on security details. The result is a fixed budget compromise based on trust in the experience of the security practitioner. Information security departments can then freely decide how to spend the money allocated to them. As long as there is no overspending, the finance department requires no further justification. For further budget requirements or in cases where additional justification is needed, participants apply a business case approach, notably when a specific business project or business problem is addressed. For instance, a large contract requires enhanced security controls to retain the customer’s business. In these situations, the value calculation becomes considerably easier as the cost (loss of contract, cost of security controls) and the benefit (future revenue) are readily available. However, this is not an ROI calculation for the security control, but rather for a complete customer solution. Security is only an enabling factor to the whole package. Nonetheless, how much the security control contributes to the overall business value remains difficult to calculate.

Participants expressed the importance that security practitioners are respected and trusted in their role. It is assumed that because of the many unknowns and lack of reliable data, business decision makers question whether they trust the practitioner to do the right thing, rather than asking whether it is a beneficial investment. However, this does not mean that there is no scrutiny on how money is invested and participants anticipate that the scrutiny of security investment decisions will increase considerably in the future. One participant likened the development to that previously seen with IT: *"I think we will see increased scrutiny on the efficiency side just the way the IT programme has. Years ago, whatever the IT people needed, you gave them. Once we started to understand IT was not magic and it needed to show business value, that began the change and I definitely see that happening in security as well".*

Similarly, some participants explained that, in their opinions, too many security investments were considered to be a failure, as they did not deliver what the project set out to accomplish. Especially where large sums are invested in security controls that failed to prevent widely publicised breaches the question as to what the value of those investments is to the organisation is raised. Considering this, participants reported that there are already signs of organisations not wanting to continue spending big on information security. Instead, they try to figure out the minimum amount that they can get away with. This trend is mitigated by the requirements imposed through existing and incoming legislation and regulation exercising libertarian paternalism (Thaler & Sunstein, 2003); In this context, participants refer to the EU General Data Protection Regulation, Directive on Security of Network and Information Systems and PCI/DSS in particular.

Principle 14: Financial valuation or performance models are rarely used to justify security investments. With increasing scrutiny on security spending, practitioners must adopt an economic value approach or be relegated to a compliance and audit function.

5.3.7 Measure value

The primary focus of participants is managing and measuring information security risk in their organisation. The categories discussed provide fundamental input towards achieving that goal. The basic input variables are the business environment, especially the resulting risk profile for a sector or organisation, drivers, challenges and risk tolerance set by senior management. Accordingly, success is measured in a variety of ways ranging from how well risks are identified, including typical components such as threat actor, threat likelihood, potential impact, weaknesses and gaps, to how complete an identified risk is mitigated. In cases where security incidents are a driver, time becomes an additional metric as practitioners try to gain control over the situation as swiftly as possible. In most cases, the measurement of choice is qualitative risk assessments, ideally based on established methodologies. However, participants pointed out that qualitative risk assessments are subjective and may lack reproducibility of outcomes. To support their efforts, information security professionals cooperate with other experienced risk functions such as operational risk. These functions can provide highly relevant business data for risk models on exposure, impact and risk clustering. Most participants adopt risk reduction metrics to measure the value of information security programmes. However, measuring the outcomes or value of 'soft' security controls such as security awareness training compared with technical controls is more difficult. Both these points may explain the tendency to deploy technical controls (which are easier to measure) over educational controls (which are often seen as more effective). While the primary focus is to manage and measure information security risk, practitioners do work with related metrics such as reducing regulatory audit findings, tracking the progression of security projects and reducing the incident scope and effectiveness of technical controls to track success and measure value along the way. Some organisations use the reduction in insurance premiums to measure the value of their security controls. One participant pointed out instances where value could be measured by linking government incentives to security programmes as an additional value aspect. However, more commonly, value is measured by understanding risk reduction in a qualitative manner. Consequently, limited evidence of security investments being evaluated for value from a financial perspective was found.

Principle 15: Practitioners use all available inputs as described in the previous principles to manage information security risks in an organisation. This primary *focus is complemented by a constant measurement cycle of success and value, often pegged to the risk tolerance levels set by senior management.*

5.4 Relationship between categories

Figure 32 illustrates the relations between these categories (represented by the thickness of the edges) through a network graph where the categories are presented as nodes scaled by their prominence in our interviews. Edge thickness indicates how connected categories were in the responses of our participants. In particular, we observe strong edges in the result categories (*manage risk* [C18], *measure value* [C19]) and the filter/control categories (*corporate finance considerations* [C8], *decision & prioritisation* [C11]). This fits well with our security investment mind map (Figure 30) that shows which information flows towards these categories. In the business environment context, *business culture and politics* [C2] influences *decisions and prioritisation* as well as the *cost of security* [C9]. *Business strategy and goals* [C3] likewise influence *decision and prioritisation* but also play a key role in *corporate finance considerations* and *security control* [C22] selection. Interestingly, the categories we consider to be drivers show fewer 'thick' edges but are well connected overall. This is especially true for the *threat landscape* [C28], which is connected to the majority of nodes with some notable relation to *security controls*, *efficiency & effectiveness* [C12] and *risk frameworks* [C20]. This finding indicates the importance of this category for the value assessment of security investments. Similarly, we find *legal and regulatory* [C16] to be well connected with a particular strong edge towards the *measure value* category. Further, the *cost of security* dominates the challenges aspect with the expected strong ties to *corporate finance considerations* and *decision & prioritisation*. The thick edge to *manage risk* is a reminder of practitioners' stance on cost-effective risk management practices.

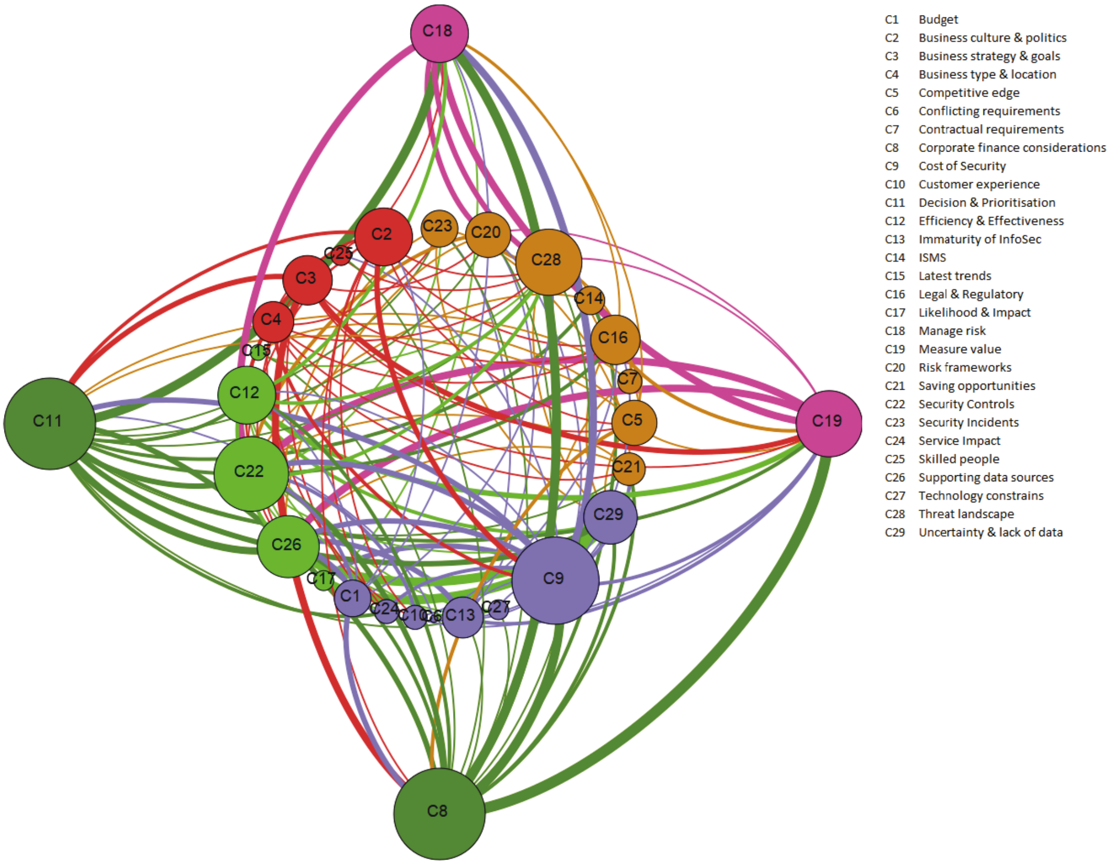


Figure 32 - Overview of the category relationship network

Another key category under challenges is *uncertainty & lack of data* [C29], which shows strong relations with *likelihood & impact* [C17] as well as *supporting data sources* [C26]. As reported previously, uncertainty is a constant underlying concern in the decision process for practitioners; the network graph highlights that this challenge is especially prominent in the context of *likelihood & impact*. We can conclude that improvements in this area would bring about considerable benefits in the evaluation process. This is further evidenced by the central role *supporting data sources* play in this context. It shows strong edges with several key decision and metric-related categories, most notably *efficiency and effectiveness*, *corporate finance*, *decision and prioritisation* and *immaturity of information security* [C13].

Turning our focus to the information security capability categories, it is of little surprise that *security controls* take centre stage. This category is strongly represented as well as widely connected. As security controls are goal-driven in this context, the strong connection to *manage risk* and *measure value* is expected. However, we also note the several thick edges towards finance-related categories (*budget, cost of security, corporate finance considerations*) as well as driving factors such as the *threat landscape*, *risk frameworks* and *customer requirements*. If we can assume that security controls are the channel through which information security risk management goals are met in an organisation, the described relationship network helps us further map a priority landscape for investment evaluations and value discussions.

By analysing the relationships of *decision and prioritisation*, we find that the business environment categories as well as compliance drivers (*legal and regulatory* [C16], *information security management systems* [14]) weigh heavy with practitioners. Together with challenges on *costs*, *lack of data* and *service impact* [C24], they form part of the *security controls* selection process that aims to *manage risk* as evidenced by the strong edge between the categories. The *corporate finance considerations* category is similar in this aspect but shows a stronger relationship with metrics and value-related areas (*budget, cost of security, business strategy, measure value*). Lastly, the *measure value* category is well connected, indicating that our participants discussed value measures in a range of contexts. However, several stronger edges point to categories of particular interest. As discussed previously, *managing risk* [C18], which is often expressed in the context of *business strategy and goals*, is highly relevant for security value discussions. The *cost of security* and *corporate finance considerations* likewise have a direct impact on the value *security controls* provide to an organisation. In this context, we also found that *customer experience–efficiency and effectiveness* is an important relationship to consider. In line with our detailed qualitative analysis in section 5.3, the network graph also points towards *legal and regulatory*, *competitive edge*, *threat landscape* and *risk frameworks* as key categories for measuring the value of information security investments.

5.5 Study limitations and challenges to validity

As with any qualitative study, these results depend on the perspective of the data taken by the researcher, experience from which conclusions are drawn and underlying information gathered in the field. There is no single true category or interpretation to be discovered, but rather as many ways of seeing the data as one can invent (Dey, 2003). Consequently, the results reflect the uniqueness of the research data and situation of each contributing participant. To ensure the validity of the findings, great care was taken with the research methodology, as described in section 5.2. Although the primary data pool of 18 participants does not make for the largest study, the information gathered was found to be rich and approaching saturation quickly due to the niche topic. Furthermore, the study was limited by geographic representation, as its focus was on western businesses, particularly those in the United States and United Kingdom. The findings presented in this chapter are thus a generalised conclusion valid in the context of the qualitative analysis. No claim of correctness outside of this can be made; however, the theoretical fundament for further research to verify and extend the findings has been set. On this basis, the next chapter aims to verify and extend the results by adopting quantitative methodologies.

5.6 Chapter summary

By following a Grounded Theory approach to analyse the semi-structured interviews conducted with information security practitioners, we identified several key categories considered when evaluating security investments and the value of information security programmes. Building on the qualitative analysis of the interviews, an axial coding approach was used to identify the major categories in the data. Through this deconstruction and reassembly process, a clearer understanding of the practitioner's mind map on this topic was obtained, allowing the researchers to construct a schematic overview of the security investment evaluation approach. We present a simplified but highly relevant framework of the organisational context in which investment decisions for information security are made in a professional environment. We found that information security investments follow a decision support process initiated by 'driving factors' and adjusted by 'challenges and constraints'. Based on these driving factors and challenges, professionals select an appropriate security capability, which is then refined through corporate decision filters. We established that the main purpose of our participants' information security programme is to add value to the organisation, commonly in the form of managed risk. Our framework highlights that this process is heavily influenced by the underlying business environment that defines what value means to a certain organisation. In addition, the detailed analysis was condensed into 15 principles aligned with the proposed evaluation framework, providing an indication of the importance of each area. The research provides extended insights into the evaluation processes of security investments in the context of organisational value frameworks by practitioners. Security practitioners rarely apply accounting performance metrics such as NPV, ROI and IRR. Rather, investments tend to be allocated through means of annually assigned budgets attached to risk-based performance metrics without further hurdle rate requirements. Notable exceptions to this practice where ad hoc requirements arise from incidents or specific business demands were found. In such situations, security investments were evaluated by using a business case approach focused on the value added. In general, decisions on security investments are made in the context of a highly complex organisational system relying on a range of unique business environment factors (section 5.3.1) closely resembling a multicriteria decision approach. These investments are not viewed as an isolated activity but as intertwined with wider business requirements, challenges and drivers to deliver value in this context. Business environment-related factors, particularly the information security function's strategy, goals and culture, deliver considerable value to an organisation. We highlighted several drivers and challenges that practitioners take into consideration when handling this topic. In particular, several key drivers (*threat landscape*, *legal and regulatory*, *risk frameworks*) and challenges (*cost of security*, *uncertainty*, *lack of data*) were found to be a crucial part of security investment strategies.

The analysis presented on this topic offers several distinct benefits:

- It serves as a baseline to practitioners to create or improve their approach to assess the value of information security in organisations. In addition, it serves academics by offering real-world data on the key factors in this context.
- It allows those organisations that have reached a higher maturity level to critically review their current processes against the findings in this study, taking special note of the identified principles.
- It provides a common ground for discourse among the professionals involved in security investment decision making to better understand the drivers, challenges and priorities in this context.
- It provides input on current developments in security value measurement to inform information security governance bodies.

Building on this, we combine the findings of this detailed qualitative analysis with the key concepts extracted from chapter 2 to verify the key factors quantitatively (chapter 7). By utilising a survey instrument, the factors in the investment decision process are evaluated for latent constructs and confirmed as structural models based on the framework constructed in this chapter.

Following on from the challenges of threat landscape uncertainty highlighted both in chapter 2 and in this chapter, we investigate that problem space more closely next. Chapter 6 describes a way in which to utilise external subject matter expertise to reduce uncertainty in future information security threat developments. While this does not address the large area of uncertainty in information security in its entirety, it does investigate one of the most common challenges faced by practitioners when making strategic decisions.

6 ANTICIPATING DEVELOPMENTS IN THREAT LANDSCAPES

Rapid changes in security threat landscapes cause uncertainty for IT operations and security professionals and may force changes to organisations' security strategy. Data that help reduce ambiguity or even predict future developments in this regard can thus be of considerable value. In this chapter, we describe a methodology and tool to achieve a reduction in uncertainty related to threat developments. We illustrate how this has been successfully applied and verified for one particular year. Based on over 200 security predictions published in 2015, we use a topic modelling approach to identify 17 underlying predicted threat developments. To verify the extent to which these predicted threat topics were realized throughout 2016, we solicited backward looking opinions from respondents with varying experience of IT and information security in a survey at the start of 2017. In addition, we reviewed secondary sources to corroborate the survey results. Based on the presented findings, we conclude that the security predictions made in 2015 for 2016 did foresee notable developments in that year. The identified latent predictions were related to hacking political campaigns, large-scale data breaches of personal data and health records, increasing threats from various types of malware, specifically ransomware, and large-scale DDoS attacks. The findings of this chapter are relevant as they can be applied as an approach to improve the effectiveness of organisations' information security strategy. The approach allows practitioners to repeat this exercise themselves on an annual basis to gain the then latest prediction output as decision support input for their information security strategy.

Information security challenges have received greater priority from the media, organisations and governments in recent years (HM Government, 2016; The White House, 2015; World Economic Forum, 2015). Yet, despite the increased focus on this area, breach notifications and new threats continue to cause considerable economic (Chandler, 2016) and socio-political (Crabtree, 2017) impacts. Advances in technical security controls and an increasingly paternalistic stance by regulators and governments in the context of information security standards are forcing cyber criminals to become innovative. This in turn is causing rapid advances in threat landscape developments, leaving security professionals uncertain as to how this should be reflected in their security strategies. Managing risks in such an uncertain setting is challenging, and thus inputs that help reduce ambiguity or even predict future developments can be of immediate economic value.

6.1 Related work

An increasing body of research across multiple domains is developing around the advantages and disadvantages of predictions and forecasts (Armstrong, 1980; Armstrong, Green, & Graefe, 2015; Denrell & Fang, 2010; Leoni, 2008). Indeed, views on the general value of forecasting range from critical to cynical (Dubner, 2011; Harford, 2016). Hence, the cyber security predictions published annually by security vendors, strategy-minded practitioners, industry bodies and laypeople should be considered with a critical thinking and bias consciousness mindset (Kallus, 2014). This is especially true when data from multiple expert forecasters have been combined to improve their results (Ungar, Mellers, Satopää, Tetlock, & Baron, 2012). However, although some predictions are simply marketing noise aiming to garner attention, the majority are made by subject matter experts with vast experience in this area. Hence, such predictions should be considered to be useful information rather than simply marketing if they are read with a critical thinking and bias consciousness mindset.

Researchers have begun to propose innovative ways in which to address uncertainty in the information security industry. Pandey and Snekkenes (2014) examine the applicability of a prediction market approach for forecasting and assessing information security events. While they conclude that prediction markets can estimate long-term threats efficiently and effectively, they concede that further research on the design of such information security prediction markets is needed. Y. Liu et al. (2015) investigate the feasibility of forecasting security breaches based on the externally observable properties of organisations' networks, relying on technical measures to assess the likelihood of breach attempts affecting single organisations. Bagchi and Udo (2003) use a modified Gompertz model to forecast increases in known threat vectors based on the sparse data collected on previous incidents. They establish a growth pattern linking the use of certain technologies to an increase in associated cyber crimes, finding that the proposed model is adequate for short-term predictions in some cases. Based on their Early Model Based Event Recognition using Surrogates (EMBERS), Ramakrishnan et al. (2014) use open source indicators such as tweets, news sources and blogs to predict civil unrest. Their research confirms the capability to forecast significant societal happenings following the described approach, as verified by an independent expert group.

In the next sections, we examine the published security predictions for 2016 collected from public sources from October 2015 to January 2016. We provide a high-level overview of the underlying themes based on a manual categorisation approach and analyse the prediction pool by utilising co-occurrence networks and topic modelling with latent Dirichlet allocation (LDA) (Blei, Ng, & Jordan, 2003).

6.2 Overview of security predictions 2016

The data on security predictions were collected through Internet search alerts, a manual review of press releases, vendor notifications and revisiting sources from previous years. Only those predictions considered to be relevant were included; relevance was defined as 'informed opinions or assumptions on developments in the information security threat landscape throughout 2016 expressed as forecast or prediction'. Data collection was conducted on a best effort basis and we do not claim complete coverage. However, our prediction dataset covers an exhaustive 238 individual predictions from 41 sources.

In the first step of the analysis, we distinguished between predictions discussing an expected change in the security threat landscape (e.g. "Increased targeting of Apple devices by cyber criminals") and those that provide general opinions on developments in the information security industry (e.g. "More Chief Information Security Officers will be hired"). For this research. we focused on security threat predictions rather than general developments. This reduced the dataset to 187 predictions. The next step was to categorise each prediction to align it with one of the 15 categories. These 15 high-level categories were originally defined in 2013 by a working group of security professionals in the finance industry based on predictions made at that time and carried forward for consistency. As with any categorisation attempt, the problem of defining too few or too many categories is a valid topic of discussion. We provide an alternative view on this in a later section. Figure 33 provides an overview of the categories and their popularity in terms of the 2016 predictions, showing topical areas and noticeable developments expected in the security threat landscape in that year according to our sources.

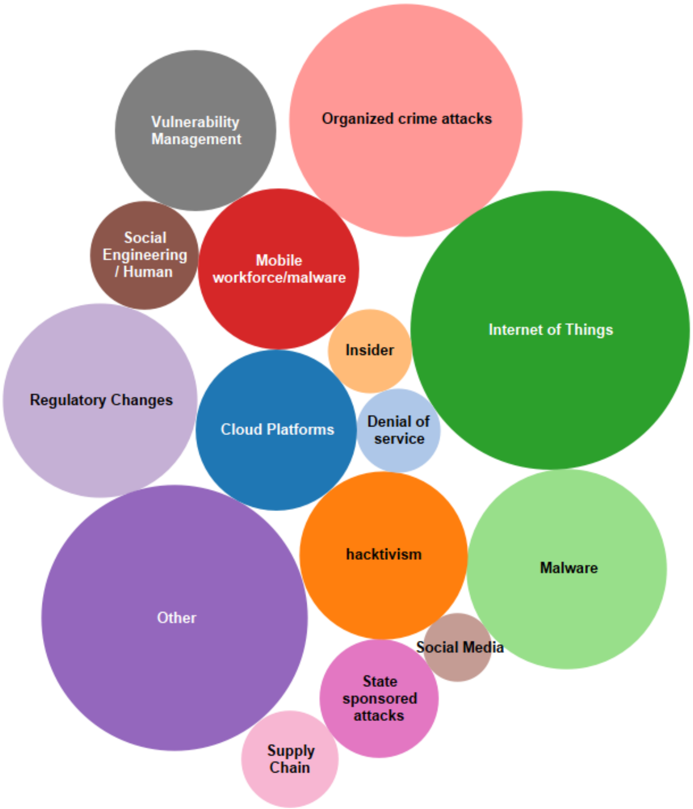


Figure 33 - Popularity of security predictions in 2016 by category

Although this figure already provides us with an intuition as to the direction in which threats may develop in the future, it is important to consider the source of these predictions. Armstrong et al. (2015) advise that good results can be achieved by combining forecasts from eight to 12 experts whose knowledge of the problem is diverse and whose biases are likely to differ. Hence, it is crucial to investigate if these categories are supported by multiple predictions made by only one vendor or if broader consensus from multiple sources exists. Figure 34 shows a detailed breakdown of the prediction distribution by vendor, highlighting that threat developments in the category “Internet of Things” are a widespread concern across most sources. Likewise, only one source is driving concerns in the “Denial of Service” category. However, the predictions for 2016 appear to be a balanced distribution across categories and sources in general.

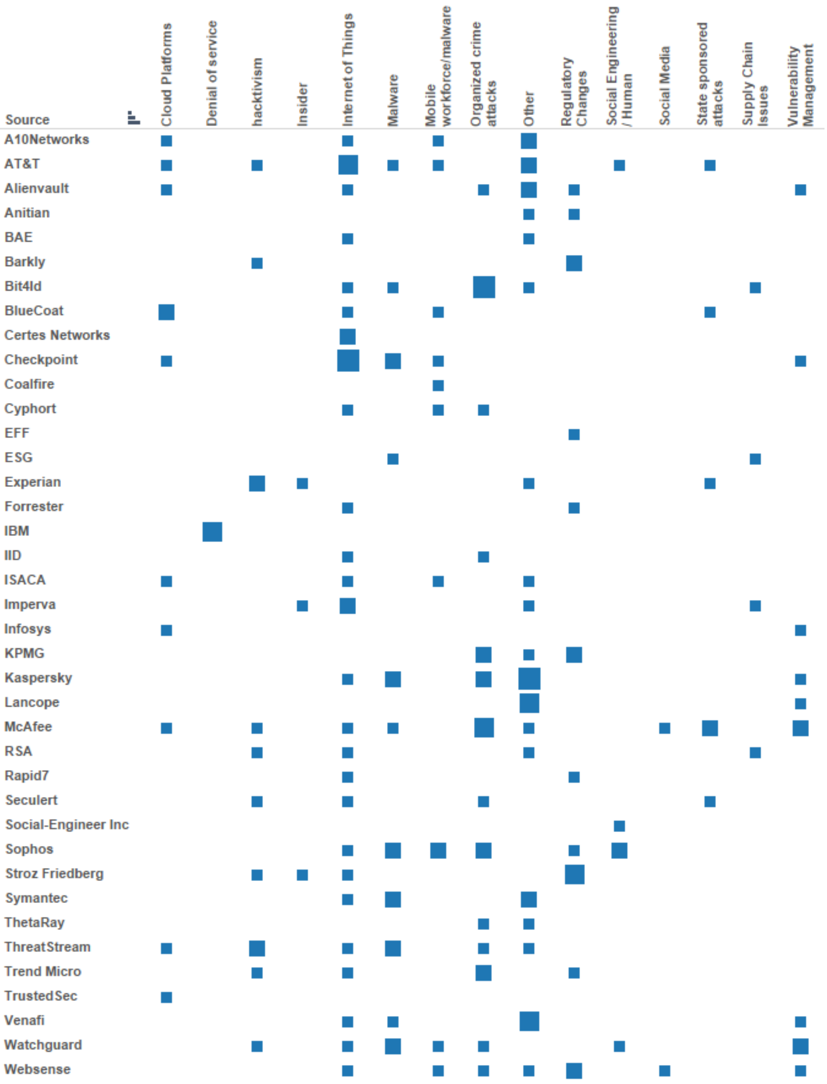


Figure 34 - Matrix of the 2016 predictions by vendor

The analysis of the 2016 predictions allows us to deduce that our sources indicate noticeable developments, particularly in the areas of “Internet of Things”, “Organised Crime Attacks” and “Malware”. However, how does this compare with the previous year? Figure 35 compares the predictions from 2014, 2015 and 2016 to understand the development trends over time.

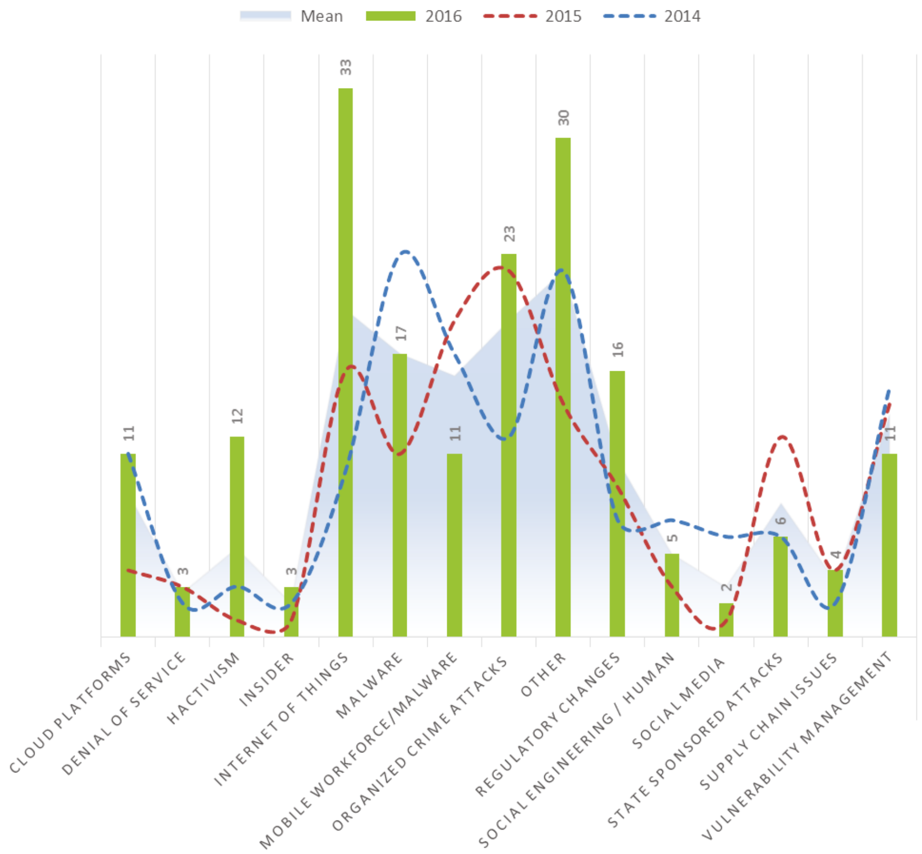


Figure 35 - Comparison of prediction categories over time

This simple visualisation indicates where new threat developments are expected. According to our sources, we should expect relatively stable threat development (as measured by the average prediction count) in the areas of “Denial of Service”, “Insider”, “Malware”, “Organised Crime Attacks”, “Social Engineering and Human Aspects”, “Social Media”, “State-sponsored Attacks”, “Supply Chain Issues” and “Vulnerability Management”. Surprisingly, we also note a drop in predictions for all things related to “Mobile Workforce and Malware”. By contrast, “Hactivism”, “Internet of Things” and “Regulatory Changes” are strong emerging areas of concern.

While most of these findings make intuitive sense to information security practitioners, certain factors may impact the validity of our findings. In addition to the potential shortcomings in the data collection process, the inclusion of additional predictions may result in a different predicted threat landscape. However, we believe the dataset to be sufficiently representative and balanced to provide a useful overview. An additional issue lies with the sources themselves; few, if any, of the predictions are made following rigid processes (Armstrong et al., 2015) and will be vulnerable to bandwagon or current event bias. Lastly, there is the issue of categorisation. Aligning individual predictions with a predefined category is rarely straightforward either, as sources may cover various aspects in one distinct prediction. Consequently, we are forced to apply a subjective ‘best fit’ approach. Recognising these challenges, we investigate an alternative view on the dataset that is largely unbiased but requires more effort to interpret the result. In the next section, we review the prediction dataset by applying text analysis approaches.

6.3 Prediction text analysis

In the first step, we define the key terms in our prediction dataset. “R” software provides a useful platform for this, as we can import our dataset and use the text mining module *tm_map* (Meyer et al., 2008). We apply corpus preparation tasks (remove punctuation, strip whitespaces, convert to lower case and remove stop words) except stemming (Porter, 1997) and create a (sparse) DTM. This allows us to calculate a correlation matrix for the key terms across the definition dataset (Figure 36). We can see that some relations are forming, such as Internet/devices, business/information/data/target and attackers/malware.

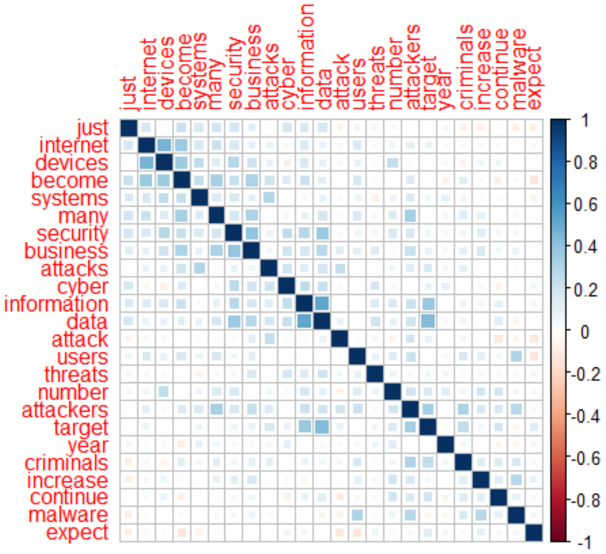


Figure 36 - Correlation plot of the key prediction terms

While this figure provides some basic insights, it is a rather limited view that does not lend itself to drawing deep conclusions about the underlying context. To gain a more meaningful view of the contextual relationships in our dataset, we used co-occurrence network analysis (Higuchi, 2015; Rice & Danowski, 1993). In textual analysis, co-occurrence networks show words with similar appearance patterns and thus high degrees of co-occurrence. The approach is based on the idea that a word's meaning is related to the concepts to which it is connected. It also has the benefit that no coder bias is introduced other than to determine which words are examined (Ryan & Bernard, 2003). However, network graphs can become too crowded unless sensible restrictions are applied. By filtering out terms with a frequency below 15 when producing the co-occurrence network graph, we reduced the information presented while preserving the important context.

Figure 37 presents a headline view of the important underlying concepts inherent to the words used in the prediction set. In addition to the minimum spanning tree, we added community detection to further emphasise the connected components. The node size illustrates the term frequency and detected communities are highlighted in different colours. Based on the dataset, we found that the 'random walk' or 'walktrap' algorithm (Pons & Latapy, 2005) provided the subjectively best community detection approach. Combined with minimum spanning tree, this explains not only the key concepts but also how words are grouped into communities.

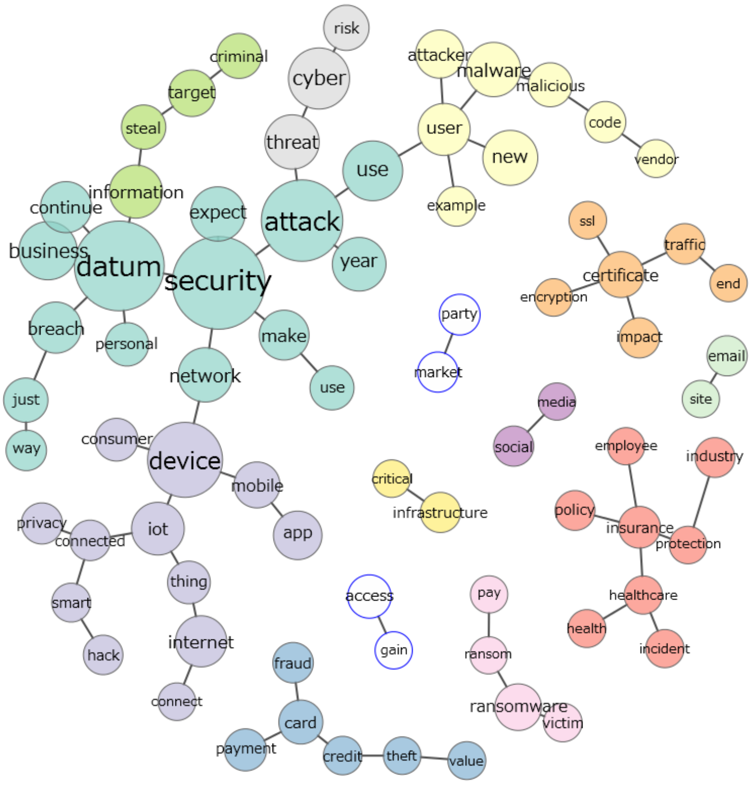


Figure 37 - Community-enhanced network graph of the 2016 security predictions

Looking at the randomly coloured communities, we see surprisingly coherent topics forming. Some are close to our manual approach such as “Internet of Things” (purple), “Ransomware” (pink) and “General Organised Crime” (green). However, we also note additional topics of interest not as obvious previously; our prediction sources highlight areas of concern with healthcare incidents and industry insurance policies (red), social media (dark purple), transport layer encryption (orange) and malicious vendor code (yellow). Despite this improved understanding of predicted developments in the 2016 threat landscape, an unbiased identification of all the underlying topics inherent to our dataset would be ideal. One of the ways in which to do this is to use topic models. For this research, we therefore utilise LDA, as described by Blei et al. (2003), to find our ‘latent’ prediction topics. Figure 38 summarises the approach adopted.

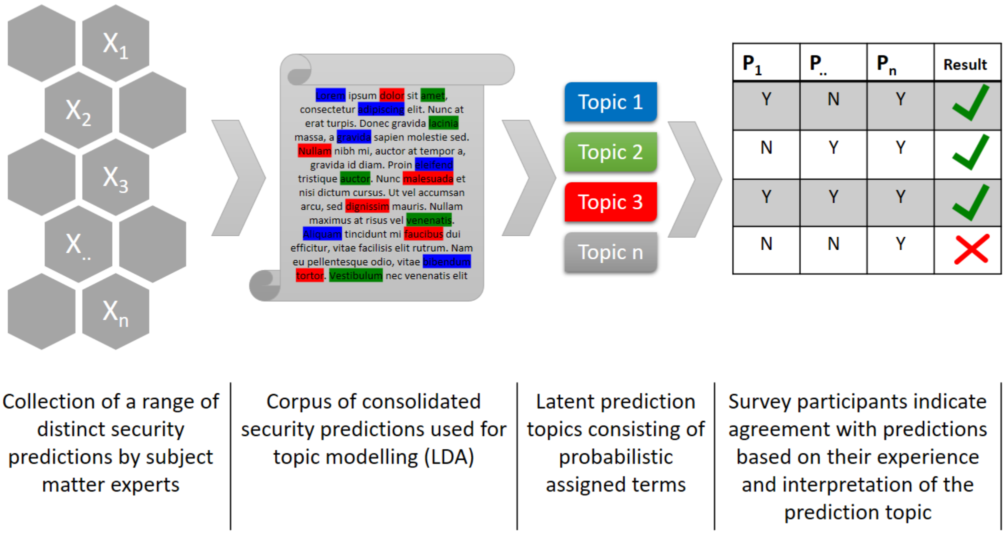

X_1
X_2
X_3
$X_{..}$
X_n
Topic 1
Topic 2
Topic 3
Topic n
P_1
$P_{..}$
P_n
Result
Y N Y ✓
N Y Y ✓
Y Y Y ✓
N N Y ✗
Collection of a range of distinct security predictions by subject matter experts
Corpus of consolidated security predictions used for topic modelling (LDA)
Latent prediction topics consisting of probabilistic assigned terms
Survey participants indicate agreement with predictions based on their experience and interpretation of the prediction topic

Figure 38 - Overview of the study approach

To understand the number of topics in our dataset, we utilised the harmonic mean approach (Ponweiser, 2012), which identified 17 topics to be the optimum. Hence, our manual categorisation approach with 15 topics was reasonable. Table 24 shows a sample of the LDA output for all 17 topics with the first six words associated with each topic. As this is an automated approach, not every topic makes immediate sense; nonetheless, the headlines paint a surprisingly clear picture, especially regarding Internet of Things, insurance risks, hackers targeting social campaigns and card payment issues.

Id	**Term 1**	**Term 2**	**Term 3**	**Term 4**	**Term 5**	**Term 6**
1	Organisation	Cyber	Security	Insurance	Risk	Policy
2	Device	Iot	Connect	Consumer	Smart	However
3	Data	Information	Breach	Personal	Steal	Health
4	Campaign	Hacker	Email	Online	Social	News
5	Apps	Vulnerability	Number	App	Apple	Android
6	Card	Payment	Attacker	Fraud	Credit	Process
7	Security	Cloud	Network	Party	Application	Access
8	Large	Next	Become	Protect	Offer	Start
9	Certificate	Traffic	Encrypt	SSL	Trust	Impact
10	Business	Base	Shift	Approach	Protection	Activity
11	Malware	Threat	Time	Opportunity	Actor	Common
12	Attack	System	Threat	Compromise	Predict	DDOS
13	Internet	Continue	Change	Provide	Another	Exploit
14	Ransomware	Target	Criminal	Ransom	Hacktivist	Engineering
15	Year	Expect	Result	High	Researcher	Global
16	Require	Victim	System	Enterprise	Software	Support
17	Increase	Cyber security	Find	Management	Government	Place

Table 24 - Security prediction topics identified by LDA

Uncertainty in threat developments is one of the largest challenges for security practitioners as we found in chapter 5. The options for anticipating potentially critical changes in the threat landscape that may impact security strategy are limited; yet, predictions about these developments tend to be discarded as marketing noise. In this section, we investigate how security professionals can use such data to reduce uncertainty and refine their security strategies. We showed possible approaches for conducting such an exercise with the example of an exhaustive collection of security predictions for 2016. We also illustrated how even a simple manual categorisation can lead to quick and useful results. Utilising more advanced text analysis and topic modelling approaches provided deeper insights into the heart of security predictions.

Understanding what was predicted to happen and knowing whether such predictions were realised are different things. Hence, we applied a questionnaire-based approach a year after the predictions were originally published to evaluate the validity of the threat topics predicted as well as reviewed secondary sources. This survey collected ex-post data on security threat developments in 2016 from respondents with varying expertise. Participants responded during February 2017 to ensure that developments in 2016 were still present in their minds, thereby reducing the temporal distance effects (Day & Bartels, 2008). For survey participant recruitment, we followed a cluster sampling approach, soliciting responses from professional networks in the information security field as well as online through Amazon Mechanical Turk. This approach was suitable for our study, as Behrend, Sharek, Meade, and Wiebe (2011) conclude that a crowdsourcing sample behaves similarly to participants from a traditional psychology participant pool. Particular attention was paid to the task design and remuneration offered, to ensure microworking tasks are meaningful and microworkers are sufficiently engaged (B. Liu & Sundar, 2018; Paolacci & Chandler, 2014). To ensure the validity and reliability of the survey content, we enlisted the help of an experienced survey designer. In addition, we ran short test surveys to gather feedback. The focus of this pretesting was to confirm that the questions were easy to understand and instructions clear as well as to solicit feedback on the survey flow and response options. Following this, we ran a pilot study with selected participants including both cyber security experts and laypeople. For this pilot study, we selected known participants to ensure feedback was open and direct as well as considered in the context of the cyber security skill level. This helped us identify any remaining issues the main study would encounter and ensure the reliability of the results.

For the survey, the 17 topics were transformed into ordinal questions to be rated by participants on a five-point Likert-type scale (strongly disagree, disagree, neutral, agree, strongly agree). In addition, we added a categorical question for participants to rate their familiarity with information security. The topic output was presented in raw form as obtained from the LDA analysis (Figure 39) to minimise the potential influence of the research team on participants' interpretation of the topic. However, based on feedback from pretesting, an interpretation was provided only for the first topic as an example. Following an introduction to the research, we stated the purpose of the survey and provided instructions for its completion. Participants were then asked to review a ranked list of words relevant to a security prediction topic. Based on feedback, additional guidance was provided to clarify that those terms higher in the list were more relevant to the particular topic. It was also explained that the red bar signifies the relevance of the terms for this particular topic, whereas the blue bar expresses the overall relevance of the term in the context of the survey. For the list of terms in the first question (Figure 39), we added a sample interpretation as suggested by participants in the trial survey:

> *"This topic could be interpreted as a notable prediction in 2016 for organisations to use cyber security insurance to manage their risks. Considering the list of words, do you agree or disagree that this was a notable development in 2016?"*

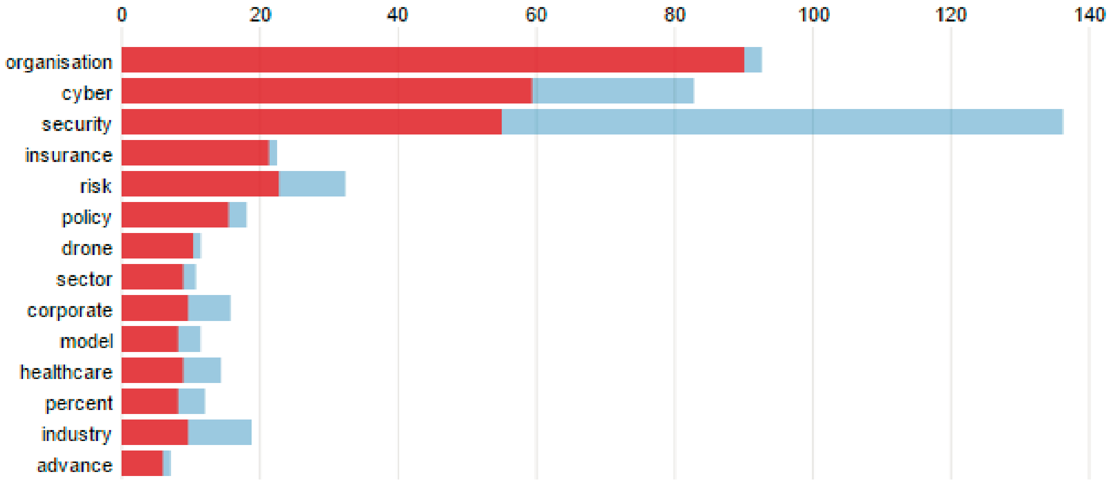


Figure 39 - Example of the presentation of a topic in the survey

To present the questions in this form, we used LDAvis (Sievert & Shirley, 2014) to visualise the topic. Figure 39 illustrates how the topic model output was presented, showing the key terms as well as their frequency within the topic (red) and across all topics (blue). High-ranked terms such as 'organisation', 'cyber', 'risk' and 'insurance' highlight the relevant threat developments for 2016 expected by participants. This approach identifies a genuinely informative structure in the underlying data and produces topics that connect with our intuitive understanding of the semantic content. Topics are typically interpretable and can be useful in many applications (Steyvers & Griffiths, 2007). Finally, all survey responses were reviewed and responses with irregular response patterns or failed attention checks were removed.

6.4 Survey analysis

We divided the sample of 134 participants into four subgroups based on their experience of cyber security: no experience, novice, intermediate and expert (Table 25). Most participants self-rated themselves as cyber security novices (61%), while only 5% stated that they had no experience of the topic. In summary, 95% of participants had some experience of cyber security.

Experience	Number	Percentage
No experience	7	5.2
Novice	82	61.2
Intermediate	31	23.1
Expert	14	10.5
Total	134	100

Table 25 - Participant distribution by experience

Topic	Mean	Median	Mode	SD
Topic 1	3.791	4	4	0.893
Topic 2	3.366	3	4	1.052
Topic 3	4.030	4	4	0.941
Topic 4	4.187	4	5	0.982
Topic 5	3.582	4	4	0.895
Topic 6	3.813	4	4	0.997
Topic 7	3.515	4	4	1.095
Topic 8	2.418	2	2	0.983
Topic 9	3.694	4	4	0.860
Topic 10	2.515	2	2	1.122
Topic 11	3.940	4	4	0.964
Topic 12	3.910	4	4	1.072
Topic 13	3.261	3	4	1.025
Topic 14	3.970	4	4	0.933
Topic 15	2.813	3	2	1.209
Topic 16	2.709	3	3	0.932
Topic 17	3.799	4	4	0.899

Table 26 - Average sample responses for each topic

The descriptive statistics in Table 26 show that participants agreed (rating of 4) with most of the presented predictions, with a limited number being rated as neutral (3) or disagree (2). Based on the mean agreement with a topic, Topic 4, Topic 3, Topic 14 and Topic 11 - in that order - received the highest scores (i.e. showed the highest agreement with the prediction coming to pass in 2016), whereas Topic 15, Topic 16, Topic 10 and Topic 8 received the lowest scores. By subgroup, Topic 4 received the highest scores across all groups (excluding the smallest subgroup of 'no experience') with similar results for Topics 3 and 11 (Table 27). Topics 10, 8, 15 and 16 received the lowest scores across all groups with the exception of Topic 3 for the 'no experience' subgroup.

Rank	**Total sample**	**No experience**	**Novice**	**Intermediate**	**Expert**
1	Topic 4	Topic 11	Topic 4	Topic 4	Topic 4
2	Topic 3	Topic 1	Topic 3	Topic 12	Topic 11
3	Topic 14	Topic 17	Topic 14	Topic 3	Topic 3
4	Topic 11	Topic 12	Topic 11	Topic 14	Topic 1
5	Topic 12	Topic 4	Topic 6	Topic 17	Topic 9
6	Topic 6	Topic 7	Topic 1	Topic 9	Topic 14
7	Topic 17	Topic 14	Topic 12	Topic 11	Topic 6
8	Topic 1	Topic 2	Topic 17	Topic 6	Topic 7
9	Topic 9	Topic 5	Topic 9	Topic 1	Topic 12
10	Topic 5	Topic 6	Topic 5	Topic 5	Topic 17
11	Topic 7	Topic 9	Topic 7	Topic 13	Topic 5
12	Topic 2	Topic 16	Topic 2	Topic 7	Topic 2
13	Topic 13	Topic 13	Topic 13	Topic 2	Topic 13
14	Topic 15	Topic 15	Topic 15	Topic 16	Topic 15
15	Topic 16	Topic 3	Topic 16	Topic 15	Topic 16
16	Topic 10	Topic 10	Topic 10	Topic 10	Topic 8
17	Topic 8	Topic 8	Topic 8	Topic 8	Topic 10

Table 27 - Topics ranked by subgroup (from highest to lowest)

As expected, we found corresponding patterns when visualising the responses by subgroup and topic, including the shift left for Topic 3 in the ‘no experience’ subgroup (Figure 40).

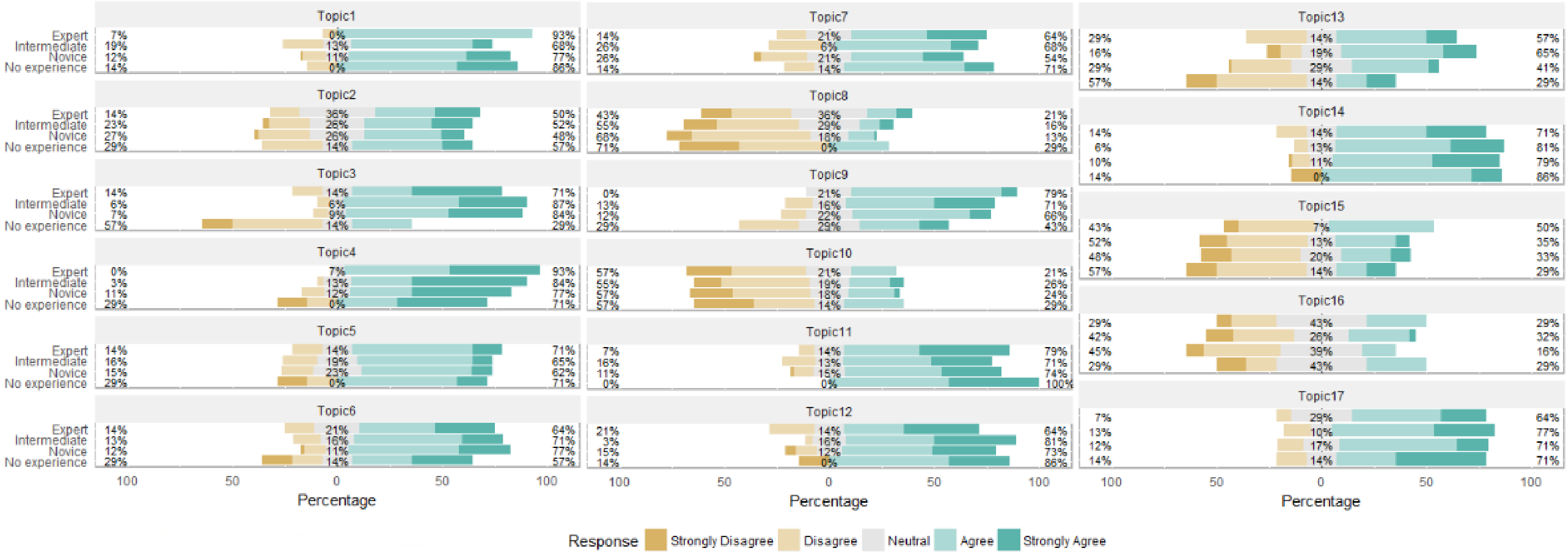


Figure 40 - Response distribution by subgroup and topic

To better understand the relevance of the differences in the results, we tested for normality and statistical significance. We used Shapiro–Wilk tests to assess the normality of the data throughout the sample. The results showed that the *p*-values are below 0.05, allowing us to conclude that the data distribution is non-normal. As a consequence, we used non-parametric tests for further analysis, namely Mann–Whitney U-tests to compare topics and maximum likelihood ratio chi-square tests to compare subgroups (McHugh, 2013).

We first conducted a Wilcoxon rank sum test with a continuity correction to compare topics for the total sample. The results showed high statistical significance ($p<0.001$) between most topics, confirming that the differences were not merely due to chance. In other words, our participants made a conscious effort to rate each topic based on their judgment, leading to distinct results. We then repeated this for the subgroups and found comparable results for 'novice', 'intermediate' and expert'. Interestingly, the 'no experience' subgroup showed low statistical significance for their responses between topics, suggesting that participants needed to have a minimum level of familiarity with cyber security to make sense of the information presented. It appears this group struggled to connect the terms presented for each prediction with the real-world context. By contrast, the more experienced subgroups were able to interpret the terms in the context, thus validating the proposed approach. To better understand the significance of the differences between subgroups (Table 27), we ran maximum likelihood ratio chi-square tests. As shown in Table 28, we found no statistically significant differences in the results. Indeed, only for Topic 3 did we approach weak significance (at the 0.1 level), as visually confirmed in Figure 40.

	Chi^2 statistic	***p*-value**
Topic 1	16.403	0.173
Topic 2	4.867	0.962
Topic 3	19.499	0.077
Topic 4	14.230	0.286
Topic 5	9.794	0.634
Topic 6	7.537	0.820
Topic 7	11.397	0.495
Topic 8	13.687	0.321

Topic 9	13.356	0.147
Topic 10	4.125	0.981
Topic 11	7.166	0.846
Topic 12	13.030	0.367
Topic 13	17.550	0.130
Topic 14	9.587	0.652
Topic 15	8.701	0.728
Topic 16	9.541	0.656
Topic 17	7.704	0.564

Table 28 - Maximum likelihood ratio chi-square subgroup test results

These results indicated that none of the differences between the subgroups were statistically significant, excluding Topics 3 and 13. For Topic 3, the difference between the ‘no experience’ subgroup and the other subgroups is statistically significant at the 0.05 level. For Topic 13, the difference between the ‘novice’ and ‘intermediate’ subgroups was statistically significant ($p<0.05$). In general, these U-test results were consistent with those of the maximum likelihood ratio chi-square test, allowing us to conclude that participants’ responses were independent of their experience given a minimum level of familiarity with security.

Next, we analysed which topics showed the strongest agreement among our participants. As the mean, standard deviation and entropy measures are inadequate to capture proximities in ordinal scales, we calculated Van Der Eijk (2001) Agreement A as well as Tastle and Wierman (2007) Consensus score (TW score hereafter) to investigate this further (Table 29). Both of these measurements were designed to analyse ordinal data by using Likert-type scales. Van der Eijk’s measurement ranges from -1 (disagree) to 1 (agreement). This scale thus represents a weighted average of the degree of agreement that exists in the simple component parts with the frequency distribution considered and does not suffer from the inconsistencies of more conventional measures (Krymkowski, Manning, & Valliere, 2009). The TW score is a probability distribution over a discrete set of choices with ordinal values that range from 0 (complete disagreement) to 1 (complete agreement). The scores for each topic were in line with the results illustrated in Figure 40; the total sample generally agreed on whether a security prediction was correct or not.

Topic	**Agreement A**	**TW**
Topic 1	0.596	0.716
Topic 2	0.388	0.605
Topic 3	0.577	0.708
Topic 4	0.593	0.652
Topic 5	0.578	0.683
Topic 6	0.534	0.664
Topic 7	0.351	0.585
Topic 8	0.5	0.647
Topic 9	0.575	0.706
Topic 10	0.323	0.571
Topic 11	0.541	0.688
Topic 12	0.5	0.635
Topic 13	0.437	0.618
Topic 14	0.59	0.715
Topic 15	0.214	0.527
Topic 16	0.47	0.665
Topic 17	0.556	0.702

Table 29 - Agreement measures for all 17 topics

Figure 41 provides an overview of the 17 prediction topics by these two scores. Topics 1, 14, 3, 9 and 17 were seen to have the strongest Agreement A and TW scores. At the other end of the scale, respondents had differing views on Topic 15, which also showed the highest standard deviation in our earlier tests. As all the scores showed agreement (for both measures), we observed general agreement among participants regardless of whether the rating was ‘prediction was correct’ or ‘prediction was incorrect’.

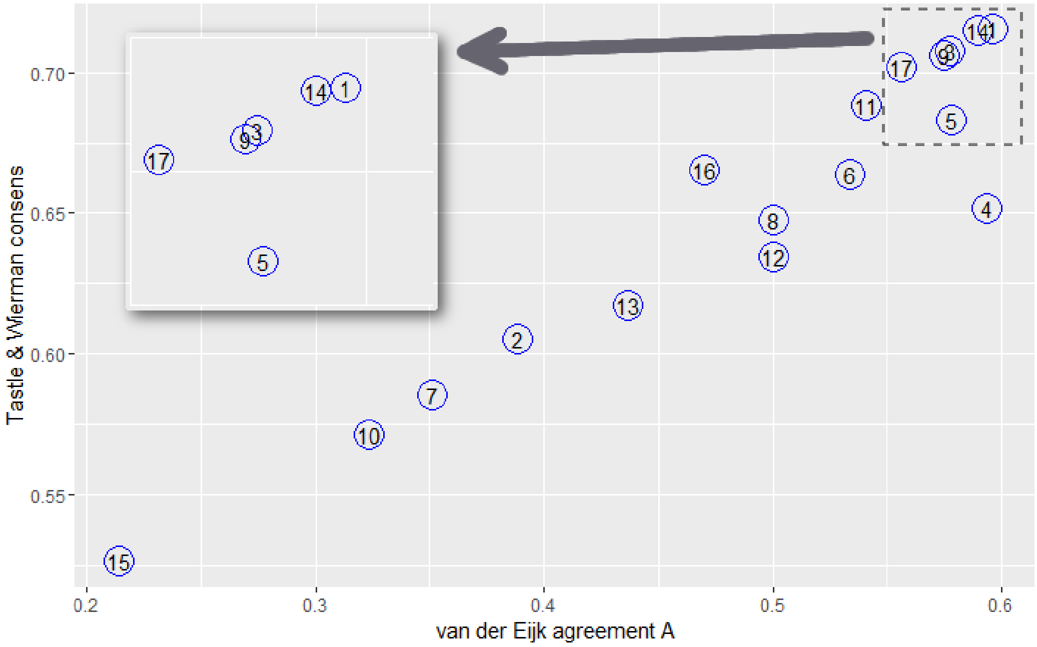


Figure 41 - Scatterplot for all topics: Agreement A and TW scores

6.5 Review of the 17 prediction topics

In this section, we provide a brief interpretation and review of the topics as well as present the key measurements for each prediction topic.

Topic 1: Organisations will increasingly make use of cyber security insurance to manage their risks in that space

Mean	Rank/mean	TW	Agreement A	Accurate
3.791	8	0.716	0.596	True

We found that participants followed our sample interpretation of this topic. With several large-scale breaches reported in 2015, it appears that our sources predicted considerable demand for cyber insurance services in 2016. Although this is not a strict threat prediction, it is clearly relevant to practitioners and their security strategy. Our participant pool agrees that this prediction was accurate. It also appears to resonate with the reports in the press (Muncaster, 2017; Murgia & Ralph, 2016) and by research institutes (GlobalData, 2017).

Topic 2: Internet of Things and connected devices will be a relevant security threat area

Mean	Rank/mean	TW	Agreement A	Accurate
3.366	12	0.605	0.388	True

This topic was expected to be one of the easier predictions to interpret, and several comments agreed with our own thoughts (*"Totally makes sense. Internet of Things was huge... and is still huge. This was predicted to be a big problem - and is"*). Much to our surprise, however, the prediction did not rank very high, especially among our two most experienced subgroups. However, after reviewing the threat developments in 2016, this prediction was shown to be correct (ENISA, 2017; McLellan, 2016; Symantec, 2016; Woolf, 2016).

Topic 3: Data breaches and stealing personal information or health records will be a relevant security threat area

Mean	Rank/mean	TW	Agreement A	Accurate
4.030	2	0.708	0.577	True

Data breaches and stealing personal data are likely to remain a threat for the foreseeable future (Morgan, 2016). This was also observed by our participants (*"There were a few major data breaches in 2016, at least one of them reaching record proportions"*). The mention of health records in this topic is noteworthy as it reflects the breach reality, at least in the first half of 2016 (McLellan, 2016).

Topic 4: A relevant security threat area is developing at the intersection of hackers, campaigns, social media, news, candidates and elections

Mean	Rank/mean	TW	Agreement A	Accurate
4.187	1	0.652	0.593	True

This was the 2016 prediction about which our participants agreed most strongly. This strong agreement was likely to have been supported by the timing of the survey in early 2017 when the media frequently reported on irregular activities in the US presidential election in 2016 (Allcott & Gentzkow, 2017; Gilsinan & Krishnadev, 2017). Some of the comments by our participants pointed to a link with the US election as well. If this threat is related to hacking activities, it is definitively a real cyber security threat. Hence, based on our survey, general reporting and other sources (ENISA, 2017; McLellan, 2016; Symantec, 2016), this prediction was accurate.

Topic 5: Vulnerabilities in large numbers of mobile apps (Android, Apple) and malicious mobile apps will be a security threat for users

Mean	**Rank/mean**	**TW**	**Agreement A**	**Accurate**
3.582	10	0.683	0.578	True

We found agreement among our participants that this prediction topic was relevant in 2016. Although security issues in the mobile space did not dominate security news compared with other topics, it was nonetheless a notable development (Murray, 2017). Indeed, McLellan (2016) reports that *"[m]obile malware is certainly still on the increase. In Q1 2016 alone, CERT UK saw 48 percent of the full-year 2015 amount of unique mobile malware samples"*. We also noted the corresponding remarks in the ENISA (2017) threat report.

Topic 6: Attacks on credit cards and payment (or financial) processes with fraudulent intentions will be a relevant security threat in 2016

Mean	**Rank/mean**	**TW**	**Agreement A**	**Accurate**
3.813	6	0.664	0.534	True

This topic is as straightforward to interpret as cyber security-related financial fraud developments. Our participants agreed that this was a problem in 2016 but also commented that this was no surprise. The prediction was correct, as evidenced by the number of large-scale breaches (Buntinx, 2017; SC Magazine, 2016). Somewhat on the fringes of this prediction, we find noteworthy attacks on financial systems such as SWIFT (Finkle, 2016), reinforcing the need to focus on the predicted developments in this threat area.

Topic 7: Cloud security and third-party network/application access control will see developing threats in 2016

Mean	**Rank/mean**	**TW**	**Agreement A**	**Accurate**
3.515	11	0.585	0.351	True

We observed general agreement by our participants that this prediction topic saw relevant developments in 2016. However, this degree of agreement was less clear than that for other topics. Publicly reported incidents in this space were scarce, with the most recognised the DropBox breach (Gibbs, 2016). Cloud-related breaches such as Yahoo (McGoogan, 2016) and Oracle (Kang, 2016) should be considered under this topic.

Topic 8: No interpretation

Mean	Rank/mean	TW	Agreement A	Accurate
2.418	17	0.647	0.5	False

In many cases, the output of topic models allows for the sensible interpretation of the underlying topic, but this is not always the case. The terms listed under this topic were too abstract to make a useful prediction. Participants did not see a relevant development, which is reflected in the scores. This is a limitation of the proposed approach.

Topic 9: We will see security threats developing with abuse/impact on trust in certificates and traffic encryption

Mean	Rank/mean	TW	Agreement A	Accurate
3.694	9	0.706	0.575	True

We found general agreement that this prediction was accurate. In 2016, there was a steady stream of privacy-related discussions on wiretapping and traffic interception, the abuse of certificate trust (J. Chen, 2016) and the erosion of trust in certificate authorities (Burton, 2017). If the prediction was broadened to encompass the wider topic of encryption, it becomes even more relevant, with high-profile cases such as mobile device encryption (Schneier, 2016) and the ransomware epidemic that became widespread in 2016.

Topic 10: Businesses with a customer base in Europe will shift their data protection approach

Mean	Rank/mean	TW	Agreement A	Accurate
2.515	16	0.571	0.323	False

Topic 10 was another difficult-to-interpret list of terms. It predicted that organisations would focus on changes in data ownership and data protection triggered by the upcoming General Data Protection Regulation for Europe. Participants felt that the topic mainly concerned generic business risk and did not describe a relevant security development in 2016.

Topic 11: Opportunistic malware attacks will remain a common attack vector for users

Mean	Rank/mean	TW	Agreement A	Accurate
3.940	4	0.688	0.541	True

As expected, malware continued to be a major threat in 2016, as evidenced by the high ranking of this topic. Indeed, ENISA (2017) states that *"[m]alware clearly tops cyber-threats for yet another year"* and delves into the various aspects of malware observed in 2016 (see Topic 14).

Topic 12: We will see an increase in attacks on systems and infrastructure with the goal to compromise credentials and conduct DDoS

Mean	Rank/mean	TW	Agreement A	Accurate
3.910	5	0.635	0.5	True

Participants focused on the DDoS aspect of this topic in their comments because of the large-scale attacks regularly reported towards the end of 2016 related to the Mirai botnet (Nordrum, 2016). Denial of service was not only a continued threat in 2016; it reached new levels of capability. Similarly to the other top-ranked threats, this topic is also confirmed by ENISA (2017) and others to be a noteworthy development.

Topic 13: The Internet will continue to change and provide new targets for exploitation

Mean	Rank/mean	TW	Agreement A	Accurate
3.261	13	0.618	0.437	True

This topic was interpreted as developing a threat landscape and attack vector for Internet-connected devices. Several terms such as ‘Chinese’, ‘power’, ‘federal’ and ‘terrorist’ were often associated with threats to critical infrastructure. While participants acknowledged the threat, they expressed that there were no obvious developments. We would align this topic with the Internet of Things trend rapidly changing the shape of the Internet and providing a rich attack surface. However, this topic is not particularly relevant alone.

Topic 14: Criminals will use ransomware and engineer new ransom techniques (targeting small businesses and platforms)

Mean	Rank/mean	TW	Agreement A	Accurate
3.970	3	0.715	0.59	True

As discussed in Topic 11, malware was a key threat in 2016, and this was strongly driven by ransomware variants. Indeed, according to Mathews (2017), SonicWall reported 638 million attacks in 2016, 167 times the number in 2015. Similarly, our participants agreed that this was a relevant threat development. We also note limited evidence of new ransom techniques affecting mobile devices (Forrest, 2016), Internet of Things (Schneier, 2017) and enterprise platforms (Goodin, 2017).

Topic 15: Hacking is expected to result in higher damage at the global level

Mean	Rank/mean	TW	Agreement A	Accurate
2.813	14	0.527	0.214	False

As with Topic 8, the output for this topic required too much interpretation to make a useful prediction. Participants did not see a relevant development, as reflected in the scores.

Topic 16: Threat developments in 2016 will require enterprises to increase efforts and resources to support and maintain their systems and software to avoid becoming a victim

Mean	Rank/mean	TW	Agreement A	Accurate
2.709	15	0.665	0.47	False

While this topic was difficult to interpret, the general position of participants was that this was no more a challenge in 2016 than in previous years.

Topic 17: Managing cyber security and anonymity online will be an increasing concern for governments

Mean	Rank/mean	TW	Agreement A	Accurate
3.799	7	0.702	0.556	True

The underlying topic here is the challenges of managing cyber security at the governmental level. Lower ranked terms such as state, legislation, cyber crime, APT and anonymity provide an intuition as to what the prediction sources described. The additional comments in the survey showed that participants agree with the notion that governments are increasingly addressing this area through rising funding and regulation. This broad topic is related to Topics 4 and 9.

6.6 Chapter summary

In this chapter, we investigated an approach for security practitioners to address one of the largest challenges when making value-based decisions in information security: reducing uncertainty in an evolving threat landscape. We used LDA, a probabilistic topic modelling approach, to identify 17 latent security threat prediction topics from 241 individual security predictions made for 2016. To verify the extent to which these predictions were realised, we gathered input from survey participants with varying security experience in early 2017. Presented with a description of these 17 topics, participants indicated whether there was indeed a notable development in that context in 2016. We found that participants saw relevant threat developments for 13 of the 17 topics with varying degrees of agreement. Moreover, the results were largely stable across subgroups of participants with various levels of experience. To better understand the robustness of the results, we conducted additional consensus-based tests, which added further weight to the survey results taken from the questionnaire. The presented results allow us to conclude that the security predictions published for 2016 did forecast notable developments in the field. According to the survey findings, the confirmed top predictions were related to hacking political campaigns (Topic 4), large-scale data breaches of personal data and health records (Topic 3), increasing threats from various types of malware (Topic 11), specifically ransomware (Topic 14), and large-scale DDoS attacks (Topic 14). We further used secondary sources to review threat developments in this context and thus provide support to the conclusions.

Our research findings are relevant to security practitioners and decision makers, who can use this approach to reduce uncertainty and improve the effectiveness of organisations' security programmes. Our approach helps tune down noise and outliers in the annual security prediction cycle, while focusing on the underlying threat developments without investing time in extensive trend studies or expensive security strategy consultancy engagements. The approach can be used as a basis to further refine organisations' security programmes by considering the circumstances and requirements applicable to the specific environment. By directing budget and efforts to the identified threat areas, investment in security can be optimised based on anticipated real-world developments. Although a tailored list of threats for any particular organisation might be difficult to supply, understanding the direction in which subject matter experts are forecasting future threat trends is advantageous.

Our approach makes conscious trade-offs and such limitations should be noted. The prediction corpus was condensed to a limited number of high-level topics by using LDA. As a consequence, the known limitations of LDA must be considered (Tang, Meng, Nguyen, Mei, & Zhang, 2014). Predefining the number of topics is a common challenge. We applied the harmonic mean approach proposed by Griffiths and Steyvers (2004), which is based on mathematical averages approximated from a specified multivariate probability distribution. For our dataset, we found 17 topics to be the optimum. In addition, the general question of whether a variant of LDA (e.g. hierarchical or enriched LDA) would produce better results in our case was not tested. Furthermore, we decided to present the topic/term list to participants without providing our interpretation to reduce the risk of influencing the rating. This required survey participants to draw their own conclusions, which is more demanding on their mental capacity and time, a common concern for interviews and survey tools. We used quality assurance questions in the survey design and added additional tests for subgroups and agreement scores to verify the robustness of our results. We took care to provide guidance on the time horizon participants should consider in their responses, but we cannot rule out a certain level of recency bias for some responses. To control for this, we provided media sources as corroborating data. Lastly, it must be noted that we describe a methodology and tool to achieve a reduction in uncertainty related to threat developments. We illustrate how this has been successfully applied and verified for one particular year. It is upon the practitioner to repeat this exercise on an annual basis to gain the then latest prediction output of course.

In the next chapter, we extend the research findings of previous chapters, particularly chapter 2, chapter 5 and this chapter, to create a conceptual latent model for information security value. In particular, we collect quantitative data from practitioners on the key components of information security value as discussed in previous chapters. The survey data are then utilised to verify a conceptual model as well as latent variables and measurement variables through structural equation modelling.

7 ASSESSING THE LATENT STRUCTURAL MODEL OF INFORMATION SECURITY VALUE IN ORGANISATIONS

Data is rapidly becoming one of the most important assets in global markets, and criminals are spotting opportunities to exploit new potential income sources. In response to this, organizations are dedicating increasing resources to information security programs. However, faced with unrelenting breach reports and rising costs, decision makers inevitably wonder which type of security investment is of real value to the organisation. In this chapter, we discuss a model describing the underlying key constructs for assessing information security value in an organisation. Based on latent variables and criteria identified as part of our research, we use a partial least squares structural equation modeling approach to verify the model's soundness. We identify five crucial variables for value-focused information security investment. The relationships among these latent variables are investigated and validated through common validity measures. We provide additional background on the topic and the design process in section 7.1 and 7.2. We find the conceptual model to be sound and suitable as underlying structure for adoption in our MCDA model (chapter 8).

As noted in chapters 2, 5 and 6, there are several common factors and relations in the context of information security value. In chapter 2, we investigated the components typically used to assess the economic value of information security investments in the academic literature. In chapter 5, we analysed senior practitioner interview data and obtained real-world input on the topic. Both these chapters illustrated the overwhelming complexity that security practitioners face when adding value to an organisation. Following the analysis of interviews discussing the value of information security and data extracted from the systematic literature on this topic, we defined a structural model and measurement variables. We then used this platform as the basis to design a survey instrument to assess our conceptual model through SEM, which is described in this chapter.

Throughout our research, we repeatedly heard that data are rapidly becoming one of the most important assets in global markets. Data are no longer just a by-product, but rather a driver of new and improved business models that generate high value. Hence, interest in this area is increasing rapidly—and not just for legitimate businesses (The Economist, 2017). Criminals are quick to spot opportunities and are adapting to these new value streams. Indeed, organised crime is embracing and exploiting billions of dollars of digital opportunities (Dethlefs, 2015; Hyman, 2013; Ponemon Institute, 2017). With losses at this magnitude and still rising, governments and regulators are playing an active role in encouraging businesses to protect their information assets (Pawlak & Wendling, 2013). This is not lost on senior executives, leading the security of an organisation's information assets to become a common agenda item in most boardrooms. As a result, security professionals are tasked with ensuring organisations are secure by addressing which of their assets should be protected, how they should be protected and how such protection adds value. However, although a substantial research body on information security risk management examines which assets to protect and how to protect them, research on the value of information security is scarce albeit rising (Anderson, 2001; Gordon, Loeb, & Zhou, 2016; Rue & Pfleeger, 2009) and the adoption of research findings by practitioners in the real world remains lacking. To improve the practical implementation of information security, we extend the body of knowledge by proposing an evidence-based model combining theoretical work with real-world experience. Recognising that information security is an interdisciplinary field with requirements along several corporate dimensions (managerial, organisational, cultural, technical, financial), we follow an exploratory convergent mixed method research approach (Creswell, 2013) to examine information security investment in this context. The background to this is described in the previous chapters, where we analysed the interview data obtained from senior practitioners and identify a range of key aspects they consider when investing in information security. We now combine those findings and the results of chapter 2 to create a new conceptual model. To verify the proposed model, we analyse the quantitative data gathered through a survey instrument designed for use with SEM. This approach allows us to investigate several key questions such as is there an underlying structural model for information security investment, what are the significant components and relationships in the model and what are the indicators of the components and how are they measured? Such a cross-sectional survey approach is suitable for answering the key questions such as ‘what’, ‘how much’ and ‘why’ (Pinsonneault & Kraemer, 1993). Figure 42 provides a schematic overview of the steps followed in this research to create the proposed model.

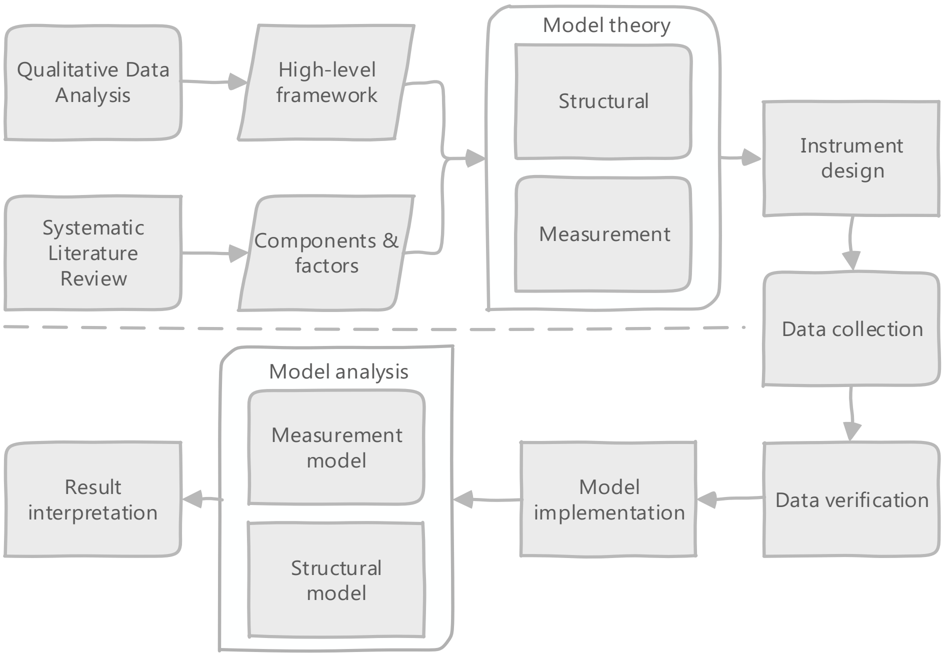


Figure 42 - Research approach for the structural model analysis

7.1 Related work

Early discussion on information security was mostly driven by technical aspects (Hitchings, 1995; von Solms, 1996), but it quickly moved onto governance topics (Dhillon & Backhouse, 2000; Dutta & McCrohan, 2002; Shuchih Ernest & Chienta Bruce, 2006) as well as focusing on value (Bojanc & Jerman-Blažič, 2008; Dhillon & Torkzadeh, 2006). Work on the economic aspects of information security (Anderson, 2001; Gordon & Loeb, 2002a; Hoo, 2000) was rapidly extended upon by research investigating the allocation and optimisation of security investment. For example, by taking into account the vulnerability of information and potential loss from a security breach, Gordon and Loeb (2002a) approach the topic as an optimal stopping problem and present a model to calculate optimal investment levels. Their model has been critically reviewed and extended by several researchers, including the original authors (Baryshnikov, 2012; Gordon et al., 2016; Matsuura, 2009; Willemson, 2010). Similarly, an ROI approach aligned with commonly used accounting principles was popular in the early days of research in this field (Al-Humaigani & Dunn, 2003; A. Davis, 2005; Mizzi, 2010; Sonnenreich, Albanese, &

Stout, 2006). However, it also attracted criticism because of the ambiguity in the underlying data as well as general applicability of the metric to information security (Gordon & Loeb, 2002b; Wood & Parker, 2004). Indeed, the publication of research on this approach and other related accounting metrics such as NPV has declined over time, as shown in chapter 2.

Cremonini (2005) improves on earlier approaches by introducing the concept of attacker returns. The author proposes coupling the ROI index with a corresponding ROA index that aims to measure attackers' convenience (or inconvenience). The notion of ROA is also a key component of game theory-based models. Bistarelli et al. (2007) use the concept of defence trees as an extension of attack trees with countermeasures and economic quantitative indexes such as ROI and ROA to evaluate the effectiveness of investment. Cavusoglu et al. (2008) argue that a game-theoretic approach is suitable as attackers modify their strategies in response to security investment by the defender. They show that sequential as well as simultaneous games in some circumstances lead to a higher payoff for the defender compared with a decision theoretic-based approach. Fielder, Panaousis, Malacaria, Hankin, and Smeraldi (2015) apply a hybrid game-theoretic–optimisation approach in the context of security spending, particularly by small and medium-sized enterprises. While they conclude that their approach works well in that context, they also highlight issues with optimal budget allocation caused by indirect costs. Carin, Cybenko, and Hughes (2008) combine several methods in their approach, using a Partially Observable Markov Decision Process for attack modelling. They find their methodology primarily suitable for approximating investment levels related to the protection of critical intellectual property in complex systems. H.-K. Kong, Kim, and Kim (2012) state that the financial focus on information security investment is inadequate and argue that any assessment should consider the multidimensionally of performance measures in an organisation. In particular, their modelling approach shows that technological and human aspects in the context of information security have a significant relationship with business performance. Hall, Sarkani, and Mazzuchi (2011) find the relation between organisational capabilities and information security to be crucial for a company's performance. They argue that a focus on organisational capabilities that raise information security and help meet organisational objectives has a positive impact on performance and competitive advantage. Weishäupl, Yasasin, and Schryen (2015) likewise take a resource-based view of the relationships between organisational resources and security investment.

7.2 Model design

Figure 43 shows the conceptual model proposed in this study, which includes five LVs: business environment (*BusEnv*), drivers (*Drivers*), threats (*Threats*), accounting aspects (*Accnt*) and security capabilities (*SecCap*). As discussed in chapter 3, information security investment is initiated by certain drivers and adjusted by challenges and constraints. Based on such drivers, challenges and constraints relevant to their environment, practitioners select the appropriate security capabilities, which are refined through organisation-specific factors such as the underlying business environment (i.e. corporate and security culture of an organisation) and accounting aspects.

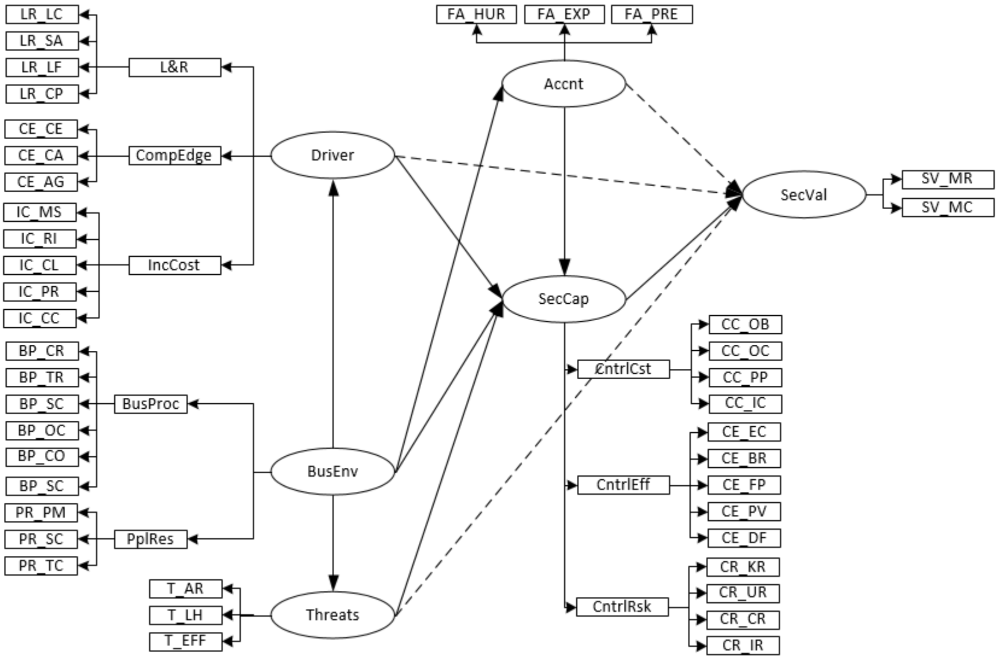


Figure 43 - Conceptual model

In our proposed model, the lower order constructs were set up as type 2 constructs by applying a two-stage approach, as this provides the benefit of more parsimony in the higher order structural model (Wetzels, Odekerken-Schröder, & Van Oppen, 2009). Readers familiar with the technology acceptance model (F. D. Davis, 1989) will note some resemblance to Davis's perceived usefulness and perceived ease of use LVs. As is common with SEM, we phrased the key research questions in the form of hypotheses and assessed significance in the context of the theorised model.

7.2.1 Business environment

The business environment represents sociotechnical considerations in the context of information security investment. Rather than relying on simple associative business attributes such as industry, firm size and geographic region, we focused on indicators related to people, the security culture and processes. This LV therefore represents the environment in which an organisation operates by understanding the corporate culture–information security relation (Gonçalves Fontes & José Balloni, 2007; Thomson & von Solms, 2006). It is a higher order construct reflectively modelled by using indicators related to the human capital resources and business processes relevant to information security considerations (Kraemer & Carayon, 2005; Van Niekerk & Von Solms, 2010). Hence, to understand the role the business environment plays in the extent to which information security adds organisational value, we propose the following hypotheses:

- H1a: The business environment of an organisation significantly influences the investment drivers and security capabilities of an organisation.
- H1b: The business environment of an organisation influences how security investment is viewed from an accounting perspective.
- H1c: The business environment of an organisation influences how threats are perceived.

7.2.2 Drivers

This LV is a higher order construct consisting of the three lower order constructs identified as common reasons for investing in information security: legal and regulatory, incident impact considerations and competitive advantage. The research by Moore et al. (2015) states that ensuring compliance and reducing incident impact are important drivers of security investment. Further, the effect of IT competency on business success has been extensively researched (Bassellier, Reich, & Benbasat, 2001); we see similar developments for information security competency being perceived as a competitive advantage. Indeed, although security requirements are increasingly defined as a part of contracts, surpassing expectations is seen as adding value and positively differentiating an organisation from its competition. To understand the role played by the driving factors in relation to security capabilities and value perception, we thus propose the following hypotheses:

- H2a: Information security investment drivers are positively associated with security capabilities.
- H2b: Information security investment drivers are positively associated with security value.

7.2.3 Threats

Recognising threats to information security is critical for any risk discussion (Whitman, 2003), as most threat attributes (who/what, why, when, how) are highly uncertain. Understanding the threat landscape and ongoing developments relevant to the organisation's industry enables security functions to direct their efforts (and investment) where they will add most value. To understand the role threats play as part of the information security function's value considerations, we propose the following hypotheses:

- H3a: Organisations' threat landscape is positively related to security capabilities.
- H3b: Organisations' threat landscape affects security value.

7.2.4 Accounting aspects

This LV represents the financial and managerial accounting aspects considered by security practitioners as part of organisational spending. While information security professionals are not expected to use complex valuation models such as ROI, NPV and IRR in their calculations, basic accounting requirements still apply to investment in security. Security functions are also expected to adhere to the organisation's guidelines on cash flow and expense type. Accountants assess the financial soundness of security investment and its contribution to the organisation's well-being (Ferrara, 2013; Gordon, Loeb, & Tseng, 2006). Hence, to understand how accounting aspects influence security capabilities and value delivery, we propose the following hypotheses:

- H4a: Organisations' financial and management accounting practices affect information security capabilities.
- H4b: Organisations' financial and management accounting practices affect information security value.

7.2.5 Security capabilities

We defined this LV as the ability of information security to deliver mission-aligned security services to the organisation. It is a higher order construct consisting of three lower order constructs representing risk control considerations, the cost aspects of controls and effectiveness (Baker & Wallace, 2007; Blatchford, 1995; Kankanhalli, Teo, Tan, & Wei, 2003). Effectiveness and risk control describe how reliable such a control is against threats, how completely it mitigates a risk and how fully it solves a problem in the context of the associated costs. To understand the degree to which security capabilities play a critical role in value delivery, we propose the following hypothesis:

- H5: Organisations' information security capabilities significantly contribute to information security value.

Table 30 summarises the five LVs adopted in the present study.

LV	**Conceptual description**
Business environment	Represents the sociotechnical aspects in the context of security investment with a focus on people and processes at the intersection of technology
Drivers	Captures the underlying reasons why organisations dedicate resources to information security controls and programmes
Threats	Represents the relevant security threats in the context of the organisation and its security investment
Accounting aspects	Describes the financial and managerial accounting aspects in the context of security investment
Security capabilities	Represents the capability considerations relevant to delivering mission-aligned security services to the organisation

Table 30 - Conceptual description of the LVs

7.3 Primary data collection

To take the conceptual model from theory to analysis, we designed a survey instrument to collect data. The survey was constructed to capture key information (on a nine-point Likert-type scale) with attention paid to its suitability for SEM analysis.

The validity and reliability of the instrument was verified by an expert survey designer with extensive experience of SEM. We also conducted test surveys among participants with cyber security expertise to confirm that the questions were easy to understand, the instructions were clear and the response options were suitable. This helped us identify any remaining issues. To recruit participants, we followed a cluster sampling approach to solicit responses from professional networks and peer groups in the information security and IT fields. In addition, the survey was opened to prescreened audiences engaged through Amazon Mechanical Turk (Behrend et al., 2011). We received 293 responses, of which 43 were removed because of data issues, leaving 250 valid responses for our analysis. We used WarpPLS (Kock, 2011) for the PLS-SEM analysis. The core of PLS is a family of alternating least squares algorithms that emulate and extend principal component analysis as well as canonical correlation analysis (Henseler et al., 2016). Originally described by Wold in a series of academic contributions, this approach has since been modified and extended (Sanchez, 2015; Wold, 1974, 1982). The PLS approach has matured through this academic discourse (Henseler et al., 2014; Rigdon, 2016; Rönkkö & Evermann, 2013). Similar to covariance-based SEM, PLS models consist of two sets of equations commonly referred to as the inner (structural) and outer (measurement) models. The structural model describes the relationship between the LVs in the conceptual model, whereas the measurement model shows the relationships between each LV and its associated indicators (Hair, Ringle, & Sarstedt, 2011).

PLS-SEM is an appropriate choice for our research for four main reasons. As described by Hair Jr et al. (2016), it is particularly useful for studies of the sources of competitive advantage and key success factors, as it can predict and identify the target constructs. This is desirable because research on information security economics is relatively new and the theoretic fundamentals are still under development. Second, PLS-SEM is advantageous when the structural model is complex and the constructs have many or very few indicators. Third, it can work with non-normally distributed data (Roldán & J. Sánchez-Franco, 2012). Finally, PLS-SEM is applied in a range of research areas (Kaufmann & Gaeckler, 2015; Richter, Sinkovics, Ringle, & Schlägel, 2016; Ringle, Sarstedt, & Straub, 2012) and has previously been used in the field of information security (H. Kong, Jung, Lee, & Yeon, 2015; Riek, Böhme, & Moore, 2014).

To assess the optimal sample size, we based our calculations on a minimum path magnitude set at 0.197, significance level of 0.05 and statistical power of 0.9. Our sample thus fulfils the requirements for SEM-PLS based on the inverse square root method and gamma-exponential method calculations (Kock & Hadaya, 2016). The 250 participants in the sample represent a diverse selection of professionals. Most work in management positions (59%) in medium-sized (43%) or large (44%) organisations and rate themselves as having moderate (58%) to high (34%) knowledge of information security. The most common responses on purchasing experience are intermediate (44%) and advanced (36%). Industry representation is balanced with the telecoms (26%) and finance industries (14%) the most common. The full survey demographics are presented in the Appendices. Figure 44 summarises the breakdown of the research participants.

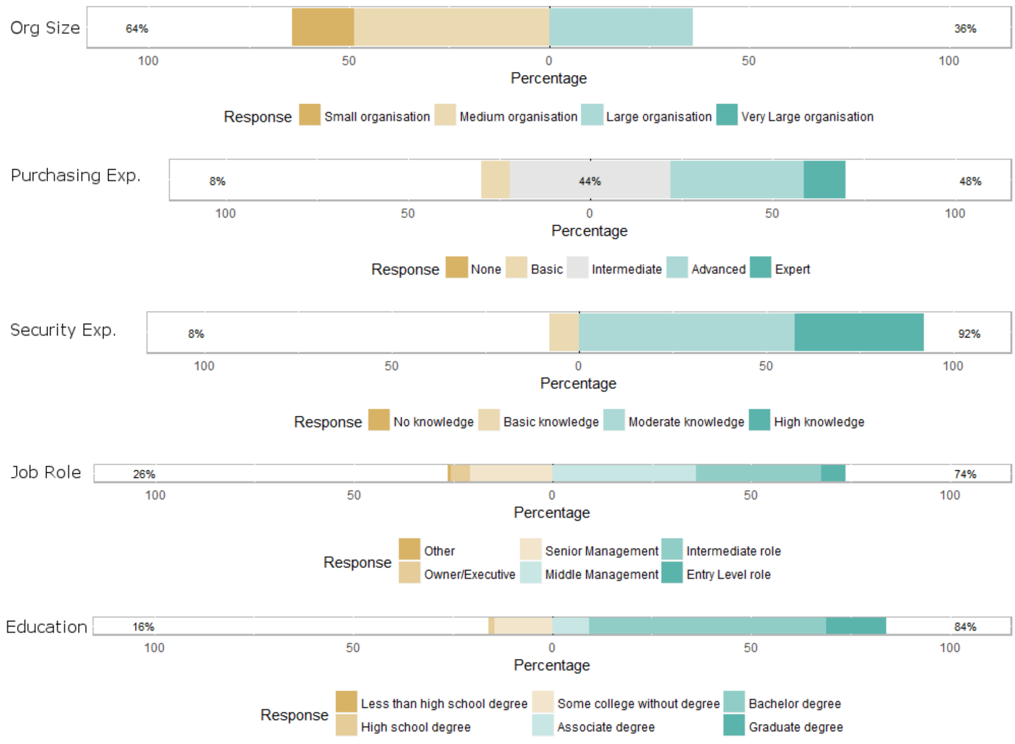


Figure 44 - Overview of survey participants

7.4 Evaluation of the measurement model

As outlined by Hair Jr et al. (2016), researchers must consider two broad types of measurement specifications when developing constructs: reflective (mode A) and formative (mode B). Following the guidelines of Jarvis, MacKenzie, and Podsakoff

(2003), we defined the constructs in our model as reflective (see Figure 43). To evaluate the reflective measurement model, we assessed its internal consistency, reliability and convergent and discriminant validity. Internal consistency is reported based on Dijkstra's rho_α, as this is a better approximation of the true reliabilities than composite reliability (CR) and Cronbach's alpha (Kock, 2017). We provide CR as an additional measure for reference. The results should be above 0.7, but in exploratory research values as low as 0.6 are also acceptable (Hair Jr et al., 2016). As shown in Table 31, all the values were well within the acceptable range without reaching the problematic 0.95 redundant measurement threshold. To establish convergent validity, we calculated the average variance extracted (AVE) of the LVs. To ensure the LV sufficiently explains the variance of its indicators, we require this measure to be above 0.5. Table 31 shows that this requirement was met for all the LVs. Indicator reliability was assessed through the outer loadings of the associated LV. Indicators with loadings above 0.7 are considered to be acceptable and should be retained (Hair et al., 2011). Table 32 provides an overview of the loadings and cross-loadings, showing that reliability was established. To assess discriminant validity, we observed the Fornell–Larcker criterion, but referred primarily to the heterotrait-monotrait ratio of correlations (HTMT). HTMT has been shown to have higher reliability for detecting the lack of discriminant validity (Ab Hamid, Sami, & Sidek, 2017; Henseler, Ringle, & Sarstedt, 2015). Table 31 lists the Fornell–Larcker results in the lower triangle, illustrating overall validity with a minor exception between *Drivers* and *BusEnv*. However, as the HTMT results in Table 33 show, all the values were below 0.9, and even below the more conservative 0.85 threshold; hence, we considered discriminant validity to be established.

	rho_α	**CR**	**AVE**	**Drivers**	**BusEnv**	**Threats**	**Accnt**	**SecCap**	**SecVal**
Drivers	0.879	0.867	0.686	0.828					
BusEnv	0.837	0.83	0.71	0.828	0.842				
Threats	0.862	0.831	0.622	0.523	0.63	0.789			
Accnt	0.794	0.793	0.562	0.731	0.723	0.514	0.749		
SecCap	0.879	0.867	0.687	0.643	0.786	0.644	0.345	0.829	
SecVal	0.816	0.816	0.69	0.404	0.48	0.419	0.135	0.734	0.83

Table 31 - Consistency and reliability measures

	Drivers	BusEnv	Threats	Accnt	SecCap	SecVal
IncCost	0.877	0.708	0.490	0.563	0.601	0.415
L&R	0.777	0.586	0.398	0.611	0.468	0.302
CompEdg	0.827	0.687	0.435	0.575	0.512	0.280
PplRes	0.629	0.817	0.511	0.524	0.658	0.394
BusProc	0.770	0.867	0.576	0.666	0.652	0.378
T_AR	0.376	0.427	0.779	0.359	0.439	0.294
T_LH	0.466	0.584	0.788	0.412	0.630	0.439
T_EFF	0.379	0.476	0.799	0.410	0.464	0.196
FA_HUR	0.551	0.561	0.312	0.764	0.201	0.049
FA_EXP	0.515	0.516	0.436	0.718	0.285	0.110
FA_PRE	0.604	0.563	0.415	0.765	0.273	0.051
CntrlEf	0.573	0.745	0.608	0.367	0.887	0.623
ContrlR	0.535	0.653	0.538	0.293	0.853	0.619
CntrlCs	0.482	0.572	0.416	0.251	0.739	0.464
SV_MR	0.353	0.422	0.383	0.134	0.631	0.841
SV_MC	0.352	0.438	0.364	0.169	0.641	0.819

Table 32 - Indicator loadings and cross-loadings

	Accnt	BusEnv	Drivers	SecCap	SecVal
Accnt					
BusEnv	0.7338				
Drivers	0.7376	0.8326			
SecCap	0.2902	0.6736	0.6138		
SecVal	0.1331	0.4273	0.4122	0.7333	
Threats	0.5329	0.6364	0.5503	0.6612	0.4332

Table 33 - HTMT results

7.5 Structural model evaluation

Given the reliability of the outer model demonstrated above, we next analysed the structural model (inner model) to (i) assess how the LVs relate to one another and (ii) express these relationships through paths. To understand the significance of the relationships, we adopted a resampling approach. In particular, following the recommendation by Kock (2014b), we applied the WarpPLS default resampling method 'Stable3', which has been shown to yield results consistent with those obtained via bootstrapping (and in many cases more accurate estimates). The results are shown in Table 34 and Figure 45, where the path coefficients are noted as beta coefficients. As is common, the confidence level is set at 0.95.

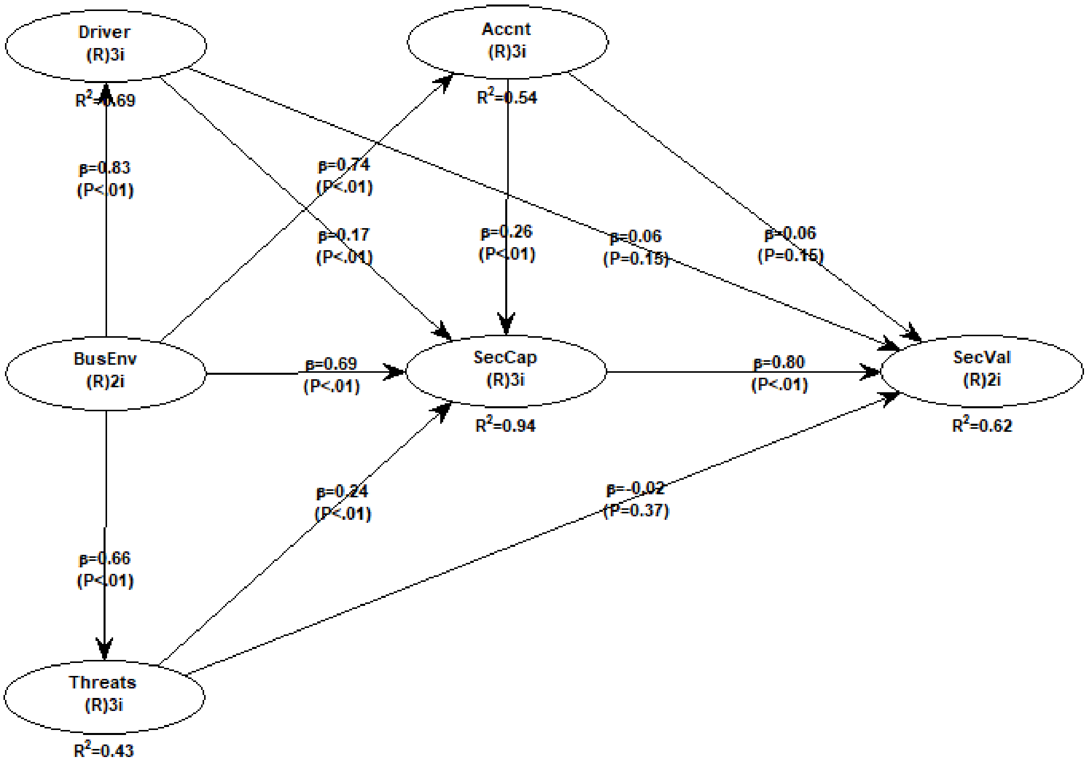


Figure 45 - Structural model results

	Drivers	BusEnv	Threats	Accnt	SecCap
Drivers		0.828			
BusEnv					
Threats		0.657			
Accnt		0.738			

SecCap	0.168	0.694	0.244	0.26	
SecVal	0.064		-0.021	0.064	0.797
Drivers		<0.001			
BusEnv					
Threats		<0.001			
Accnt		<0.001			
SecCap	0.003	<0.001	<0.001	<0.001	
SecVal	0.152		0.369	0.152	<0.001

Table 34 - Structural model path coefficients (top) and significance levels (bottom)

The coefficient of determination (R^2 value) measures how much of the variance in the endogenous constructs is explained by the exogenous constructs. The R^2 values range from 0 to 1 with substantial, moderate and weak effect thresholds at 0.75, 0.5 and 0.25, respectively (Hair et al., 2011). The adjusted R^2 values for our model are *Drivers* (0.685), *Threats* (0.430), *Accnt* (0.542), *SecCap* (0.943) and *SecVal* (0.617) and thus fall mostly into the moderate to substantial brackets. Likewise, for the effect sizes, which are the absolute values of the individual contributions of the corresponding predictor LVs to the R^2 coefficients of the criterion LV in each LV block (Kock, 2014a), we find medium (>0.15) to large (>0.35) results, with few below the small (>0.02) threshold (Table 35).

	Drivers	**BusEnv**	**Threats**	**Accnt**	**SecCap**	**SecVal**
Drivers		0.686				
BusEnv						
Threats		0.432				
Accnt		0.544				
SecCap	0.113	0.564	0.16	0.107		
SecVal	0.027		0.01	0.014	0.593	

Table 35 - Effect sizes for the path coefficients

To assess the predictive validity associated with the model, we observed Geisser's Q2 (Geisser, 1974) values for the LVs. Acceptable predictive validity is represented by a Q2 value above zero, which was the case for all our endogenous LVs: *Drivers* (0.687), *Threats* (0.435), *Accnt* (0.540), *SecCap* (0.740) and *SecVal* (0.568). In summary, our proposed model satisfied the consistency, reliability and convergent and discriminant validity requirements. Hence, we used the model to answer our research questions in the next section.

7.6 Results and discussion

First, we examine the influence of the business environment on information security investment and identify the significant effects on the LVs in the model. To test H1a, we investigate the relations *BusEnv* -> *Drivers* and *BusEnv* -> *SecCap*. With a *β* coefficient of 0.828 (*p*<0.001) and a large effect size (0.686), we find that the business environment significantly influences information security investment. Moreover, as this relation is the strongest observed in our model, it should be the first area for professionals aiming to improve their security functions to investigate. Similarly, the relation *BusEnv* -> *SecCap* shows a strong *β* coefficient (0.694, *p*<0.001) and a large effect size of 0.564. As security capabilities represent the ability of the security function to deliver business-aligned security services to the organisation, this strong relation is intuitive. Next, we investigate H1b to understand if security investment is treated differently from an accounting perspective depending on the business environment. We find a strong relation between *BusEnv* and *Accnt* (*β*=0.738, *p*<0.001), perhaps because as organisations increase in maturity, their accounting requirements become more refined. In other words, a small locally trading business is unlikely to have the same accounting processes as a highly regulated global enterprise. We conclude that the business environment shows a significant relation with accounting considerations in the context of information security investment. A similar explanation may be true for the *BusEnv–Threats* relationship (H1c). We find a high *β* coefficient (0.657) significant at the 0.1% level as well as a large effect size (0.432). This finding indicates a significant relation between threat considerations and the underlying business environment. As the business becomes more conscious of information security, it is reasonable to assume that the consideration of threats in the context of security investment rises as well. Based on the above-presented results, we therefore accept H1.

To understand the relation between the drivers and security capabilities of an organisation (H2a), we next analyse these two LVs. We find the path *Drivers* ->

SecCap to be highly significant (p=0.003); however, with a β coefficient of 0.168, it is somewhat weaker than expected compared with the other parts of the model. Reminding ourselves that the model results are based on reported real-world data, we suspect that this result may indicate that current practices do not sufficiently consider business drivers when creating security capabilities in the organisation. We believe this offers an opportunity for security professionals to realign their strategy with business-specific security drivers. Observing the path *Drivers -> SecVal*, we note that the relation is not significant (β=0.064, p=0.152) and thus H2b is rejected. On closer inspection, however, we find mediating effects (i.e. an effect for a path with two segments) and note a total effect of β=0.199 (p< 0.001), suggesting that drivers indeed significantly affect security value but that such an effect is delivered through security capabilities.

H3a proposes that an organisation's threat landscape is positively related to its security capabilities. In other words, as the (perceived) threat level strengthens, so do security capabilities. We find this reflected in the results of the model with high significance observed on the path *Threats* -> *SecCap* (β=0.244, p<0.001). As a consequence, security programmes that do not consider relevant threats are likely to over- or under-deliver on security capabilities. H3b examines whether threats directly relate to security value; this does not appear to be the case. The path *Threats -> SecVal* does not reach significance (p=0.369). However, we observe a mediated effect through *SecCap*, resulting in a total effect of β=0.174 (p=0.003) on *SecVal*. These results allow us to conclude that understanding relevant threats is important when delivering security value through the organisation's security capabilities.

Although research has commonly assessed the profitability of information security investment (European Network and Information Security Agency, 2012; Wood & Parker, 2004), such valuation assessments remain uncommon in the real world, with basic accounting questions such as expenditure type, hurdle rate and insurance premium impact more frequently used. In H4a, we investigate the effect of these accounting processes on security capabilities. The path *Accnt -> SecCap* has a positive β of 0.26 with high significance (p<0.001) and a medium effect size (0.107). This finding indicates a positive effect on *SecCap* when accounting requirements form part of the security control investment process. The assumption here is that the requirement causes security practitioners to take a broader view of security control selection and thus results in an overall improved choice. Further, the low effect size is intuitive as we would expect accounting aspects to have only limited impact on security capabilities. For H4b, the direct path *Accnt* -> *SecVal* does not reach significance (*β*=0.064, *p*=0.152). Instead, we find it to be mediated by *SecCap*, resulting in an indirect effect *Accnt* -> *SecCap* -> *SecVal* of *β*=0.272 (*p*<0.001).

Finally, H5 proposes that security capabilities play a key role in securing the organisation and delivering value. The path *SecCap* -> *SecVal β* coefficient (0.797) is highly significant (*p*<0.001), and thus H5 is supported. It might seem clear that changes in security capabilities are strongly related to the achieved security value. Nonetheless, this would be an oversimplification. Indeed, the reasons behind this strong relation are the LVs and indicators in the model, which contribute to the overall effect confirmed in H5.

In summary, we identify several indirect effects in the inner model that tie requirements across the various LVs to the value outcome. Consequently, this study's results support the assumptions of the conceptual model on those aspects relevant to a value-oriented information security investment model. Table 36 summarises the results of the tested hypotheses.

Hypothesis	**Path**	**β**	**p-value**	**Effect size**	**Validation**
H1a	BusEnv ≥ Driver	0.828	<0.001	0.686	Supported
H1a	BusEnv ≥ SecCap	0.694	<0.001	0.564	Supported
H1b	BusEnv ≥ Accnt	0.738	<0.001	0.544	Supported
H1c	BusEnv ≥ Threats	0.657	<0.001	0.432	Supported
H2a	Drivers ≥ SecCap	0.168	0.003	0.113	Supported
H2b	Drivers ≥ SecVal	0.064	0.152	0.027	Rejected
H3a	Threats ≥ SecCap	0.244	<0.001	0.160	Supported
H3b	Threats ≥ SecVal	-0.021	0.369	0.010	Rejected
H4a	Accnt ≥ SecCap	0.260	<0.001	0.107	Supported
H4b	Accnt ≥ SecVal	0.064	0.152	0.014	Rejected
H5	SecCap ≥ SecVal	0.797	<0.001	0.593	Supported

Table 36 - Results of the tested hypotheses

We highlight several of the limitations of the study that need to be considered when interpreting the results. First, research on information security value in the organisational context is still in its infancy; it is not yet a topic commonly considered by practitioners and self-assessing one's knowledge in a survey context is difficult. We addressed this limitation by targeting relevant peer groups and prescreening participants. Although we used several controls to maximise the quality of the survey data, it is nonetheless possible that survey participants over- or underestimated their level of knowledge. Second, the survey response represents the respondent's thoughts at a point in time, which does not necessarily reflect the actual situation in the work environment. This is a well-known shortcoming of survey instruments and generally acceptable as long as accounted for (Pinsonneault & Kraemer, 1993). Lastly, our data analysis approach (i.e. PLS-SEM) inherits the limitations common to this approach. As described in section 7.2, the quantitative part of the study is based on findings obtained through a GT qualitative analysis and aims to discover knowledge. PLS is suitable for this task. To ensure the consistency, reliability and validity of our results, we used several methods common to SEM. However, we make no claim that this is the only or the best model in this context.

7.7 Chapter summary

In this chapter, we proposed a conceptual model for assessing information security value in organisations. Based on the findings of previous chapters and survey results gathered for the quantitative analysis, we proposed a model consisting of five LVs that represent the key areas in this context. We then investigated how these LVs relate to each other and analysed which relationships are significant by using PLS-SEM, finding support for our proposed model.

We highlight several findings that represent valuable contributions to both practitioners and researchers in this field. Our assumption that the underlying business environment plays a fundamental role in the delivery of value-oriented security services to an organisation was supported by highly significant path coefficients. Practitioners can immediately apply this insight by reflecting on the sociotechnical aspects of their environments and ensuring that their current security programmes are a good fit for their organisations. The misalignment of the business environment and drivers can result in considerably worse outcomes for security value as evidenced by the large effect size found in this study. For researchers, this finding provides a statistical basis for investigating the sociotechnical aspects of information security and its relation to business outcomes in more detail. The model further highlights the significance of understanding the threat attributes relevant to an organisation. While many practitioners will already include threat considerations in their control selection processes, our results provide additional guidance that the business environment must define which threat attributes are relevant and should be considered to deliver value-oriented security capabilities. We further proposed accounting considerations to be a significant LV when defining security capabilities and security value delivery. This hypothesis was supported in the analysis, with a significant indirect effect on security value. This important insight suggests that the value of information security benefits from accounting scrutiny. While we did not find evidence that more advanced financial valuation methods (e.g. ROI, NPV) are common in this context, we do observe a positive impact on security capabilities where accounting aspects are considered. Security practitioners should thus identify those accounting requirements important to their finance departments and proactively optimise security capabilities to improve business-specific security value. Finally, we found significant support for our hypothesis that security capabilities are crucial to achieving business-aligned security value. This finding was evidenced by the highly significant path coefficient and large effect size in the security capabilities–value relation. The importance of this result is twofold. First and most obvious, we provide strong evidence that security capabilities have the largest direct effect on the value organisations gain from information security investment. Second, our model shows that the value outcome is strongly influenced by organisation-specific constructs that must be considered when creating security capabilities; a cookie-cutter approach to information security will not result in optimal value.

In summary, this chapter proposed a conceptual and empirically tested model that outlines the underlying constructs to consider when assessing information security value in an organisation. We presented important insights and highlighted use cases for practitioners to apply our findings in their environments. In particular, the findings contribute significantly to our understanding of information security value chains within organisations. The presented model and proposed constructs provide a validated basis on which we can extend in the next chapter. The following chapter applies the latent construct findings to real-world information security investment decision scenarios. This provides additional information on each indicator and presents a value-prioritised multicriteria decision model utilising stochastic multicriteria acceptability analysis (SMAA).

8 STRUCTURED MULTICRITERIA DECISION MAKING FOR VALUE-PRIORITISED SECURITY INVESTMENTS

The media and research regularly issue reports on organised crime exploiting billions of dollars of digital opportunities (Dethlefs, 2015; Hyman, 2013; Ponemon Institute, 2017). We previously investigated the economic impact of such breach events in chapter 3. With losses at this magnitude and still rising, governments and regulators are taking an active role in encouraging businesses to protect their information assets (Home Office Science Advisory Council, 2018; Pawlak & Wendling, 2013). This pressure is increasingly felt by non-regulated industries as well, as requirements filter down through the supply chain. Boards find themselves in a situation where they need to ensure their organisations manage information security risks and compliance requirements appropriately, while also balancing organisational resource use and optimising value for stakeholders. This poses a tough challenge for security professionals who are tasked by the board to ensure the organisation is secure and, while doing so, justify how the programme adds value to its core business. While practitioners are generally comfortable with the 'how' to secure the organisation, the value justification tends to be more challenging. The approach often taken is one of 'needs must' to achieve a minimum level of security and/or align the organisation with industry standard frameworks to respond to a breach (L. A. Gordon, M. P. Loeb, & W. Lucyshyn, 2003). These are viable approaches and do provide security benefits, but won't lead to a security program that emphasises value for the organisation. Of course, each organisation is different and has different views on how security does add value to their business. For some organisations compliance with certain regimes is perceived to be most valuable, for others it is a sensible balance between security and business process optimisation and yet others aim to use security capabilities to unlock new markets and business opportunities. However, for most organisations it will be a cross section of all these that represents value in their business.

In this chapter, we present a multicriteria decision model that information security practitioners can use to deliver value in their security control investments. This model combines the insights from the expert interviews on the value aspects of information security (chapter 5), key components in this context derived from the academic literature (chapter 2) and latent constructs underlying security investment decisions with real-world criteria preference defaults relevant in this context (chapter 7) as well as utilises SMAA for making an alternative selection.

8.1 Related work

Decisions in the field of information security tend to be complex due to the diverse intersecting research areas that need to be considered (Dhillon & Backhouse, 2001; Dhillon, Oliveira, Susarapu, & Caldeira, 2016). This complexity increases further if we add the concept of information security value to the problem space. As discussed in earlier chapters, academic research proposes a variety of approaches and models that focus on different aspects of information security and value. For example, Gordon and Loeb (2002a) present a benefit maximisation approach that considers the vulnerability of information to a security breach and potential loss should such a breach occur. This model inspired further research (Baryshnikov, 2012; Farrow & Szanton, 2016; Matsuura, 2009; Willemson, 2010), including updated guidance by the original authors (Gordon, Loeb, Lucyshyn, & Zhou, 2018; Gordon et al., 2016). Arora, Hall, Pinto, Ramsey, and Telang (2004) propose a risk-based value approach utilising incident types and bypass rates as input criteria. Cavusoglu et al. (2008) follow a game-theoretic approach to determine security investments in which they consider attributes such as vulnerabilities, hacker utility and payoff from investments. The approach described by Cremonini (2005) also aims to improve ROI-based evaluations by integrating them with an ROA index, including attacker gains and control efficiency as attributes.

There is considerable overlap between these models (Neubauer & Hartl, 2009; Rue & Pfleeger, 2009). At a general information security level, Dhillon and Torkzadeh (2006) utilise a value-focused thinking approach to identify fundamental means and values that are essential for protecting the information resources of a firm. Pettigrew and Ryan (2012) investigate how senior professionals approach key decisions related to information security value under uncertainty. Their open-ended interviews provide a condensed view of the fundamental aspects of the information security decision space. Similarly, Moore et al. (2015) conduct in-depth interviews with senior security professionals to explore how firms identify, prioritise and invest to manage cyber security risks. Their conclusions highlight the challenges related to project resourcing, recruiting qualified personnel, overcoming uncertainty in the threat landscape and measuring value. In this work, we follow a Grounded Truth approach (chapter 5.2) to investigate the underlying categories, criteria and processes in information security investment decisions. It is a suitable approach for this research. Based on a constructivist paradigm, this theory acknowledges that meaning is constructed by individuals and is not simply something merely waiting to be discovered. A similar approach is followed by Dor and Elovici (2016), arriving at comparable results. Although presented in a different manner, the results of these studies confirm the common manifest/latent categories and criteria considered by decision makers, highlighting that the topic of information security value must be seen as a multicriteria decision making problem.

Multicriteria decision making can be described as a collection of formal approaches adopted to explore complex decision matters considering multiple, typically conflicting, criteria of both a quantitative and a qualitative nature. It helps decision makers disaggregate complex problems into manageable chunks, allowing a more focused view on how certain options achieve or contribute to objectives, before reassembling it for decision guidance. Based on the work by Keeney and Raiffa (1976) as well as the seminal paper by Zionts (1979), multicriteria decision making is built on decision theory and notably driven by Operational Research. At a high level, multicriteria decision making consists of multicriteria decision analysis (MCDA; see Belton and Stewart (2002) for their integrated view of MCDA) and multi-objective decision making. MCDA is typically concerned with ranking, sorting or selecting finite alternatives based on criteria, whereas multi-objective decision making aims to maximise or minimise an objective function subject to constraints. Liou and Tzeng (2012) provide an excellent overview of recent development in this space; see also Greco et al. (2016) as well as (Marttunen, Lienert, & Belton, 2017) for an extensive survey on this matter.

MCDA has been successfully applied to complex decision studies across a range of research areas: healthcare (Diaby, Campbell, & Goeree, 2013; Saint-Hilary, Cadour, Robert, & Gasparini, 2017), information security (Lv, Zhou, & Wang, 2011; Ou Yang, Shieh, Leu, & Tzeng, 2009), environmental research (Durbach & Davis, 2012;

Gbanie, Tengbe, Momoh, Medo, & Kabba, 2013; Greco, Ishizaka, Matarazzo, & Torrisi, 2017), sports science (J. Calder & Durbach, 2015) and policymaking (Beuthe, Eeckhoudt, & Scannella, 2000). Please refer to Mardani et al. (2015) for a more comprehensive literature review on this topic.

8.2 Structuring the decision problem space

According to Belton and Stewart (2002), the principal goal of MCDA is to help decision makers understand the problem and make the relevant values and judgements to guide them in identifying a preferred course of action through the process of synthesising and organising the relevant information. Gaining an appreciation of the problem is the first step. Understanding the problem space is crucial to making robust decisions. While the problem and its components may appear obvious at first glance, problem structuring is a fundamental and often overlooked precursory step in information security investment decision making for time-pressured decision makers in the field. The likely consequence of omitting this step is a suboptimal investment decision, or even a decision that addresses the wrong problem (Mitroff & Featheringham, 1974).

Based on their *"Through complexity to simplicity"* principle, Belton and Stewart (2010) argue that problem structuring starts by surfacing and capturing the underlying complexities to allow decision makers to better understand and manage the problem at hand. In our research, we utilised a GT approach to discover the relevant underlying problem structure with the help of qualitative analysis (chapter 5). The GT approach allows for the collection of rich and vivid primary data from research subjects, which in turn emphasises the lived experience and is fundamentally well suited to locating meaning and connecting such meaning to the real world (Miles & Huberman, 1994). By examining, re-examining and reflecting on the views shared in expert interviews, the relations and components relevant to information security value were identified. As a result, complexity was stripped away and the simplicity of the key underlying components was distilled to further define the problem space. Supported by in vivo coding relationship graphs and conceptual building blocks, this tailored approach resembles soft operational research problem structuring methods such as strategic options development and analysis (Eden, 2004; Georgiou, 2011). Our interview design guided participants towards responses with a *"value-focused thinking"* mindset (Keeney, 1994) instead of taking an alternative-focused or problem solving position. This was an important aspect to our research, as our original intention was to explore the general information security value problem space rather than a specific security investment alternative.

Our grounded truth work allowed us to form a conceptual model of information security value aspects and provided detailed qualitative results. To solidify our assessment of the key components, criteria and relations in this problem space, we followed an exploratory convergent mixed method approach (QUAL -> QUANT). By combining the results of the qualitative analysis with the key findings from our SLR on economic valuation methods (chapter 2), we created a survey to gather quantitative data on the topic (see chapter 7). While it would be too time- and resource-intensive to repeat the full process for every one-off decision, we found this approach to problem structuring highly useful for structuring the space for a repeated decision problem. As our goal is to explore the problem space to build a decision model valid for all information security investment decisions, the depth of the process and resources invested is justified. It provides a deep understanding of a general latent problem structure derived from primary and secondary data analysis. Hence, we can confidently build on this to further develop the decision model.

The results of our extensive problem structuring efforts reveal their strengths when applied in the context of a one-off decision problem in an organisation. Such an application allows us to considerably streamline local problem structuring efforts, as the relevant criteria are already identified and an established baseline of weights provided, as discussed in the next section. However, the practitioner must still define some aspects of the concrete information security problem s/he is addressing in the complex one-off decision for the organisation.

While our model provides the fundamental platform for real-world information security investment decision problems, organisation-specific requirements demand a local definition. At the local level, the practitioner must identify whether a specific need for security controls exists (e.g. resulting from regulatory requirements, risk management actions or strategic security planning) and select from the available alternatives. Simply put, the security practitioner has the responsibility to define if and where investment in security controls is needed. For most practitioners, this will be a familiar exercise, as this is part of their usual responsibilities in the context of security programme management and planning.

Once the requirement for a security investment is established, an initial analysis of the problem will open a range of possible alternatives from which to choose. For example, an organisation pursuing a security certification such as the UK's CyberEssentials Plus (A. Calder, 2014) may identify the need to provide malware protection in their environment. Based on the security practitioner's input, a prescreened set of alternatives, excluding those that do not meet certain minimum specifications, will be taken into the MCDA in our proposed model. While it may be possible to skip the prescreening step and simply include all the alternatives available, the resulting overhead would be unmanageable in most cases depending on the organisation's comfort with such processes and whether the local problem structuring is conducted following a formal or informal approach (Belton & Stewart, 2010). Either way, the number of alternatives should be reduced to a sensible shortlist based on subject matter expert input. Figure 46 provides an overview of our workflow, with the bottom left part of the illustration representing the problem structuring approach discussed.

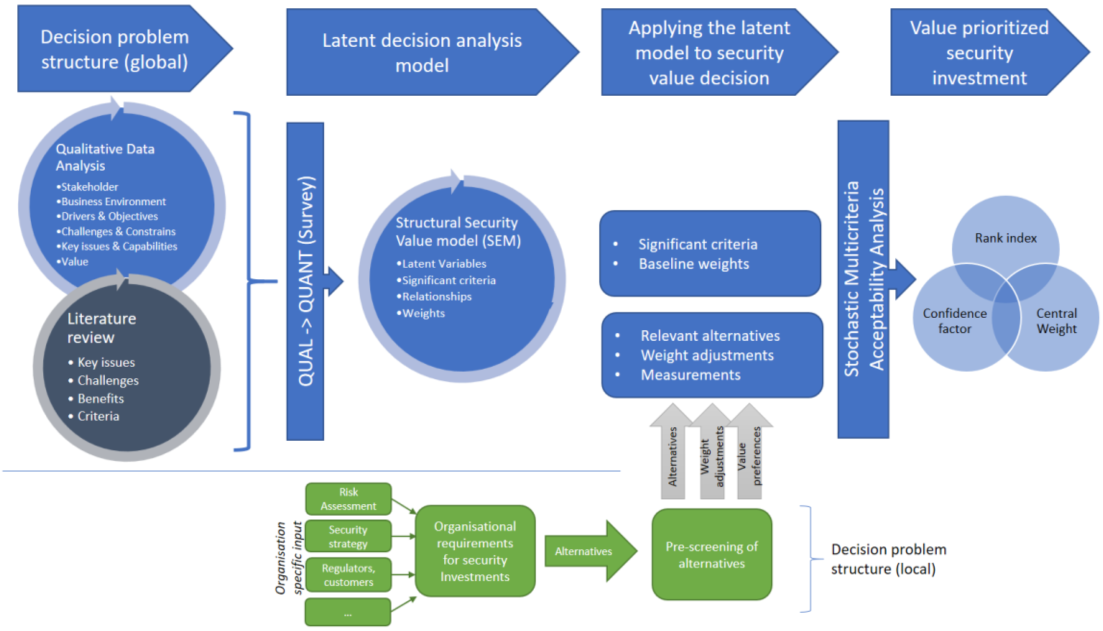


Figure 46 - MCDA model overview

For additional information on problem structuring as well as insightful views on current developments in problem structuring method (PSM) approaches, see the work of Marttunen et al. (2017).

8.3 Building the model

With an understanding of the problem structure, we can continue building the model for information security investment decisions. At an abstract level, a model represents a transformation of a complex real-world phenomenon into a simplified construct. As stated by Moretti, Öztürk, and Tsoukiàs (2016), researchers build models to better understand and better represent a given situation. This allows agents to convert inputs into meaningful outputs through the structured application of appropriate formulas (logical or mathematical). As previously described, we followed a mixed method approach to condense the complex phenomena into a simplified construct that retains the important characteristics and features.

Of the inputs to our decision model, criteria, alternatives and weights are the most important. In the MCDA context, an alternative (or option) is the object or action evaluated during a decision process. Criteria are the performance aspects of the decision that allow decision makers to evaluate an alternative in that context. The weight represents the relative importance of a criterion; it is a scaling factor that relates a criterion score to those of other criteria. A typical example for a decision problem in our case would be a set of information security controls ($A = \{a_1, \dots, a_n \mid a \in \mathbb{R}\}$), which is evaluated against a set of criteria ($C = \{c_1, .., c_n \mid c \in \mathbb{R}\}$) such as purchase cost and efficiency, where each criterion c_n is given a certain importance ($W = \{w \in \mathbb{R} \middle| w \geq 0 \; and \; \sum_{j=1}^{n} = 1\}$).

We obtained the context-relevant criteria from the SLR and qualitative analysis of the semi-structured interviews. We then empirically tested our latent model and its variables by using PLS-SEM. From the set of 60 criteria identified during our qualitative research, 20 criteria were discarded during the PLS analysis, as survey participants did not consider them to be important (i.e. insignificant loadings). The remaining criteria were tested as part of the outer model, showing satisfactory reliability (loadings and cross-loadings) and discriminant validity (Fornell–Larcker, HTMT). Establishing the criteria in this way provides us with confidence about their key considerations (Belton & Stewart, 2002), particularly ‘value reference’, ‘non-redundancy’, ‘judgmental independence’, ‘balancing completeness and conciseness’ and ‘operationality’.

In addition, we leveraged the results of our SEM calculations to obtain indicative objective weights (*W*) for each criterion based on rescaled outer construct weights. Since the dataset consists of 250 subject matter expert responses, we drew on an objective criteria weight baseline stemming from a representative sample set of real-world experiences. Security decision makers can then apply this weight baseline to obtain a relative importance distribution representative of an average organisation. Decision makers can even change or supplement these weights following other methods to establish subjective weights for each proposed criterion (e.g. through the simple multi-attribute rating technique (SMART) or swing methods). However, this may require the guidance of an experienced decision analyst and introduces wider interpretation questions, as outlined by E. U. Choo, Schoner, and Wedley (1999).

Interpretation issues, or more generally uncertainty, are common to most MCDA scenarios, but particularly so in the information security context as outlined in the findings of the qualitative interview analysis, cyber security interpretation analysis and analysis of cyber threat predictions. Research distinguishes between internal and external uncertainty in this context. Internal uncertainty commonly refers to aspects of the problem structure and inputs related to the problem. Stewart and Durbach (2016) advise that resolvable internal uncertainties (relating to imprecision or the ambiguity of meaning) are addressed as part of the problem structuring phase. Our model follows this recommendation. External uncertainties are concerned with issues outside the control of the decision maker and are more difficult to address. This type of uncertainty stems from a lack of knowledge about the consequences as well as randomness or unpredictability in relation to the processes and states of nature. It is best handled by responses of a technical nature such as market research and forecasting (Belton & Stewart, 2002).

In our problem space, we encountered such uncertainty in various forms. For instance, uncertainty in the security threat landscape is a common challenge for practitioners. Misinterpreting or ignoring changes in this area can result in the misallocation of investment in security controls that are unable to address new threats. We proposed a novel way in which to reduce uncertainty in this area through our ‘wisdom of the crowd’ threat prediction modelling approach in chapter 6. This approach helps decision makers understand future threat developments as perceived by a suitably large pool of predictions contributed from a variety of sources (the ‘crowd’, cf. 6.2), thereby improving confidence in planning for suitable security investment options.

Related to this, the activities of threat sources (i.e. the likelihood of threat) as well as potential economic impact of such an activity are key external uncertainties. Although this is a topic of ongoing research, especially in the game theory and real options area (see chapter 2), we found no evidence of a suitable quantitative approach to address it. We thus follow the view of Stewart and Durbach (2016) that elegant mathematical models inaccessible to practitioners are of little practical value. Instead, we capture the criteria measurements related to these areas based on decision maker and subject matter expert views in qualitative form.

To assemble the multicriteria decision model, we examine the criteria identified in the problem definition phase. As described previously, we identified 40 relevant criteria for assessing information security investment value. Based on feedback obtained leading up to the case studies, we consolidated two criteria (IC_IR, IC_PR) as they proved challenging to understand. All the criteria presented in Table 37 provide the measurement solicitation question alongside the baseline weight. We also provide further details about the criteria in the context of information security investment decisions and highlight references in the literature that provide additional research relevant to the criterion.

Criteria	**Baseline Weight**	**Decision Point**	**Further Detail**	**References**
FA_EXP	0.009	How well is the control investment aligned with companies' financial controller guidelines on expense type (CapEx/OpEx) or related accounting requirements?	From a financial controller perspective, investments in security controls are no different to other operational investments made by the organisation. Security control investments must follow the same rules of corporate finance controlling. When evaluating security investments, practitioners need to consider how well the controls align with the guidelines and preferences issued by their finance departments to support organisations' financial strategy and goals.	(Jensen, Schwenk, Gruschka, & Iacono, 2009; Lucas, 2014; Nepal & Jamasb, 2015)
FA_HUR	0.004	How likely is it that the control investment fulfils the hurdle rate requirements the organisation imposes on investments?	If the organisation imposes hurdle rate requirements on investments, how likely is it that the evaluated security control investment will pass the process? From chapter 5, we know that some organisations require security investment decisions to pass such hurdles and must, at least superficially, hold up to financial	(Borking, 2010; Čapko, Aksentijević, & Tijan, 2014; Gallaher, Link, & Rowe, 2008; Rowe & Gallaher, 2006)

			key performance metric analysis.	
FA_PRE	0.005	What impact will an investment in this control have on cyber insurance premiums?	Cyber insurance is becoming an increasingly important risk management tool for many organisations. While the insurance market in this space is still immature, underwriters are constantly refining their risk models to distinguish security controls that reduce impact effectively and thus lead to lower premiums. A negative impact in this context would result in an increase in premiums or prevent the organisation from obtaining cyber insurance. Investment in a control with a positive impact would reduce premiums or provide other insurance-related benefits.	(Baer & Parkinson, 2007; Bailey, 2014; Biener, Eling, & Wirfs, 2015; Hulisi, Srinivasan, & Nirup, 2011)
BP_CO	0.013	To what extent does the implementation of this security control need to be communicated or explained to end users and/or customers?	Security controls that are too demanding or complex in their use for customers (internal or external) are less desirable as the required instructions may trigger information fatigue or overload. Information overload occurs when the information-processing requirements	(Albrechtsen, 2007; D'Arcy, Herath, & Shoss, 2014; Eppler & Mengis, 2004)

			exceed the information-processing capacity. Not only is the amount of information (quantitative aspect) to be integrated crucial, so are the characteristics (qualitative aspect) of the information. As most customers and end users are not security experts, and usually do not need to be, overly complex or demanding use requirements will lead to poor value perception of the control.	
BP_CR	0.017	To what extent will the security control disrupt business processes or cause them to be more complex or complicated to deliver?	Business stakeholders generally care about business-relevant aspects; examples of this are customer priorities, ease of product use, product adoption rates, generated revenue and legal compliance. Security controls must offer a balanced value proposition considering both business process requirements and security requirements. Those controls that provide maximum security value while minimising the negative impact on business processes will contribute more value to the organisation.	(Post & Kagan, 2007; Roeckle, Schimpf, & Weidinger, 2000)

BP_OC	0.007	To what extent will investment in this control limit the organisation in regard to other business investments and opportunities?	Investment in security controls may impact the organisation's ability to invest in other projects or business opportunities. This is especially the case with comparably large security investments or where security controls account for a considerable amount of the available project budget. In this context, Srinidhi et al. (2008) explain that effective governance is underpinned by prioritisation and investment decisions about how much and where to invest. The diversion of funds away from productive assets reduces cash flow and increases the vulnerability of the firm to financial distress from cyber attacks in the long run. Security control investments (financial, resources or otherwise) should not prevent the organisation from pursuing other business opportunities.	(Srinidhi et al., 2008, 2015)
BP_BP	0.018	How will this control investment impact user morale and productivity?	Security controls may affect the ability of the workforce to deliver on their tasks or use a service. The needs of the information security	(T. C. Herath & Rao, 2009; Michaud, 2017; Post & Kagan, 2007; E

			function to protect assets must be balanced with the ability of personnel to do their job. Security controls perceived as unnecessarily intrusive to workflows (get in the way of doing work), or that are meant to monitor and control employees, can result in lower morale and productivity. Those security controls that are less perceptible, while still delivering on their security benefits, can contribute more value to the organisation.	Eugene Schultz, Proctor, Lien, & Salvendy, 2001)
BP_SC	0.044	Will this control conflict with or complement currently used security controls?	Most organisations have at least a basic set of security controls in place, either due to previous conscious investments or due to the default security features provided by their IT environment. Security controls are typically designed to provide particular security benefits; for example, firewalls provide preventative control for network-based threats, whereas network intrusion detection systems focus on detective capabilities. It is not	(Casey & Stellatos, 2008; Cavusoglu, Raghunathan, & Cavusoglu, 2009; Kantarcıoğlu & Clifton, 2005)

			uncommon for security controls to conflict. For example, data is encrypted to preserve confidentiality, which causes issues monitoring data flows for data loss prevention (DLP) reasons. Ideally, controls are deployed in a synergistic manner to complement each other and maximise their value to the organisation.	
BP_TR	0.043	How well will this control fit with the existing technology standards and infrastructure used by the organisation?	It is important to consider how security controls interact with the environment for which they are intended. A control that depends on a certain underlying technology that is not available or in use by an organisation cannot provide the full benefits expected of it. Examples include encryption methods or libraries that cause performance issues for the product and malware protection solutions that do not work with parts of the corporate technology stack. Security controls that offer compatibility with the current as well as strategic technology stack of the	(Carayannis & Turner, 2006; P.-y. Chen, Kataria, & Krishnan, 2011; Gupta & Chow, 2008)

			organisation offer higher value, both on security performance as well on reduced maintenance and support overheads.	
CC_IC	0.027	What is the expected implementation cost for this control (e.g. professional services, expenses, internal resource costs)	The direct cost of implementing a security control can be substantial and is thus an important factor for the selection of controls. The internal and external costs related to implementation commonly include professional services costs, expenses, staff resource costs, downtime of services due to implementation, provisioning and hosting costs, staff training and communications and so on. Security controls with lower implementation costs are preferable over those with high costs as they require less upfront investment and reduce sunk costs in the early phases.	(Arora, Hall, Pinto, et al., 2004; Brecht & Nowey, 2013; Čapko et al., 2014; Olifer, Goranin, Kaceniauskas, & Cenys, 2017)
CC_OB	0.042	What percentage of the overall security budget does the investment in the control	In most organisations, budgets for information security are limited and must be strictly managed to ensure they are used where they	(Anwar, Montanari, Gutierrez, & Campbell, 2009; Brecht & Nowey,

		represent?	add the most value. The proportion of the overall available budget a security control consumes plays a key role in the desirability of the control. Following the principle of layered security, a varied set of security controls is often preferred over a single control. Investing in a single control that consumes most of the available budget limits the budget and thus the choice of other controls, increases the reliance on the control and consequently risks a considerable loss in security value if the control is underperforming.	2013; Huang & Behara, 2013; Tosh, Molloy, Sengupta, Kamhoua, & Kwiat, 2015)
CC_OC	0.030	What is the expected annual cost to operate this control (ongoing operational cost)?	In their control selection process, practitioners should consider the ongoing maintenance cost of the control. Although not necessarily a security consideration, practitioners should be conscious of the cost impact over multiple periods of the control's lifespan. Those controls with higher annual costs are more susceptible to underdeliver on their value	(Brecht & Nowey, 2013; Čapko et al., 2014; Olifer et al., 2017; Thomas, 2009)

			proposition if the threat landscape shifts or if they are not properly operated and maintained. Depending on the organisation's accounting preferences, a control investment with a higher initial cost and low maintenance cost in subsequent periods may be preferred over a control with sustained high annual costs.	
CC_PP	0.026	What is the purchase price of the control?	The initial purchase price is one of the key factors in security control decisions. It represents the monetary amount an organisation pays for the selected control, considering any charges for shipping, tax, customs, discounts due to early payment, payment method and mutual benefit deals. In the context of this criterion, security controls that have a lower purchase price are more desirable than those at a higher purchase price.	(Brecht & Nowey, 2013; Čapko et al., 2014; Thomas, 2009)
CE_BR	0.052	How difficult is it to circumvent or bypass the security control?	The value a security control offers to the organisation diminishes if it can be easily circumvented. This may be due to technical	(Boss, Kirsch, Angermeier, Shingler, & Boss, 2009; Cavusoglu,

			shortcomings or the nature of the control (e.g. security awareness training). In practice, security controls that are harder to bypass are the preferred option. In many cases, practitioners can consult the testing results from trusted organisations to obtain information on the performance of certain technologies or products.	Mishra, & Srinivasan, 2005; Gu, Zhang, & Lee, 2008)
CE_DF	0.040	How likely is it that the security control will deter or discourage attacks or misbehaviour?	Although it is a more common feature of physical security, information security controls may also be chosen for their dissuasive characteristics. The use of certain security controls can have a deterrent effect on potential threat agents. Such controls are desirable as they may reduce the amount of attacks or discourage malicious behaviour due to their deterrent character. This is common with physical security controls (CCTV, guards, fences) and applies to some information security controls as well. In some cases, this	(D'Arcy, Hovav, & Galletta, 2009; T. C. Herath & Rao, 2009; Straub & Nance, 1990)

			may require proactive messaging (e.g. DDoS protection, user behavioural monitoring, FIPS 140-2 compliant encryption) to achieve the deterrent effect.	
CE_EC	0.019	How confident are we that this control performs effectively according to its intended purpose?	A common assumption by non-practitioners is that security controls work as advertised and effectively deliver the benefits promised by the solution provider. Senior practitioners with experience in this field know that this is not always the case; controls vary widely in their ability to function effectively in an organisation's environment. Technology-based security controls may suddenly stop working, affect the performance of infrastructure or platforms, underperform under heavy load, cause issues or delays to production services and so on. Security controls that efficiently deliver security benefits add more value than those controls that require constant monitoring, tuning and support to deliver the same benefits.	(Hagen, Albrechtsen, & Hovden, 2008; Kankanhalli et al., 2003; Torres, Sarriegi, Santos, & Serrano, 2006)

CE_FP	0.045	What is the false positive rate (noise-to-signal ratio) of this control?	Information security practitioners are rarely faced with simple good/bad scenarios. In many cases, it is difficult to clearly distinguish between legitimate activity (e.g. administrative activities) and malicious activity (e.g. credential abuse). This challenge is reflected in the performance of security controls as well. A high volume of type 1 errors affects trust in a control and consumes unnecessary and expensive (human) resources to verify results, thus reducing the overall value of the control. Depending on the type of control, this will have a negative impact on other areas such as staffing requirements, training requirements, business stakeholder management and security awareness training. Security controls with a low false positive rate add more value.	(Axelsson, 1999; Cavusoglu et al., 2005; Joo, Hong, & Han, 2003)
CE_PV	0.046	How quickly will the control provide its security benefits to the organisation?	There can be a considerable difference in how quickly a security investment adds value to the organisation. Compared with technical controls	(Q. Chen, Abdelwahed, & Erradi, 2014; Hawkins, 2018; van Wieren, Doerr,

			(e.g. firewalls, encryption, anti-virus software), controls that influence user behaviour or address security culture take more time until the benefits are realised. Generally, security controls that deliver value to the organisation sooner (higher velocity) are preferred as they reduce the exposure time window.	Jacobs, & Pieters, 2016)
CR_CR	0.046	How well does the security control address the identified compliance requirements?	A common reason for investment in security controls is to address compliance requirements (e.g. PCI, FISMA, HIPAA) in the organisation. Those controls that address compliance requirements add more value to the organisation. Those that help address the requirements of multiple compliance regimes add additional value compared to those which cover only one. Even if an organisation is not required to comply with information security-relevant legal and regulatory requirements, a forward-looking security practitioner will consider the shifting regulatory landscape and	(Kwon & Johnson, 2014; Pinder, 2006)

			organisation's business strategy (e.g. new markets) to future-proof security investments.	
CR_IR	0.039	How well does the security control address an immediate security issue?	Ideally, decisions to invest in security controls are proactive and planned to address risks before an impact occurs. However, investments in security controls can often be reactive and in response to urgent issues in the organisation's security stance. This is often the case following compromises of security or where the organisation has become aware of an immediate change in the threat landscape. Security controls addressing an immediate need tend to be of higher value to the organisation.	(L. A. Gordon et al., 2003; Rowe & Gallaher, 2006)
CR_KR	0.052	To what extent does the security investment address the identified risks in the organisation?	Over recent decades, information security has developed into an increasingly mature risk management discipline. Most organisations rely on some form of information risk management approach to assess and address the information security requirements in their	(Baskerville, 1991; Bojanc & Jerman-Blažič, 2013; Straub & Welke, 1998)

			environments. The result of these risk management processes usually leads to a prioritised list of known security risks that the organisation intends to manage. Investments in security controls that address known risks at the top of the list add more value to the organisation than those risks ranked lower.	
CR_UR	0.035	How well is the security investment expected to mitigate currently unknown risks in the organisation?	A key deliverable of information security risk management is to direct resources to the highest value activities under imperfect or uncertain information scenarios. Consequently, there will be unknown or yet unidentified risks that are not directly addressed by existing control investments. However, certain security controls will, due to their inherent function and characteristic, provide benefits in scenarios that have not been directly considered. Examples of this may be extensive security awareness education or machine learning-based solutions. Security controls that are	(C. H. Loch, DeMeyer, & Pich, 2011; Mahmood & Afzal, 2013; L. Wang, Jajodia, Singhal, Cheng, & Noel, 2014)

			likely to mitigate yet unknown risks can be of higher value.	
CE_AG	0.008	What impact will the security investment have on the organisation's ability to be agile in its business approach?	To allow the organisation to compete and survive in competitive and uncertain market environments, it must be agile when opportunities are identified and counteract negative market developments. To manage security risks and protect the organisation, security controls can inhibit the business' ability to execute swiftly. Controls that do not offer the right balance between managing risk and enabling the organisation to best use those important assets tend to lose value for the organisation.	(Harkins, 2016b; Imache, Izza, & Ahmed-Nacer, 2012; Zaini & Masrek, 2013)
CE_CA	0.014	To what extent does the security investment result in a competitive advantage for the organisation?	The past decade has seen a sharp rise in attention to and focus on information security and data protection by organisations, governments and the public alike. Organisations can use this attention to leverage their security investments as a business	(Ahmad, Bosua, & Scheepers, 2014; Halaweh & Fidler, 2008; Harkins, 2016a; Suh & Han, 2003)

			advantage. Security controls can contribute to this by protecting the organisation’s crown jewels, fending off industrial espionage, providing benefits through customer security enhancements (trust) above competitors’ offerings and allowing the organisation to pursue new markets or business opportunities that have high entry requirements.	
CE_CE	0.017	What is the expected impact on customers and their experience in relation to the service or product protected by the control?	Security controls can be a competitive advantage, but they can also have the opposite effect. Investing in security controls that make it more difficult for employees or customers to use the services protected by the control provides limited value. As a consequence, employees may waste time and resources finding ways in which to circumvent the control and customers may demand increased support or simply stop using the service.	(Dhillon et al., 2016; Weir, Douglas, Carruthers, & Jack, 2009; Weir, Douglas, Richardson, & Jack, 2010)
IC_CC	0.016	If an incident occurs, to what extent will the security	In the case of a serious security incident, the costs related to the notification of data subjects	(Hurtaud, Flamand, de la Vaissiere, & Hounka,

		investment help reduce costs related to customer notifications?	can be considerable, especially if a large amount of data/records have been affected. Investments in security controls that reduce the need for or cost of notification activities following an incident add additional value to the organisation.	2015; Ishaq, 2016; Romanosky, 2016)
IC_CL	0.022	If an incident occurs, to what extent will the security investment help reduce the loss of customers?	As a result of a security incident, customers may lose trust in the organisation's ability to protect their data and interests, resulting in a loss of customers (abnormal churn). Likewise, potential customers may be discouraged from signing up or converting to full customers, further amplifying the churn effect. Investment in controls that can reduce this impact provide more value to the organisation.	(Ablon, Heaton, Lavery, & Romanosky, 2016; M. Lee & Lee, 2012)
IC_MS	0.015	If an incident occurs, to what extent will the security investment help reduce the impact on market share/share price?	Security incident costs are commonly reported in the context of market share and stock price impact. Those security investments that help reduce the loss of market share are preferred. Controls directly contributing to this attribute	(Gatzlaff & McCullough, 2010; Gordon, Loeb, & Lei, 2011; Kulikova, Heil, van den Berg, & Pieters, 2012)

			are often less technical in nature and more focused on building and communicating trust. They include controls related to incident response and crisis management, crisis management exercises and training, early compromise detection and so on.	
IC_PR	0.049	If an incident occurs, to what extent will the investment help reduce the cost related to public relations or the impact on the organisation's reputation/brand?	In the event of a major security incident, the organisation may come under close scrutiny by the public, with the media and experts volunteering their version of the situation. In most cases, organisations have an interest in controlling the message to reduce the (likely negative) impact on their brand and reputation. This often requires investing considerable resources in public relations experts/campaigns. Investment in controls that reduce the cost or time taken up by such post-breach activities thus add value.	(Gatzert, Schmit, & Kolb, 2016; Hovav & Gray, 2014; Kindervag, Shey, & Mak, 2015; West, 2016)
LR_CP	0.015	To what extent will the security investment help	Following an incident, business partners may claim breach of contract on data protection	(Kindervag et al., 2015; Romanosky, Hoffman, &

		reduce contractual penalties in the case of an incident?	terms, while shareholders may claim that the company's board of directors breached its fiduciary duties or wasted company resources. Security controls that reduce the legitimacy or impact of these claims and related costs offer more value to the organisation.	Acquisti, 2014)
LR_LC	0.014	To what extent will the security investment help reduce the cost related to legal counsel and proceedings?	Where organisations suffer from major data breaches, especially if customer data is involved, there is a high likelihood of legal consequences (e.g. consumer class action lawsuits). Even if the organisation is not found to be guilty, legal and litigation costs can be considerable. Investment in controls that reduce the impact of such breaches, or their legal costs, are of higher value to the organisation.	(Cooter & Rubinfeld, 1989; Romanosky et al., 2014; Takach, 2016)
LR_LF	0.022	To what extent will the security investment help reduce the financial fines imposed by legal and	Security incidents where regulated data is affected can lead to large regulatory fines. The magnitude of fines is often scaled in line with the organisation's non-compliance with the	(Goodman & Ramer, 2007; Romanosky et al., 2014; Takach, 2016)

		regulatory bodies?	regulatory requirements and lack of security controls implemented to protect data (negligence). Controls that help reduce fines in an incident scenario add more value to the organisation.	
LR_SA	0.015	To what extent will the security investment help reduce the impact of non-financial legal and regulatory actions against the organisation?	Non-financial penalties can be severe, including preventing the organisation from being able to handle regulated data (e.g. health, personal, financial) and revoking the license to operate. Settlement agreements may mandate strict security and audit requirements to be able to continue business. Investments in security controls that reduce the likelihood of such actions enable the organisation to continue trading in the case of a security breach.	(Goodman & Ramer, 2007; Romanosky et al., 2014; Takach, 2016)
PR_PM	0.025	How much project management overheads does this security investment require for its implementation?	Many organisations utilise project management to oversee the implementation of changes in their business environment. Project management practices provide benefits in speed and raise the chance of implementation	(Barclay & Osei-Bryson, 2010; Snedaker & Rogers, 2006; Whittaker, 1999; Zhou, Vasconcelos, & Nunes, 2008)

			success but incur additional costs. In addition, project management offices can be under-resourced compared with demand for their services. Security controls that are less dependent on project management resources tend to be more desirable, as they avoid potential bottlenecks and do not tie up project manager resources that may add more value in revenue-generating projects.	
PR_SC	0.026	To what extent does the security investment depend on dedicated security staff to deliver the desired benefits?	Security controls vary widely in their requirements for specialist knowledge to be able to maximise the value they provide. Some controls can provide unusually high security benefits, but will only deliver when operated by large teams of skilled security professionals or highly specialised experts. This is a tangible, and costly, issue for many organisations due to the current worldwide shortage of information security professionals in the labour market. Investments in security controls that have	(Ben-Asher & Gonzalez, 2015; Furnell, Fischer, & Finch, 2017; Hayes & Bodhani, 2013)

			lower requirements for dedicated security staff, while still delivering the benefits desired, tend to result in higher value to the organisation.	
PR_TC	0.020	How much initial and ongoing training do employees need so that the organisation gains the desired value from this control?	The training and education of employees that operate or interact with the security control can be a considerable cost factor for the organisation. Although many controls can be implemented without training security staff or employees, this may result in a reduction in the benefits provided by the control. In the worst case, the control could become a business inhibitor, as employees do not understand how to use a particular feature, or security staff might become frustrated with their lack of ability to properly operate the control and ignore it entirely.	(Botta et al., 2007; Lockwood & Ansari, 1999)
T_AR	0.018	How resistant is the security control to the resources a typical threat source will bring to bear against the	Security control investments should take resources (computer, human, environmental) and the commitment of those resources by a threat source into consideration. For example,	(K.-K. R. Choo, 2011; LeMay, Ford, Keefe, Sanders, & Muehrcke, 2011)

		organisation's assets?	a threat source with high levels of resourcing (nation states) may be willing to initiate and sustain intensive threat events against the organisation. If the organisation's relevant threat sources are less well resourced, the security control investment should reflect this. Depending on the threat sources the organisation identified to be in scope, security controls that have higher resistance against sustained and well-resourced threats add more value. Control investments should be aligned with current and expected threat sources to avoid overspending on capabilities that are not required to adequately protect the organisation. Relevant threat sources should be taken from organisations' prioritised threat list used in risk management activities.	
T_EFF	0.013	To what extent will the security control reduce the speed at which a relevant	The speed at which a threat source can achieve the maximum negative impact (e.g. steal or tamper with intangible assets, interrupt	(Cremonini, 2005; Hutchins, Cloppert, & Amin, 2011; van Wieren

		threat source achieves the maximum negative impact?	services) is an important aspect to consider for two reasons. First, the longer an attack needs to be sustained, the higher is the resource cost for the threat source to achieve its desired goal. Second, a longer time to impact increases the chances of the organisation discovering the activity and/or allows time to organise an ordered response. Security controls that reduce the velocity with which a threat causes such an impact should be considered to be of higher value to the organisation.	et al., 2016)
T_LH	0.032	How probable is it that a relevant threat source would act against the organisation that this control would mitigate?	Based on the threat source list for the assets in scope, an assessment should be made if it is probable that a threat source would act against the organisation's assets that this control would mitigate. For example, an investment in phishing protection is unlikely to mitigate the actions taken by an insider. Security controls that address the threat events that an adversary may execute add higher value to the	(Arora, Hall, Pinto, et al., 2004; Hutchins et al., 2011; E. Eugene Schultz, 2002)

		organisation.	

Table 37 - Complete overview of the decision criteria

Soliciting criteria measurements from subject matter experts and decision makers is a key part of the MCDA process. To obtain useful measurements, the problem space and criteria must be well understood. Owing to the uncertainty inherent in many of our criteria, the most practical method for measurement solicitation in our case is a five-point Likert-type scale. The Likert scale is a psychometric scale common to a range of measurement solicitation scenarios such as surveys. It is an easily understood method of capturing the intensity of a decision maker's views on a certain criterion. For those criteria where quantitative measurements tend to be more readily available, we propose collecting responses as cardinal measures (e.g. purchase price). Additional information on measurement type and utility direction is provided in the Appendices.

Owing to the nature of the topic, the measurements for most criteria require solid knowledge about the problem space and specific organisational environment. Information security risk management is a complex topic, even without the added value dimension. We assume the decision maker to be an experienced security practitioner with a thorough understanding of the problem and the organisation to which the model is applied. However, on the matter of external uncertainties related to control efficiency, we suggest consulting resources that can provide assurance on alternative performance such as the Common Criteria Evaluation and Validation Scheme (Dusart, Sauveron, & Tai-Hoon, 2008; Kizza, 2015). Practitioners may also consider assurance services[12,13,14] and peer communities[15] to research their choice of alternatives.

Likewise, on the matter of the external threat landscape and unknown risks we refer to the previous chapter on understanding relevant developments in the threat landscape. Illustrated in Figure 46, we use SMAA to support our model with MCDA utilising the inputs described. Introduced in Lahdelma et al. (1998), SMAA represents a family of MCDA methods for problems where the uncertainty is so significant that it should be considered explicitly. Originally developed as a way in which to address

[12] NSS Labs (https://www.nsslabs.com).

[13] ICSA Labs (https://www.icsalabs.com).

[14] Anti-Malware Testing Standards Organization (https://www.amtso.org/).

[15] Gartner Peer Insights (https://www.gartner.com/reviews/).

the often cited Helsinki harbour decision problem (Hokkanen, Lahdelma, & Salminen, 1999), SMAA and its variations have subsequently been applied to a range of real-world decision problems (Lahdelma & Salminen, 2010). For example, Tervonen and Figueira (2008) provide a comprehensive overview of extensions to SMAA.

Owing to its suitability for decision processes with uncertain or inaccurate preference and criteria information, SMAA is particularly attractive for information security decision making. Information security practitioners are faced with uncertainty at almost every step of the decision process (Dlamini, Eloff, & Eloff, 2009) and thus a method that can handle inaccurate or uncertain model inputs is highly beneficial. It is able to achieve this through its inverse analysis of the space of feasible parameter values. Instead of requiring precise input parameters from decision makers, SMAA can compute multidimensional integrals over feasible parameter spaces to explore the entire weight space. As a result, it provides outputs that help decision makers identify the preferred alternative given the preference for certain criteria. However, simulation studies conclude that decisions based on the SMAA acceptability index are not recommended if the weight space is unconstrained (Durbach & Calder, 2016). In our model, we therefore constrain the weight w of each criterion c to improve the quality of the decision output. We apply the criteria weights (w) obtained from the PLS-SEM model, relax the restrictions $((w - 0.5 * w), (w + 0.5 * w))$ to allow for variation and set constraints on the weight space for the decision problem (W'):

$$W' = \left\{ w \in W \middle| w_j^{min} \leq w_j \leq w_j^{max},\ j = 1, \dots, n \right\}$$

This is to further allow for uncertainty in the established preferences. If so desired, this can be relaxed further or restricted based on the preferences of a decision maker.

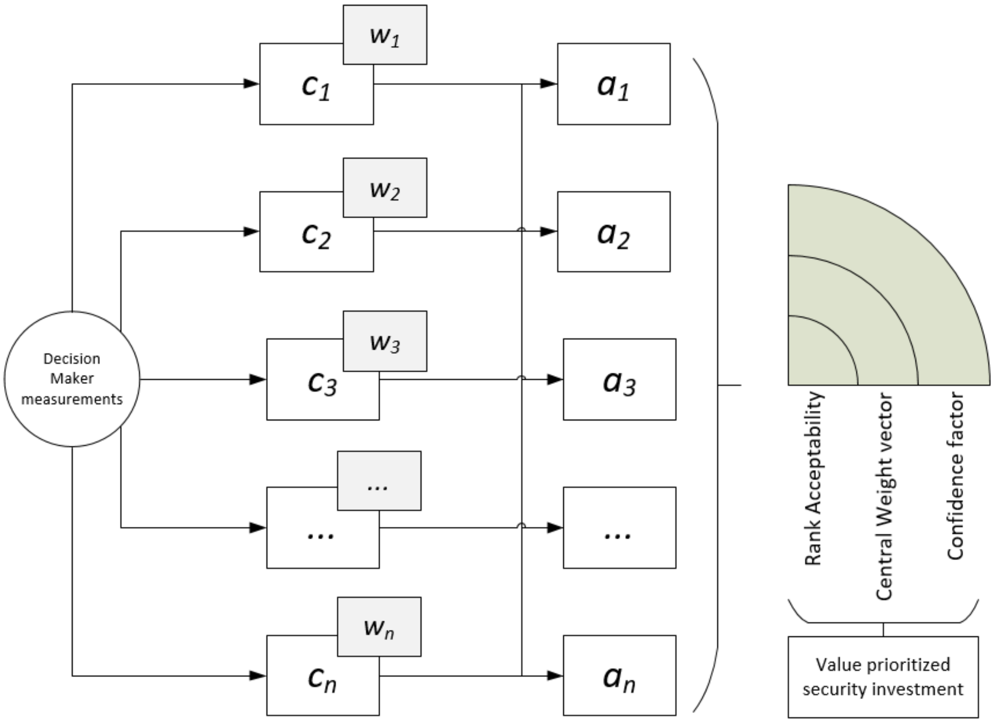


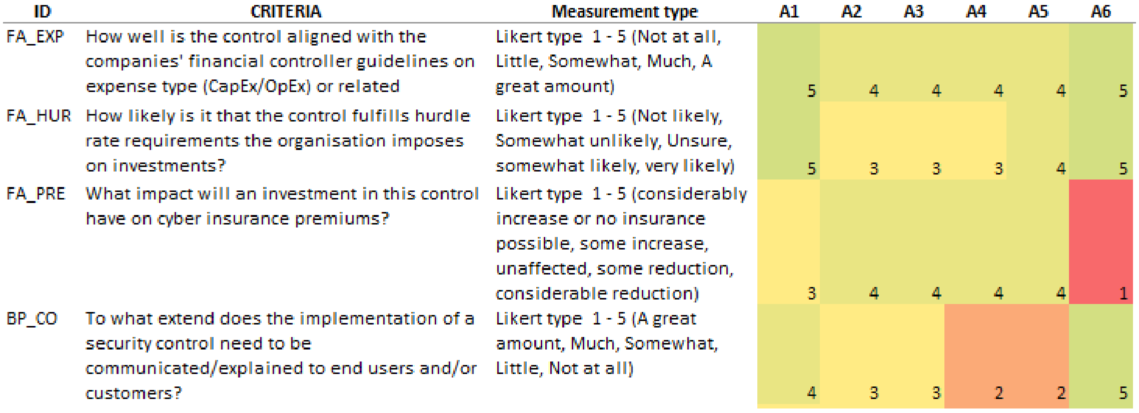
Figure 47 - Schematic overview of the criteria, weights and alternatives in an MCDA scenario (SMAA)

The outputs of the analysis are rank acceptability, central weight vectors and confidence factors for the alternatives, allowing for a value-prioritised security investment selection (Figure 47). The acceptability index shows when an alternative would become the preferred choice based on different weight valuations. The central weight vector describes the preference distribution under which an alternative achieves preferred rank, whereas the confidence factor provides guidance on whether the criteria are sufficient to make an informed decision.

8.4 Application of the model

The application of the model to real-world information security problems is straightforward, as the problem structure is defined, relevant criteria established and preference baselines available. Possible alternatives under consideration need to be prescreened as appropriate for the organisation's information security programme. That is, a shortlist of alternatives should be selected by information security practitioners based on the decision context. Although, from an implementation viewpoint, it is possible to include an exhaustive selection of alternatives in the model (e.g. all malware protection solutions available in the market), this does not seem advisable due to the evaluation efforts required by the decision maker.

Following this, the measurements of each criterion must be obtained. Ideally, decision makers would have quantitative measurements to support their decision processes. However, for most of the criteria considered in the context of information security, obtaining precise data is difficult or impossible (Algarni & Malaiya, 2016; Layton & Watters, 2014; Romanosky, 2016). To account for this, our model works with quantitative criteria measurements where such information is usually available (CC_IC, CC_OB, CC_OC, CC_PP) and qualitative inputs where not. Figure 48 illustrates the first four criteria measurements for a six-alternative decision scenario.



ID	CRITERIA	Measurement type	A1	A2	A3	A4	A5	A6
FA_EXP	How well is the control aligned with the companies' financial controller guidelines on expense type (CapEx/OpEx) or related	Likert type 1 - 5 (Not at all, Little, Somewhat, Much, A great amount)	5	4	4	4	4	5
FA_HUR	How likely is it that the control fulfills hurdle rate requirements the organisation imposes on investments?	Likert type 1 - 5 (Not likely, Somewhat unlikely, Unsure, somewhat likely, very likely)	5	3	3	3	4	5
FA_PRE	What impact will an investment in this control have on cyber insurance premiums?	Likert type 1 - 5 (considerably increase or no insurance possible, some increase, unaffected, some reduction, considerable reduction)	3	4	4	4	4	1
BP_CO	To what extend does the implementation of a security control need to be communicated/explained to end users and/or customers?	Likert type 1 - 5 (A great amount, Much, Somewhat, Little, Not at all)	4	3	3	2	2	5

Figure 48 - Performance measurement sample

We take the measurements as the input for the SMAA calculations, utilising the smaa package in the “R” software (R Core Team, 2018; Van Valkenhoef, 2018). The model input represents an $N \times n \times m$ parameter space, including the corresponding weights as shown in Table 38. The number of iterations (N) is set to 10,000, which achieves sufficient accuracy for the SMAA results (Tervonen & Lahdelma, 2007). The weight space constraints (W') are calculated by using the hitandrun package (HAR), which generates a Markov chain whose stable state converges on the uniform distribution over a polytope (Tervonen, van Valkenhoef, Baştürk, & Postmus, 2013). This provides randomised constrained weights distributed around the criteria base weight for each iteration N of the calculation.

$c_{1,..,n}$= Decision criteria $a_{1,..,m}$=Alternatives $w'_{1,\ldots,n}$= criteria weight range ($w_j^{min} \leq w_j \leq w_j^{max}$) N= Number of iterations	$\begin{array}{c} \begin{array}{cc} & \begin{array}{ccccc} c_1 & \cdots & c_j & \cdots & c_n \end{array} \\ \begin{array}{c} a_1 \\ \vdots \\ a_i \\ \vdots \\ a_m \end{array} & \begin{bmatrix} x_{11} & \cdots & x_{1j} & \cdots & x_{1n} \\ \vdots & & \vdots & & \vdots \\ x_{i1} & \cdots & x_{ij} & \cdots & x_{in} \\ \vdots & & \vdots & & \vdots \\ x_{m1} & \cdots & x_{mj} & \cdots & x_{mn} \end{bmatrix} \end{array} \\ \times N \\ \begin{array}{ccccc} w'_1 & \cdots & w'_j & \cdots & w'_n \end{array} \end{array}$

Table 38 - Simplified decision matrix

We next apply the model to two case studies based on real-world decision problems information security practitioners have faced in large or global organisations.

8.5 Case study 1

The first case study considers a decision problem in a large organisation re-evaluating the protection of the computer assets in one of their business critical revenue-generating production environment from malicious code. The environment runs on a mixed platform (Microsoft, Linux) with high requirements on availability and low latency. Owing to concerns about the latency impact, no malware protection has previously been used in this environment. Instead, risk owners have relied on compensating security controls such as network segregation to mitigate risks. However, the organisation recently suffered from a malware outbreak that caused a considerable negative impact in this environment and raised concerns over the lack of standard security controls and suitability of compensating controls. To address this risk, the information security function ran a project to research and propose possible alternatives based on practitioner experience and technology consulting services in line with the organisation's requirements (Table 39) (This case study provides a sanitised and simplified version of the original alternative portfolio.)

Alternative	**Description**	**Detail**
AVSol1	Free anti-virus solution	An anti-virus solution providing basic malware protection capabilities alongside limited

		reporting and management functionality
AVSol2	Established commercial anti-virus solution	A commercial, enterprise-class malware protection solution offering advanced capabilities, reporting, management and support across multiple technology platforms.
AVSol3	Innovative machine learning based anti-virus solution	An innovative malware protection solution applying a machine learning-based protection approach
AppWL	Application whitelisting	An application whitelisting solution that offers high malware protection capabilities by restricting computer to access only approved processes on the underlying platform
HIPS	Open source host intrusion prevention system	A centrally managed, open source host-based intrusion detection and prevention system supporting multiple technology platforms
Unchanged	No change	No additional action taken

Table 39 - Case study 1: Snapshot of alternatives

The measurements of each criterion for each alternative were obtained from subject matter experts working on the projects (see Appendix Chapter 8-2). By running the model with the relevant measurements plugged in, we obtain the rank acceptability index shown in Table 40 and Figure 49. AVSol2 is ranked first with a probability of 0.7001 at the central weight vector shown in Figure 50 (confidence factor = 1.0 (Figure 51)). As AVSol2 takes either rank 1 or rank 2 with a ~97% probability, it represents the best choice in this scenario from an information security value perspective based on the constrained central weight vector (Figure 50) providing an information security value-relevant preference baseline.

	Rank					
Alternative	1	2	3	4	5	6
AvSol1	0.2257	0.4228	0.2223	0.1090	0.0202	0.0000
AvSol2	0.7001	0.2686	0.0313	0.0000	0.0000	0.0000
AvSol3	0.0000	0.0007	0.0071	0.1447	0.8475	0.0000
AppWL	0.0017	0.0477	0.1147	0.7093	0.1266	0.0000
HIPS	0.0725	0.2602	0.6246	0.0370	0.0057	0.0000
Unchanged	0.0000	0.0000	0.0000	0.0000	0.0000	1.0000

Table 40 - Case study 1: Rank acceptability table

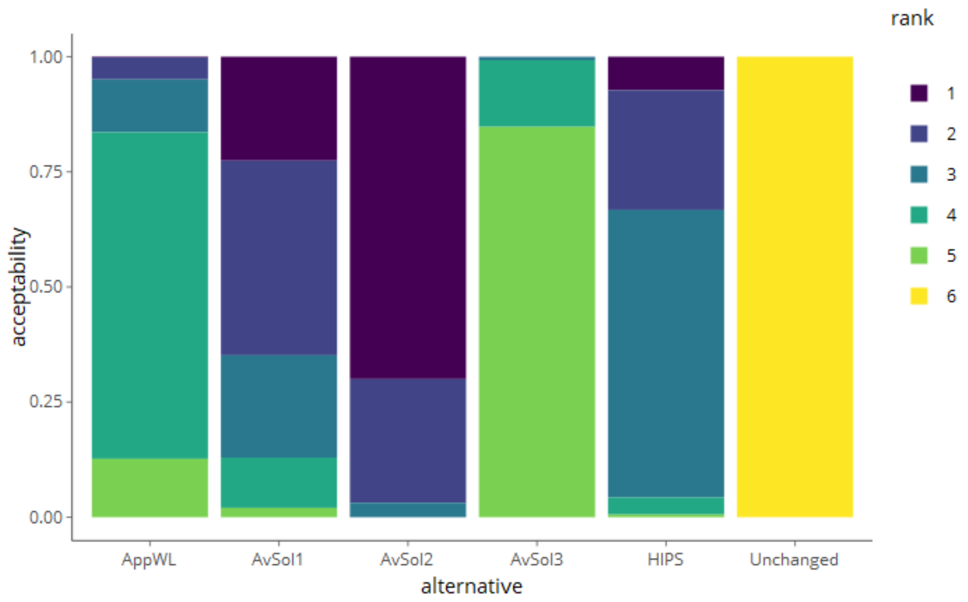


Figure 49 - Case study 1: Acceptability of alternatives

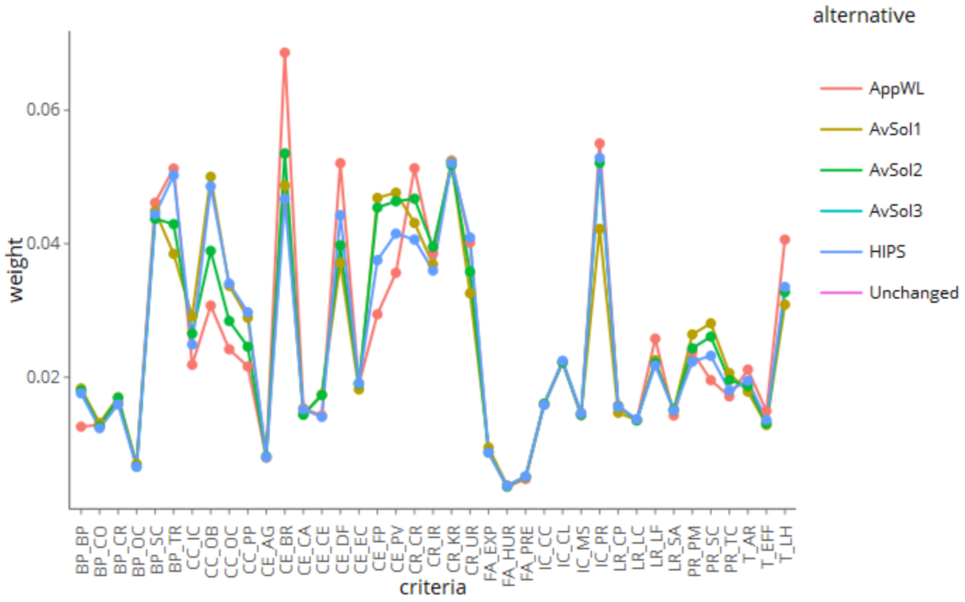


Figure 50 - Case study 1: Central weight vectors

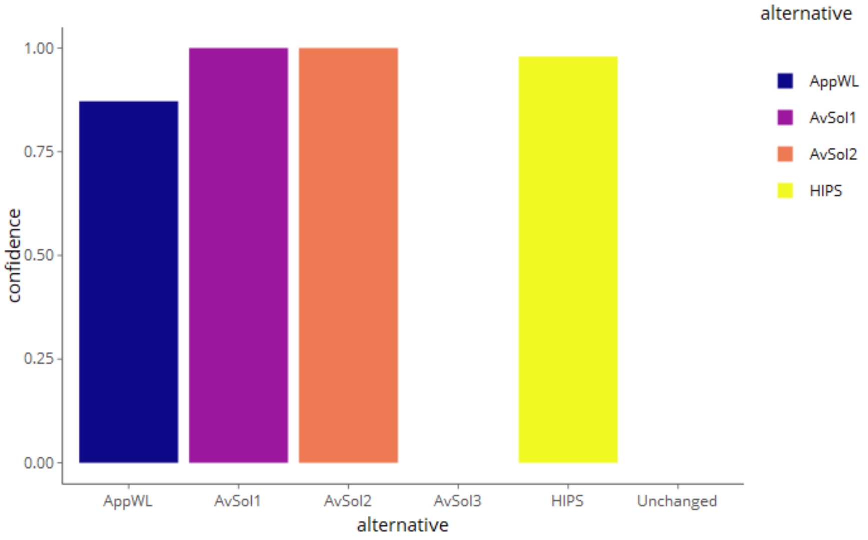


Figure 51 - Case study 1: Confidence factors

Both AVSol1 and HIPS may be ranked first if the criteria weights for the model are adjusted as shown in the respective central weight plot lines, whereas AVSol3 and Unchanged cannot under the given conditions. Figure 52 shows an isolated central weight plot illustrating this point. If the decision maker’s preference changes such that criteria such as BP_TR, CC_OB, CC_OC, CC_PP and CE_DF have a higher preference, whereas CE_FP, CE_PV, CR_CR and CR_IR are adjusted to a lower preference, the HIPS alternative may rank first. This allows decision makers to further analyse under which preference conditions an alternative becomes more or less attractive.

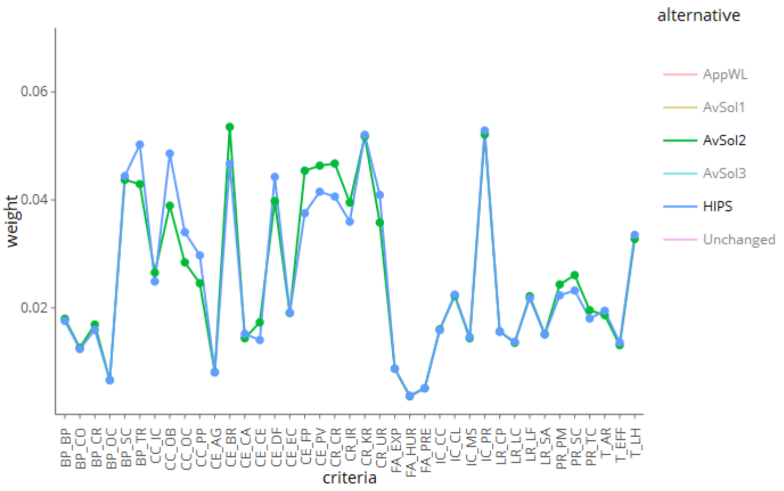


Figure 52 - Case study 1: Central weight vectors, AVSol2 vs. HIPS

The decision maker originally favoured the alternative AppWL due to its strong security and technical benefits. Based on the model output, this position was revisited. The relatively weak performance in the model was reviewed, which led to a reassessment of what the organisation considers to be important in this context. The decision maker realised that too much focus was being paid to the inherently strong features of application whitelisting, which led to overlooking less favourable criteria that would have resulted in lower-than-expected added value. The high ranking of AVSol1 was a surprise to the decision maker and encountered some criticism, mostly centred on the protective capability and manageability of the solution. However, following further discussion and review of the corresponding weight vector, it was conceded that the alternative might indeed be a valid choice in some scenarios.

8.6 Case Study 2

The second case study discusses a large organisation with less mature information security capabilities. Owing to a lack of security controls, the company suffered a second data leakage event in two years. The root cause of the data leak was established as employees being successfully ‘phished’ by cyber criminals. Following this, adversaries managed to extract sensitive information related to business strategy as well as sensitive data from the compromised employees. Senior management decided that appropriate action must be taken to avoid similar incidents in the future. To address this, the information security practitioner proposed several possible solutions tailored to the organisational and decision context (Table 41).

This case study represents a different type of decision making problem. Whereas case study 1 focused on choosing a solution for a defined technical problem, this case study illustrates how the model can be used to consider security control investments at a higher level. The decision maker can analyse a range of quite different security control options (technical, human, process) and compare these with the organisation's information security value criteria. This approach is highly beneficial, as each control option offers a different value profile to the organisation and selecting the alternative providing the best value is challenging. (Again, this case study is sanitised and simplified for presentation purposes.)

Alternative	**Description**	**Detail**
ConfHrd	Improvements in the security configuration of the organisation's email environment	Various configuration options to enhance the protection of the organisation's email environment (SPF, DKIM, DMARC). DMARC is designed to fit into an organisation's existing inbound email authentication process. It helps email receivers determine if the purported message represents what the receiver knows about the sender. If not, DMARC includes guidance on how to handle the suspicious messages
E_ATP	A commercial solution for advanced email threat protection	A cloud-based email threat protection service with advanced safeguards to identify and stop unknown malware, harmful links, suspicious

		emails and spam
aware	Security awareness with a focus on phishing attacks	A commercial security awareness training solution that helps organisations educate their employees on the risks of phishing attacks. Phishing awareness training provides employees with knowledge on how to spot and report phishing attempts and helps staff keep their skills sharp through staged exercises
DLP	A commercial DLP solution	DLP helps prevent sensitive information from leaving the organisation. DLP products mostly rely on rules to protect sensitive information so that employees cannot accidentally or maliciously share it with unauthorised parties and put the organisation at risk
Unchanged	No change	No additional action taken

Table 41 - Case study 2: Snapshot of alternatives

As in case study 1, the measurements of each criterion for each alternative were established with the decision maker. Based on the input, the standard model identifies E_ATP as the likely choice with acceptability for rank 1 at a ~0.92 probability (Table 42). This provides a strong indication that E_ATP represents the best choice in this scenario from an information security value perspective. The constrained central weight vector (Figure 54) illustrates the typical preference vector leading to this result. The relatively stark difference in the constrained weight plots for E_ATP and Aware is worth noting. This represents the difference in the nature of the control (technical vs. human) and indicates that the latter could become the preferred solution if the decision maker's preferences for certain criteria change. The decision maker may also decide that DLP is the best value alternative if the organisation is less concerned about potential workflow challenges or simply favours other criteria where this alternative is comparatively strong as shown in the central weight vector.

The result made intuitive sense to the practitioner as E_ATP had previously been independently recommended to the organisation. The result for the Aware alternative was somewhat surprising as phishing awareness training was seen as a fundamental tool to protect the organisation from such attacks. Reviewing the criteria weight vectors for the alternatives provided useful insights into the outcome and sparked discussion on several criteria (e.g. what is important to the organisation, how much inconvenience is acceptable in the current security culture, what is the right balance between protection velocity and longevity). DLP was not previously perceived to be a top choice because of concerns about costs, overheads and intrusiveness. Following the exercise, DLP is being revisited to discuss in more detail its potential to add value.

	Rank				
Alternative	1	2	3	4	5
ConfHrd	0.0000	0.0000	0.0036	0.9964	0.0000
E_ATP	0.9178	0.0822	0.0000	0.0000	0.0000
Aware	0.0012	0.2141	0.7847	0.0000	0.0000
DLP	0.0810	0.7037	0.2117	0.0036	0.0000
Unchanged	0.0000	0.0000	0.0000	0.0000	1.0000

Table 42 - Case study 2: Rank acceptability table

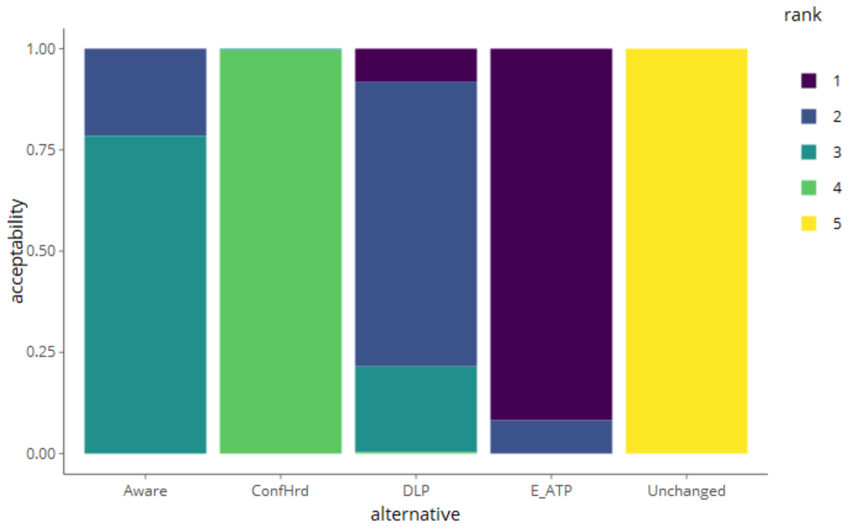


Figure 53 - Case study 2: Acceptability of alternatives

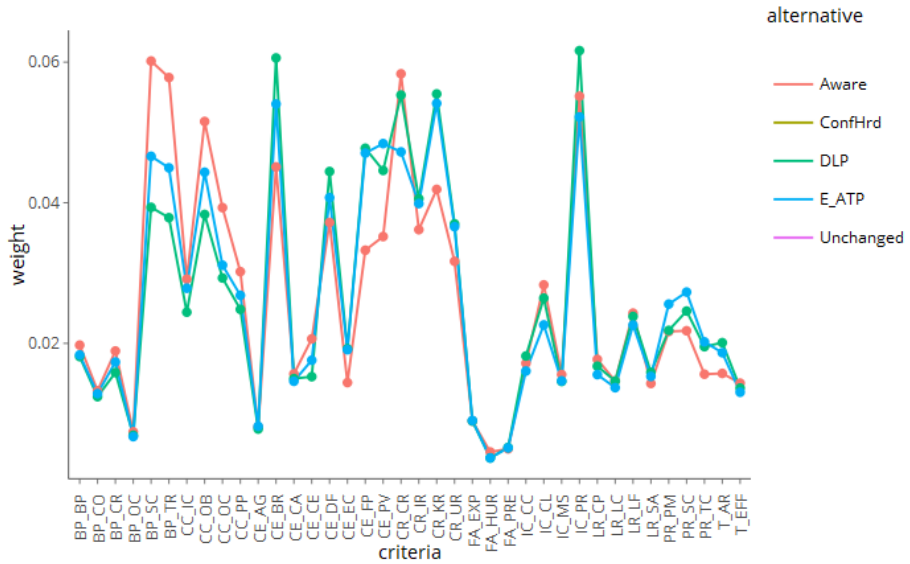


Figure 54 - Case study 2: Central weight vectors

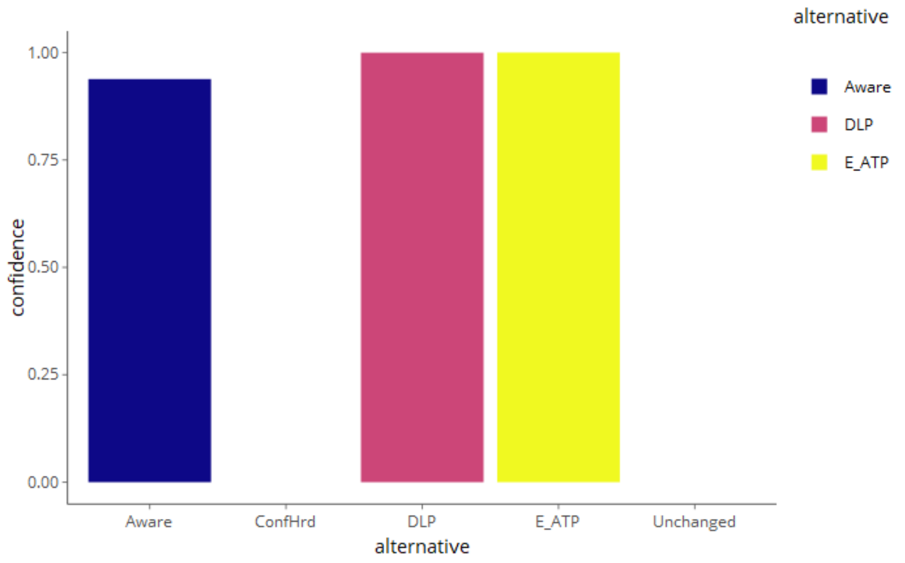


Figure 55 - Case study 2: Confidence factors

Although these case studies are only indicative, they illustrate the benefits of the model along several dimensions. We cannot claim that the decision maker enjoyed the process of providing measurements on 39 criteria for the alternatives portfolio. However, the feedback was positive insofar that the criteria were mostly easy to provide measurements for and it was helpful to approach each alternative from various value viewpoints. Some criteria were more difficult to provide measurements for, but the simplified Likert scale approach avoided this becoming an obstacle. In general, providing measurements required limited time investment and left practitioners with more confidence in their understanding of the problem space. Although the model features a relatively long list of relevant criteria, which might make it seem less attractive, each criterion represents part of what information security value means to organisations. As we saw in case study 2, decision makers may be led to focus too heavily on certain criteria while ignoring, or at least undervaluing, other criteria. The model thus ensures that all value criteria are considered, but leaves enough flexibility through weight vectors for deliberate adjustments. It not only shows which alternative provides the best value to the organisation, but also presents the criteria weights that are the basis for that outcome. Owing to its transparency, we found the model robust in application. The output includes probabilities for all feasible solutions, which means that SMAA describes how robust the model is subject to different uncertainties in the input data (Lahdelma & Salminen, 2016). By adding a control alternative ('Unchanged'), we can also observe the behaviour of each criterion/alternative combination compared with the status quo. As the implementation allows for rapid changes in weight constraints (including an unconstrained model), decision makers can then test the results against varying preferences to ensure the outcomes are suitable. As with most models, however. more real-world testing is required to study the long-term outcomes of such value-prioritised decisions (this was not possible under the time constraints of this research).

8.7 Discussion

As we derived our model from extensive research on what information security value means to practitioners and what components are considered in the academic literature, it incorporates highly relevant criteria on information security value. Unlike purely financial approaches, we take a wider view of what such value represents to an organisation. Similar to the definition of IT value by Parker, Benson, and Trainor (1988), we see the value of information security as its ability to enable and enhance business performance. It enables value-focused decision making that does not only consider the criteria common to decision processes in this area such as price, technical capability and user experience. It also includes the financial as well as non-financial aspects of the security investment decision. While the criteria related to direct costs and financials comprise a substantial amount of the weight, we found that non-financial criteria typically considered by information security practitioners outweigh them. Our model reflects this in the range of criteria condensed through empirical research as well as the criteria weight baseline derived from the primary inputs of practitioners.

However, this also introduces challenges for decision makers. While measurements of financial criteria such as direct costs tend to be readily available (e.g. CC_OC, CC_PP), measurements of other criteria are harder to establish. During our research, we investigated quantitative measurement options for the criteria set; however, we concluded that these are often infeasible for real-world application because of the efforts required to obtain precise measures. For example, it may be feasible, but certainly not straightforward, for an organisation to approximate the direct cost incurred by a specific security incident, especially since the outcomes change depending on the context. As one information security practitioner astutely stated in our interviews, *"The ranges are so wide that actually, there is very little point applying a sophisticated model to it"*.

Since the effort of obtaining such information is ill balanced with the expected benefits gained from using it in mathematical models, we opted for a qualitative approach based on simple Likert-type measurements. However, this approach introduces other challenges as the model interprets the Likert rating as a precise input. From a context perspective, this is not a problem, as the rating input is consistent across all the alternatives. Nevertheless, the decision maker should understand that the output is based on uncertain qualitative inputs and may not be as clear-cut as the charts suggest.

We tested the use of wider Likert scales and visual analogue scales to assess their potential to improve the qualitative data input and found that the Likert scale was preferred by practitioners owing to its simplicity and ease of use. The final ranking results were similar between the simple measurements and visual analogue scales, which corresponds with the findings of Guyatt, Townsend, Berman, and Keller (1987). Considering the inherent uncertainty in this problem area, we found this approach to offer benefits due to its ease of use while providing a sufficiently accurate input. Yet, the model is designed with information security professionals in mind, and the usefulness of the model output depends on sensible inputs by practitioners who have the required knowledge and experience to provide meaningful measurements.

Although little mathematical or decision theory knowledge is required, they should have extensive subject matter expertise in information security and a good knowledge of the organisation. When required, the practitioner should also consult relevant industry data.

Another important feature of the model is the criteria weight baseline, which enables information security practitioners to leverage the weights derived from real-world survey data and thus quickly and directly apply representative weights instead of conducting lengthy exercises establishing criteria weights from scratch. The model can be used in an unconstrained SMAA weight space as well, but we cannot recommend this approach. In their simulation experiment, Durbach and Calder (2016) find that the average accuracy of SMAA models is poor if no weight information is provided. Applying constrained weights considerably improves the output of the model as it refines the weight vector for each criterion according to the real-world experiences of the surveyed practitioners. Criteria weights can easily be changed by decision makers if needed in the context of the specific organisation or scenario. This can be useful if certain local criteria preferences, for example purchase cost, are well outside the global weight vector defined in the standard model. In this case, the baseline still provides useful anchor values.

Based on our research, we found that time is often an overlooked aspect when considering information security value. It is present in financial calculations (e.g. NPV) and represented in risk discussions in the form of likelihood estimates, but it tends not to be included in the overall value proposition. Our model mentions several criteria that consider the time aspect in this context. We found that practitioners deem the velocity at which a control adds the desired value (CE_PV) to be an important value aspect. This is complemented by the resilience of the control against relevant threat actor actions (T_EFF). Investing in a control that offers its full value quickly may be undesirable if it is overcome by threat actors just as quickly. In many cases, controls require ongoing investment in people resources (PR_TC) to retain the value it originally offered the organisation. In a constantly evolving space such as information security, there is no room for a ‘set and forget’ approach. Considering the efforts required to keep the control at the anticipated level is important to understand its long-term value to the organisation.

However, some time/value aspects are not considered in the model. For example, while we consider the current impact of controls on usability and business process interruption (CE_AG, BP_BP), we do not explicitly consider the shifts in that space over time. Any practitioner that tried to establish, what was then considered 'intrusive' security controls such as multifactor authentication a decade ago, understands the extent to which the notion of 'acceptable security controls' can change. Security controls once considered to be too intrusive, and as such adding poor value to organisations, may be more widely accepted and valued in the future.

8.8 Chapter summary

We presented a model for structured multicriteria decision making in the context of value-prioritised information security investments. The basis of this work is rooted in an extensive literature review as well as the primary data collected from senior practitioners on the topic of information security value aspects. We followed a mixed method research approach to incorporate our SLR output, analysis of the structured expert interviews and practitioner survey data to thoroughly structure the problem space. Based on a structured equation model, we then obtained a set of 39 criteria, as well as their outer weights, which are crucial in the context of information security value. For each criterion, detailed guidance and further references were provided to the practitioner to solicit measurements in context of the organisation and alternatives portfolio. Acknowledging the uncertainty inherent to this problem space, we used SMAA as the analysis methodology to arrive at a value-prioritised ranking of alternatives. Owing to its suitability for decision processes with uncertain or inaccurate preference and criteria information, SMAA is particularly attractive for information security decision making. Based on simple case studies, we then illustrated possible applications of the model and discussed the benefits and challenges in each scenario. The results were presented utilising the rank acceptability, central weight vector and confidence factor, clearly showing the impact of each criterion on the output.

Our model provides several benefits to security practitioners. First, it offers a reliable criteria portfolio focusing on what is relevant in the context of information security value in an organisational context. Practitioners can simply use the criteria presented in this research to ensure they consider the relevant value aspects in their decisions. Second, our preference baseline offers a real-world representation of how an average practitioner weighs each criterion in his/her decisions. Decision makers can confidently apply the baseline without conducting another weight solicitation exercise. When the baseline does not represent the preferences of an organisation, the weights can easily be adapted either individually or by configuring the weight constraints parameter. Third, the measurement input for the model is deliberately quick and simple. During our research, we heard many times that precise data are unavailable and that efforts to gather such data are better spent elsewhere. Consequently, we use simple qualitative measurements for a range of relevant criteria instead of requiring the tedious gathering of precise measurements that are not obtainable for most practitioners. Of course, where more precise data are available, practitioners can modify each criterion measurement scale to accommodate this increased accuracy. Fourth, the model output is transparent and allows decision makers to understand the underlying reasons for the final result. By using SMAA, practitioners can see clearly which criteria drive the ranking outcome. In turn, this also offers a sensitivity measure, as modifying the measurement or weight of a criterion provides feedback on the robustness of the model.

The approach presented here helps practitioners understand the value aspects of their information security investments and allows for a value-prioritised decision process. Unlike other disciplines such as wealth management, information security cannot simply maximise output along one vector. Attempting to maximise the protection of the organisation while minimising costs will not contribute the desired value; organisations are not just in business to be secure. Rather, information security must consider a multiplicity of value vectors to balance the criteria presented in this research. Merton (1994) aptly states, *"At times, the mathematics of the models become too interesting and we lose sight of the models' ultimate purpose. The mathematics of the models is precise, but the models are not, being only approximations to the complex, real world"*.

It is tempting to produce elegant mathematical models that work well with random test data. However, without the means to collect the necessary data in the real world, such models are of limited use to practitioners in the field. Instead, we propose a model that provides clear benefits in value-prioritised decision making based on uncertain information. Over time, as relevant data become more readily available in this space, the model can be improved further by replacing qualitative with quantitative measurements.

In the final chapter, we summarise the research and provide concluding thoughts on the research questions.

9 CONCLUSION

Leading into this thesis, we argued that information security value is a challenging topic for practitioners. They need to understand the current and future threats to organisations' information assets, prioritise those with the highest probability to be realised on the highest valued assets and investigate the value propositions of controls. We assumed this to be a highly complex undertaking due to the many possible factors to be considered and uncertainty about the key aspects of the decision process.

During this research, we found this assumption to be entirely true. This manifested itself early in the research through the ambiguity in the terminology used by practitioners to reference the problem space. Some practitioners use the term 'cyber security' analogous to 'information security', whereas others see a distinct difference in what these terms represent. To address this, we analysed the authoritative definition sources in the literature and isolated key components in the definition sets in chapter 3. Based on these findings, we produced an improved and representative definition of cyber security. In addition, we contributed an exhaustive set of authoritative sources for further research in this field.

In chapter 2, we turn our focus to a systematic review of the literature on economic information security decision making processes. Based on a selection of highly relevant papers describing the approaches supporting decision processes for information security investments, we identified nine common approaches and extracted the key elements of each primary study. Research on approaches related to utility maximization, game theory and real options theory showed the highest representation, with making accurate estimates and complex application being the key challenges in most studies. In general, we noted a considerable overlap of elements across all approaches which we took forward for further analysis in chapter 7.

To understand the value information security can add to organisations, we examined the impact of publicly reported information security incidents on the share prices of organisations in chapter 3. In particular, we investigated the impact of repeat data breaches by using the event study method. Our study found that a significant negative reaction follows the first reported data breach event, whereas inconclusive results were drawn about subsequent events. However, the significant results for the combined event pool led us to conclude that information security breaches result in a negative economic impact for organisations.

By extending our literature review on the key elements of information security value, we collected real-world data on this topic through semi-structured interviews with senior practitioners. Following a grounded theory approach, in chapter 5, we identified several of the key categories considered by practitioners when evaluating security investments and the value of information security programmes. This allowed us to construct a schematic overview of security investment evaluations in organisations. In addition, the detailed interview analysis was condensed into 15 principles offering a condensed view on important findings. Illustrated through a relationship network of qualitative codes, we found that decisions on security investments are made in the context of a highly complex organisational system relying on a range of business environment factors. In other words, practitioners do not view security investments as an isolated activity but rather intertwined with the wider business requirements, challenges and drivers to deliver value in context.

One of the most common challenges faced by practitioners in their strategic investment decisions is uncertainty about information security threat developments. Reducing uncertainty in this area would enable practitioners to improve decisions in the context of value-prioritised information security investments considerably, as resources would more often be spent in areas likely to encounter relevant events. To address this, we proposed an approach in chapter 6 to utilise publicised security threat predictions by subject matter experts to reduce threat landscape uncertainty. Based on a collection of security predictions for 2016, we used latent Dirichlet allocation to find 17 latent prediction topics. A year later, we revisited these prediction topics and conducted a survey collecting ex post data on security threat developments from respondents with varying expertise to evaluate the validity of the threat topics predicted. The survey results confirmed relevant threat developments for 13 of the 17 predicted threat topics with varying degrees of agreement, largely stable across the subgroups of participants. Security practitioners can thus use this approach to reduce uncertainty about value-prioritised information security investment decisions.

By combining these insights with those gained from chapters 2 and 5, we defined the structure and measurement variables in a conceptual model of information security investment decisions in chapter 7. We then used this to design a survey instrument to assess our model by using PLS-SEM. We found significant support for the inner and outer models, describing the five LVs and their directional relationship. The results showed that the underlying business environment, driving factors and threat landscape play a fundamental role in the delivery of value-oriented security investments. These are mediated by security capabilities (i.e. a security programme or function). We further found that accounting considerations have a significant indirect effect on security value, suggesting that the value of information security benefits from accounting scrutiny. The SEM analysis provided strong evidence that security capabilities have a large direct effect on the value organisations gain from information security investment. It also showed that the value outcome is strongly influenced by organisation-specific aspects that must be considered when creating security capabilities, as a cookie-cutter approach to information security will not result in the optimal value.

This finding was an important aspect of the last chapter, in which we presented an SMAA-based multicriteria decision model for information security practitioners to deliver value in their security control investments. As we derived our proposed model from extensive research on what information security value means to practitioners and which components are considered in the academic literature, it incorporates highly relevant criteria on information security value as well as their typical preferences derived from our structural outer model. We presented an end-to-end MCDA approach that incorporates the findings from our mixed method research, focusing on ease of use when practitioners make value-prioritised decisions. We then used SMAA due to its suitability for decision processes with uncertain or inaccurate preference and criteria information. This enabled us to present the results utilising rank acceptability, central weight vectors and confidence factors, allowing practitioners to clearly understand which criteria drive the outcome. Finally, we provided two case studies that illustrate the use of the model in different decision contexts.

9.1 Research questions

As our research questions have been incorporated in the thesis structure, we addressed each question in previous chapters. In this section, we provide a brief conclusion recapitulating the detailed findings.

As a reminder, we asked five research questions at the beginning of this thesis:

I. What do we mean by cyber security and how does it differ from information security?

II. Which information security value models are currently proposed to manage and evaluate information security investments in organisations?

III. What are the key factors relevant to information security investments and are these similar across models?

IV. How do information security practitioners view the topic of information security value? What factors are relevant in the real world?

V. Which of the gaps identified in the research questions would, if addressed or resolved, lead to advancement in this space?

RQ I was answered in chapter 3 in which we analysed the authoritative definitions of cyber security and provided an improved definition that combined some of the aspects of existing definitions. To understand the difference between the terms, we compared our findings with related work on information security definitions, finding that the scope of the term ‘cyber security’ is closer to that of systemic or macroeconomic concerns, whereas ‘information security’ is more focused at the organisational level.

To answer RQ II, we conducted an SLR and found 25 relevant publications discussing nine high-level approaches, as described in chapter 2. We deconstructed these papers to obtain the key aspects mentioned by the original authors relevant to their approaches. This resulted in eight categories of key elements (benefit, cost, function, impact, resource, threat, volatility, vulnerability) with several element attributes in each category. The detailed element list also served as important input for RQ III. In addition, we observed trends over time to understand which approaches have received the most attention by the research community.

Chapter 5 examined the key factors that practitioners consider in the context of information security value in their organisations. Our qualitative analysis and network relationship overview provided a detailed report on such factors and highlighted conflicts and consensus in the responses between our research and those of existing studies. Chapters 5 and 7 also addressed RQ IV by examining which factors are relevant in the real world from the viewpoints of information security practitioners. Based on our interview data, we described the building blocks of an information security investment framework that our participants assembled for us as well as condensed our findings into 15 principles that summarise practitioners' views on information security value. In chapter 7, we extended this by combining the findings of chapters 2 and 5 into a survey instrument that allowed us to collect quantitative data from a wider pool of practitioners. Based on these survey data, we tested our conceptual model by using SEM to sharpen our view of the relevant factors in this context further.

Lastly, RQ V was addressed throughout this thesis. First, we identified and bridged the gap between the meanings of cyber security and information security. Second, we noted and addressed the absence of previous work that has systematically reviewed the information security economics space in the context of evaluation models. This was a considerable gap in the research and has been addressed by this thesis. Third, we observed the gap in the research on the impact of data breach events on organisations. While there are numerous studies and research reports on this topic as outlined in chapter 3, an investigation on the impact of repeat data breaches of the same organisation was absent. Fourth, in our interviews with senior practitioners, we identified several of the issues with current information security value assessment approaches, the most critical being the challenges of uncertainty and complexity. This matched the results of our SLR. We also described an innovative way in which to reduce uncertainty about threat developments in chapter 6. We further accounted for uncertainty in our decision model by utilising an analysis model suitable for such situations (SMAA) and addressed the complexity issue by providing an empirically tested structural model that offers the most important value criteria in this context to practitioners. In addition, our model provided a weight baseline (preferences) for each criterion based on the responses of over 200 practitioners (chapter 7), which can be readily applied in practice. Lastly, we showed that our model is simple to adopt, as it does not require practitioners to collect precise figures on impact. We considered feedback that such figures are rarely available and complex mathematical models requiring such input are of limited use for most practitioners. Our model provides useful value-prioritised results based on easy-to-provide inputs, while being sufficiently flexible to integrate precise data when they are available.

9.2 Contributions

The contributions of the research are described in each chapter and are presented in this section in summarised form.

In our first of its kind systematic literature review on information security economic evaluation approaches we highlight key components and challenges extracted from relevant academic papers. We categorise and summarise the key challenges and benefits mentioned in the studies to understand the shared features in this context. We also provide a detailed breakdown of those elements authors consider to be the most relevant for their approaches and analyse commonalities across approaches. In addition, by observing trends in research over time, we identify which approaches are favoured by researchers and which are most influential. This condensed view can be used by professionals and academics to support their research in this area. We present an overview of authoritative sources and definitions of cyber security in chapter 3 which extends on current knowledge by contributing an improved definition building on these authoritative definitions. Both, the methodology and the improved definition are noteworthy contributions to the field. The approach is useful to practitioners and researchers alike as it provides a way to quickly come to an unbiased agreed definition of the term in questions. Specific for cyber security, this exercise can be repeated with relative ease, including additional definitions. The improved definition as presented by this research is useful for practitioners who require a clear definition of what cyber security means, either for business, government or legal reasons. Our definition consists of the most relevant components across 28 authoritative definitions and is as such highly representative. Chapter 4 contributes the first event study assessing impact of repeat data breaches providing early days insights into whether the market reacts differently in such situations. We observe statistically significant impact in our sample of companies being affected by data breaches more than once, leaving us to conclude that information security breaches result in a negative economic impact on organisations. Following this we conduct extensive qualitative analysis of important aspects and considerations security professionals consider in context of information security value to their organisations. We present a simplified but highly relevant framework of the organisational context in which investment decisions for information security are made in a professional environment. We found that information security investments follow a decision support process initiated by ‘driving factors’ and adjusted by ‘challenges and constraints’. Based on these driving factors and challenges, professionals select an appropriate security capability, which is then refined through corporate decision filters. Our detailed interview analysis leads to 15 principles offering a condensed view of our most important findings. In addition, we conduct a brief relationship network analysis of the coded responses to provide further detail on the hot topics in decision processes. Our analysis shows that decisions on security investments are made in the context of a highly complex organisational system relying on a range of unique business environment factors. Practitioners do not view information security investments as an isolated activity but rather intertwined with the wider business requirements, challenges and drivers to deliver value in this context. In chapter 6 we turn our focus to a novel approach for utilising security predictions towards decision support for information security programs. We illustrate how this has been successfully applied and verified for one particular year. Based on over 200 security predictions published in 2015, we use a topic modelling approach to identify 17 underlying predicted threat developments. To verify the extent to which these predicted threat topics were realized throughout 2016, we solicited backward looking opinions from respondents with varying experience of IT and information security in a survey at the start of 2017. In addition, we reviewed secondary sources to corroborate the survey results. Based on the presented findings, we conclude that the security predictions made in 2015 for 2016 did foresee notable developments in that year. This method provides an easy and cost efficient way to gain insights into anticipated thread landscape developments through topic modelling. Our results show that those threat developments covered by the collected security predictions were realised to a substantial extent. This finding indicates that security practitioners can use this approach to reduce uncertainty in the context of value-prioritised information security investment decisions. In our structural equation modelling analysis (chapter 7) we illustrate how security capabilities have a large direct effect on the value organisations gain from information security investment. We also show that the value outcome is strongly influenced by organisation-specific aspects that must be considered when creating security capabilities, as a cookie-cutter approach to information security will not result in optimal value. The conceptual model which we derived from our framework in chapter 5 and output of chapter 2, describes the underlying key constructs for assessing information security value in an organisation. Practitioners can immediately apply this insight by reflecting on the sociotechnical aspects of their environments and ensuring that their current security programmes are a good fit for their organisations. Misalignment of business environment and drivers can result in considerably worse outcomes for security value as evidenced by the large effect size. For researchers, this finding provides a statistical basis for investigating the sociotechnical aspects of information security and its relation to business outcomes in more detail. Lastly, in chapter 8 we combine our research findings and present an exhaustive set of relevant MCDA criteria with their corresponding weights in context of information security investment decisions. Acknowledging the uncertainty inherent to this problem space, we used SMAA as the analysis methodology to arrive at a value-prioritised ranking of alternatives. Our model provides several benefits to security practitioners. First, it offers a reliable criteria portfolio focusing on what is relevant in the context of information security value in an organisational context. Second, our preference baseline offers a real-world representation of how an average practitioner weighs each criterion in his/her decisions. Decision makers can confidently apply the baseline without conducting another weight solicitation exercise. Third, the measurement input for the model is deliberately quick due to simple qualitative measurements for a range of relevant criteria instead of requiring the tedious gathering of precise measurements that are not obtainable for most practitioners. Fourth, the model output is transparent and allows decision makers to understand the underlying reasons for the final result. This is crucial for practitioners to further improve and optimise decision outcomes based on shifting value views within the local and global information security environment.

9.3 Future research

The proposed model offers several avenues for improvement. It is derived from exhaustive qualitative and quantitative research at a particular point in time. Hence, future researchers should revisit the studies presented in chapters 5 and 7 to gain additional primary data, ideally from an even larger pool of participants. This would allow them to verify, optimise or improve the fundamental research findings on which our model is built. In particular, the key factors in this context and importance of such factors to practitioners may change over time and this could lead to a modification of the structural model.

Moreover, as with most models, additional real-world testing is required to examine the long-term outcomes of the value-prioritised decisions; this was not possible under the time constraints of this research. Similarly, additional research on threat predictions and developments is required to solidify the indicative positive results presented in chapter 6. This could be achieved by repeating the research for the coming year as well as extending the participant pool for the post hoc surveys. Lastly, the fast-moving area of cyber security offers rich research opportunities as mentioned in chapter 3. The term ‘cyber security’ continues to evolve as definitions are adjusted to reflect the current understanding of the space. This offers another opportunity to reassess current authoritative definitions and extend our work.

We close with a quote from a senior information security practitioner that we found fitting:

“*We are in the relationship business; we have to convince people who don’t understand information security. Make it simple, make it understandable...tell them why and show them how you can make it better. There are certain investments you have to make, to make it better*”.

REFERENCES

Ab Hamid, M., Sami, W., & Sidek, M. M. (2017). *Discriminant Validity Assessment: Use of Fornell & Larcker criterion versus HTMT Criterion.* Paper presented at the Journal of Physics: Conference Series.

Ablon, L., Heaton, P., Lavery, D. C., & Romanosky, S. (2016). *Consumer attitudes toward data breach notifications and loss of personal information*: Rand Corporation.

Ahmad, A., Bosua, R., & Scheepers, R. (2014). Protecting organizational competitive advantage: A knowledge leakage perspective. *Computers & Security, 42*, 27-39. doi:https://doi.org/10.1016/j.cose.2014.01.001

Al-Humaigani, M., & Dunn, D. B. (2003). *A model of return on investment for information systems security.* Paper presented at the Proceedings of the 46th IEEE International Midwest Symposium on Circuits & Systems, Vols 1-3, New York.

Alavi, M., & Henderson, J. C. (1981). An Evolutionary Strategy for Implementing a Decision Support System. *Management Science, 27*(11), 1309-1323. doi:10.2307/2631218

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security, 26*(4), 276-289. doi:http://dx.doi.org/10.1016/j.cose.2006.11.004

Algarni, A. M., & Malaiya, Y. K. (2016, 7-8 May 2016). *A consolidated approach for estimation of data security breach costs.* Paper presented at the 2016 2nd International Conference on Information Management (ICIM).

Allcott, H., & Gentzkow, M. (2017). Social Media and Fake News in the 2016 Election. *National Bureau of Economic Research Working Paper Series, No. 23089*. doi:10.3386/w23089

Anderson, R. (2001). *Why information security is hard - An economic perspective.* Paper presented at the 17th Annual Computer Security Applications Conference, Proceedings, Los Alamitos.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Eeten, M. G., Levi, M., . . . Savage, S. (2013). Measuring the Cost of Cybercrime. In R. Böhme (Ed.), *The Economics of Information Security and Privacy* (pp. 265-300): Springer Berlin Heidelberg.

Andoh-Baidoo, F. K., Amoako-Gyampah, K., & Osei-Bryson, K. M. (2010). How Internet Security Breaches Harm Market Value. *Security & Privacy, IEEE, 8*(1), 36-42. doi:10.1109/MSP.2010.37

Androutsopoulos, I., & Malakasiotis, P. (2010). A survey of paraphrasing and textual entailment methods. *J. Artif. Int. Res., 38*(1), 135-187.

Anwar, Z., Montanari, M., Gutierrez, A., & Campbell, R. H. (2009). Budget constrained optimal security hardening of control networks for critical cyber-infrastructures. *International Journal of Critical Infrastructure Protection, 2*(1), 13-25. doi:https://doi.org/10.1016/j.ijcip.2009.02.001

Armin, J., Thompson, B., & Kijewski, P. (2016). Cybercrime Economic Costs: No Measure No Solution. In B. Akhgar & B. Brewster (Eds.), *Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities* (pp. 135-155). Cham: Springer International Publishing.

Armstrong, S. (1980). The seer-sucker theory: The value of experts in forecasting. *Technology Review*, 16-24.

Armstrong, S., Green, K. C., & Graefe, A. (2015). Golden rule of forecasting: Be conservative. *Journal of Business Research, 68*(8), 1717-1731. doi:http://dx.doi.org/10.1016/j.jbusres.2015.03.031

Arora, A., Hall, D., Piato, C. A., Ramsey, D., & Telang, R. (2004). Measuring the risk-based value of IT security solutions. *IT Professional, 6*(6), 35-42. doi:10.1109/mitp.2004.89

Arora, A., Hall, D., Pinto, C. A., Ramsey, D., & Telang, R. (2004). *An ounce of prevention vs. a pound of cure: How can we measure the value of IT security solutions?* Retrieved from

Axelsson, S. (1999). *The base-rate fallacy and its implications for the difficulty of intrusion detection*. Paper presented at the Proceedings of the 6th ACM conference on Computer and communications security, Kent Ridge Digital Labs, Singapore.

Badenhorst, K. P., & Eloff, J. H. P. (1990). Computer security methodology: Risk analysis and project definition. *Computers & Security, 9*(4), 339-346. doi:http://dx.doi.org/10.1016/0167-4048(90)90104-2

Baer, W. S., & Parkinson, A. (2007). Cyberinsurance in IT Security Management. *IEEE Security & Privacy, 5*(3), 50-56. doi:10.1109/MSP.2007.57

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

Bailey, L. (2014). Mitigating moral hazard in cyber-risk insurance. *JL & Cyber Warfare, 3*, 1.

Baker, W. H., & Wallace, L. (2007). Is information security under control?: Investigating quality in information security management. *IEEE Security & Privacy, 5*(1).

Barclay, C., & Osei-Bryson, K.-M. (2010). Project performance development framework: An approach for developing performance criteria & measures for information systems (IS) projects. *International Journal of Production Economics, 124*(1), 272-292. doi:https://doi.org/10.1016/j.ijpe.2009.11.025

Baryshnikov, Y. (2012). *IT Security Investment and Gordon-Loeb's 1/e Rule.* Paper presented at the WEIS.

Barzilay, M. (2013, 2013-08-05). A simple definition of cybersecurity. Retrieved from http://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=296

Baskerville, R. (1991). Risk analysis: an interpretive feasibility tool in justifying information systems security. *European Journal of Information Systems, 1*(2), 121-130. doi:10.1057/ejis.1991.20

Bassellier, G., Reich, B. H., & Benbasat, I. (2001). Information Technology Competence of Business Managers: A Definition and Research Model. *Journal of*

Management Information Systems, 17(4), 159-182. doi:10.1080/07421222.2001.11045660

Baylon, C. (2014). *Challenges at the Intersection of Cyber Security and Space Security: Country and International Institution Perspectives*. Retrieved from London: http://www.chathamhouse.org/publication/challenges-intersection-cyber-security-and-space-security-country-and-international

Beecham, S., Baddoo, N., Hall, T., Robinson, H., & Sharp, H. (2006). Protocol for a systematic literature review of motivation in software engineering. *University of Hertfordshire*.

Behrend, T. S., Sharek, D. J., Meade, A. W., & Wiebe, E. N. (2011). The viability of crowdsourcing for survey research. *Behavior Research Methods, 43*(3), 800. doi:10.3758/s13428-011-0081-0

Belton, V., & Stewart, T. (2002). *Multiple criteria decision analysis: an integrated approach*: Springer Science & Business Media.

Belton, V., & Stewart, T. (2010). Problem Structuring and Multiple Criteria Decision Analysis. In M. Ehrgott, J. R. Figueira, & S. Greco (Eds.), *Trends in Multiple Criteria Decision Analysis* (pp. 209-239). Boston, MA: Springer US.

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior, 48*, 51-61. doi:https://doi.org/10.1016/j.chb.2015.01.039

Beuthe, M., Eeckhoudt, L., & Scannella, G. (2000). A practical multicriteria methodology for assessing risky public investments. *Socio-Economic Planning Sciences, 34*(2), 121-139. doi:https://doi.org/10.1016/S0038-0121(99)00021-X

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of Cyber Risk: An Empirical Analysis. *The Geneva Papers on Risk and Insurance - Issues and Practice, 40*(1), 131-158. doi:10.1057/gpp.2014.19

Biolchini, J., Mian, P., Ana, & Travassos, G. (2005). *Systematic Review in Software Engineering*. Retrieved from

Bistarelli, S., Dall'Aglio, M., & Peretti, P. (2007). Strategic games on defense trees. In T. Dimitrakos, F. Martinelli, P. Y. A. Ryan, & S. Schneider (Eds.), *Formal Aspects in Security and Trust* (Vol. 4691, pp. 1-15).

Blakley, B., McDermott, E., & Geer, D. (2001). *Information security is information risk management*. Paper presented at the Proceedings of the 2001 workshop on New security paradigms, Cloudcroft, New Mexico. http://dl.acm.org/citation.cfm?doid=508171.508187

Blatchford, C. (1995). Information security controls — Are they cost-effective? *Computer Audit Update, 1995*(Supplement 3), 11-19. doi:https://doi.org/10.1016/0960-2593(95)90080-2

Blei, D. M., Ng, A. Y., & Jordan, M. I. (2003). Latent dirichlet allocation. *J. Mach. Learn. Res., 3*, 993-1022.

Bodin, L. D., Gordon, L. A., & Loeb, M. P. (2005). Evaluating Information Security Investments Using the ANALYTIC HIERARCHY PROCESS. *Communications of the ACM, 48*(2), 79-83.

Boehmer, E., Masumeci, J., & Poulsen, A. B. (1991). Event-study methodology under conditions of event-induced variance. *Journal of Financial Economics, 30*(2), 253-272. doi:http://dx.doi.org/10.1016/0304-405X(91)90032-F

Bojanc, R., & Jerman-Blažič, B. (2008). An economic modelling approach to information security risk management. *International Journal of Information Management, 28*(5), 413-422. doi:10.1016/j.ijinfomgt.2008.02.002

Bojanc, R., & Jerman-Blažič, B. (2012). Quantitative Model for Economic Analyses of Information Security Investment in an Enterprise Information System. *Organizacija, 45*(6), 276-288. doi:10.2478/v10051-012-0027-z

Bojanc, R., & Jerman-Blažič, B. (2013). A Quantitative Model for Information-Security Risk Management. *Engineering Management Journal, 25*(2), 25-37. doi:10.1080/10429247.2013.11431972

Borking, J. (2010). Assessing investments mitigating privacy risks. *Het binnenste buiten*, 255-273.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems, 18*(2), 151-164. doi:10.1057/ejis.2009.8

Botta, D., Werlinger, R., Beznosov, K., Iverson, L., Fels, S., & Fisher, B. (2007). *Towards understanding IT security professionals and their tools*. Paper presented at the Proceedings of the 3rd symposium on Usable privacy and security, Pittsburgh, Pennsylvania, USA.

Bowman, C., & Ambrosini, V. (2000). Value Creation Versus Value Capture: Towards a Coherent Definition of Value in Strategy. *British Journal of Management, 11*(1), 1-15. doi:doi:10.1111/1467-8551.00147

Brecht, M., & Nowey, T. (2013). A Closer Look at Information Security Costs. In R. Böhme (Ed.), *The Economics of Information Security and Privacy* (pp. 3-24): Springer Berlin Heidelberg.

Brereton, P., Kitchenham, B. A., Budgen, D., Turner, M., & Khalil, M. (2007). Lessons from applying the systematic literature review process within the software engineering domain. *Journal of Systems and Software, 80*(4), 571-583. doi:http://dx.doi.org/10.1016/j.jss.2006.07.009

British Standards Institute. (2013). ISO/IEC 27001 *Information technology – Security techniques – Information security management systems – Requirements (ISO/IEC 27001:2013)* (pp. 34). Geneva: BSI Standards Limited.

Brown, S. J., & Warner, J. B. (1985). Using daily stock returns - the case of event studies. *Journal of Financial Economics, 14*(1), 3-31. doi:10.1016/0304-405x(85)90042-x

Budgen, D., & Brereton, P. (2006). *Performing systematic literature reviews in software engineering*. Paper presented at the Proceedings of the 28th international conference on Software engineering, Shanghai, China.

Buntinx, J. (2017). Top 6 Payment Card Data Breaches of 2016. Retrieved from The Merkle website: https://themerkle.com/top-6-payment-card-data-breaches-of-2016/

Burton, G. (2017). Symantec in yet-another dodgy digital certificate revocation. Retrieved from The Inquirer website: http://www.theinquirer.net/inquirer/news/3003118/symantec-in-yet-another-dodgy-digital-certificate-revocation

Calder, A. (2014). *Cyber Essentials: A Pocket Guide*: IT Governance Ltd.

Calder, J., & Durbach, I. (2015). Decision Support for Evaluating Player Performance in Rugby Union. *International Journal of Sports Science & Coaching, 10*(1), 21-37. doi:10.1260/1747-9541.10.1.21

Campbell, K., Gordon, L. A., Loeb, M. P., & Lei, Z. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security, 11*(3), 431-448.

Capko, Z., Aksentijevic, S., & Tijan, E. (2014). Economic and financial analysis of investments in information security. *2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 1550-1556. doi:10.1109/mipro.2014.6859812

Čapko, Z., Aksentijević, S., & Tijan, E. (2014, 26-30 May 2014). *Economic and financial analysis of investments in information security.* Paper presented at the 2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO).

Carayannis, E. G., & Turner, E. (2006). Innovation diffusion and technology acceptance: The case of PKI technology. *Technovation, 26*(7), 847-855. doi:https://doi.org/10.1016/j.technovation.2005.06.013

Carin, L., Cybenko, G., & Hughes, J. (2008). Cybersecurity Strategies: The QuERIES Methodology. *Computer, 41*(8), 20-26. doi:10.1109/MC.2008.295

Casey, E., & Stellatos, G. J. (2008). The impact of full disk encryption on digital forensics. *SIGOPS Oper. Syst. Rev., 42*(3), 93-98. doi:10.1145/1368506.1368519

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of Internet security breach announcements on market value: Capital market reactions for breached firms and Internet security developers. *International Journal of Electronic Commerce, 9*(1), 69-104.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). A Model for Evaluating IT Security Investments. *Communications of the ACM, 47*(7), 87-92.

Cavusoglu, H., Mishra, B., & Srinivasan, R. (2005). The Value of Intrusion Detection Systems in Information Technology Security Architecture. *Information Systems Research, 16*(1), 28-46. doi:10.1287/isre.1050.0041

Cavusoglu, H., Raghunathan, S., & Cavusoglu, H. (2009). Configuration of and Interaction Between Information Security Technologies: The Case of Firewalls and Intrusion Detection Systems. *Information Systems Research, 20*(2), 198-217. doi:10.1287/isre.1080.0180

Cavusoglu, H., Raghunathan, S., & Yue, W. T. (2008). Decision-Theoretic and Game-Theoretic Approaches to IT Security Investment. *Journal of Management Information Systems, 25*(2), 281-304.

Chandler, A. (2016). How Ransomware Became a Billion-Dollar Nightmare for Businesses. *The Atlantic*. Retrieved from https://www.theatlantic.com/business/archive/2016/09/ransomware-us/498602/

Chen, J. (2016, January 2016). Let's Encrypt Now Being Abused By Malvertisers. Retrieved from http://blog.trendmicro.com/trendlabs-security-intelligence/lets-encrypt-now-being-abused-by-malvertisers/

Chen, P.-y., Kataria, G., & Krishnan, R. (2011). Correlated Failures, Diversification, and Information Security Risk Management. *MIS Quarterly, 35*(2), 397-422. doi:10.2307/23044049

Chen, Q., Abdelwahed, S., & Erradi, A. (2014). A Model-Based Validated Autonomic Approach to Self-Protect Computing Systems. *IEEE Internet of Things Journal, 1*(5), 446-460. doi:10.1109/JIOT.2014.2349899

Choi, H., & Varian, H. A. L. (2012). Predicting the Present with Google Trends. *Economic Record, 88*, 2-9. doi:10.1111/j.1475-4932.2012.00809.x

Choo, E. U., Schoner, B., & Wedley, W. C. (1999). Interpretation of criteria weights in multicriteria decision making. *Computers & Industrial Engineering, 37*(3), 527-541. doi:https://doi.org/10.1016/S0360-8352(00)00019-X

Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security, 30*(8), 719-731. doi:https://doi.org/10.1016/j.cose.2011.08.004

Clinton, L. (2014). *Cyber-Risk Oversight*. Retrieved from http://www.nacdonline.org/Cyber

Congressional Research Service. (2014). *Cybersecurity Issues and Challenges: In Brief.* (R43831). Retrieved from https://www.fas.org/sgp/crs/misc/R43831.pdf.

Cook, D. J., Mulrow, C. D., & Haynes, R. (1997). Systematic reviews: Synthesis of best evidence for clinical decisions. *Annals of Internal Medicine, 126*(5), 376-380. doi:10.7326/0003-4819-126-5-199703010-00006

Cooter, R., & Rubinfeld, D. (1989). Economic analysis of legal disputes and their resolution. *Journal of Economic Literature, 27*(3), 1067-1097.

Corley, C., & Mihalcea, R. (2005). *Measuring the semantic similarity of texts*. Paper presented at the Proceedings of the ACL Workshop on Empirical Modeling of Semantic Equivalence and Entailment, Ann Arbor, Michigan.

Cornell University. (2016). Critically Analyzing Information Sources: Critical Appraisal and Analysis. Retrieved from http://guides.library.cornell.edu/c.php?g=31866&p=201757

Corrado, C. J. (1989). A nonparametric test for abnormal security-price performance in event studies. *Journal of Financial Economics, 23*(2), 385-395. doi:http://dx.doi.org/10.1016/0304-405X(89)90064-0

Couto, F. M., Silva, M. J., & Coutinho, P. M. (2007). Measuring semantic similarity between Gene Ontology terms. *Data & Knowledge Engineering, 61*(1), 137-152. doi:http://dx.doi.org/10.1016/j.datak.2006.05.003

Cowan, A. R. (1992). Nonparametric event study tests. *Review of Quantitative Finance and Accounting, 2*(4), 343-358. doi:10.1007/BF00939016

Crabtree, J. (2017). Russia is 'weaponizing misinformation': UK Defense Minister. *CNBC*. Retrieved from http://www.cnbc.com/2017/02/03/russia-is-weaponizing-misinformation-uk-defense-minister.html

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review, 4*(10).

Creasey, J. (2013). Cyber Security Incident Response Guide, 56. Retrieved from http://www.crest-approved.org/guidance-and-standards/cyber-security-incident-response-guide/index.html

Cremonini, M. (2005). Evaluating information security investments from attackers perspective: the return-on-attack (ROA).

Creswell, J. W. (2013). *Research design: Qualitative, quantitative, and mixed methods approaches* (4 ed.): Sage publications.

Cronin, P., Ryan, F., & Coughlan, M. (2008). Undertaking a literature review: a step-by-step approach. *British journal of nursing (Mark Allen Publishing), 17*(1), 38-43.

Cutler, D. M., Poterba, J. M., & Summers, L. H. (1989). What moves stock prices. *Journal of Portfolio Management, 15*(3), 4-12. doi:10.3905/jpm.1989.409212

CyBOK. (2018). Cyber Security Body of Knowledge Retrieved from https://www.cybok.org

D'Arcy, J., Herath, T. C., & Shoss, M. K. (2014). Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *Journal of Management Information Systems, 31*(2), 285-318. doi:10.2753/MIS0742-1222310210

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research, 20*(1), 79-98. doi:10.1287/isre.1070.0160

Davis, A. (2005). Return on security investment – proving it's worth it. *Network Security, 2005*(11), 8-10. doi:10.1016/S1353-4858(05)70301-9

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly, 13*(3), 319-340. doi:10.2307/249008

Day, S. B., & Bartels, D. M. (2008). Representation over time: the effects of temporal distance on similarity. *Cognition, 106*(3), 1504-1513. doi:10.1016/j.cognition.2007.05.013

De Marneffe, M.-C., MacCartney, B., & Manning, C. D. (2006). *Generating typed dependency parses from phrase structure parses.* Paper presented at the Proceedings of LREC.

deBondt, W. F. M., & Thaler, R. (1985). Does the Stock Market Overreact? *The Journal of Finance, 40*(3), 793-805. doi:10.2307/2327804

Demetz, L., & Bachlechner, D. (2013). To Invest or Not to Invest? Assessing the Economic Viability of a Policy and Security Configuration Management Tool. In R. Böhme (Ed.), *The Economics of Information Security and Privacy* (pp. 25-47): Springer Berlin Heidelberg.

Dengpan, L., Yonghua, J., & Mookerjee, V. (2011). Knowledge sharing and investment decisions in information security. *Decision Support Systems, 52*(1), 95-107. doi:10.1016/j.dss.2011.05.007

Denrell, J., & Fang, C. (2010). Predicting the Next Big Thing: Success as a Signal of Poor Judgment. *Manage. Sci., 56*(10), 1653-1667. doi:10.1287/mnsc.1100.1220

Department of Justice. (2014). Justice Department, Federal Trade Commission Issue Antitrust Policy Statement on Sharing Cybersecurity Information [Press release]. Retrieved from https://www.justice.gov/opa/pr/justice-department-federal-trade-commission-issue-antitrust-policy-statement-sharing

Dethlefs, R. (2015). How cyber attacks became more profitable than the drug trade. *Fortune*. Retrieved from http://fortune.com/2015/05/01/how-cyber-attacks-became-more-profitable-than-the-drug-trade/

Dey, I. (2003). *Qualitative data analysis: A user friendly guide for social scientists*: Routledge.

Dhillon, G., & Backhouse, J. (2000). Technical opinion: Information system security management in the new millennium. *Commun. ACM, 43*(7), 125-128. doi:10.1145/341852.341877

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal, 11*(2), 127-153.

Dhillon, G., Oliveira, T., Susarapu, S., & Caldeira, M. (2016). Deciding between information security and usability: Developing value based objectives. *Computers in Human Behavior, 61*, 656-666. doi:https://doi.org/10.1016/j.chb.2016.03.068

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal, 16*(3), 293-314. doi:10.1111/j.1365-2575.2006.00219.x

Diaby, V., Campbell, K., & Goeree, R. (2013). Multi-criteria decision analysis (MCDA) in health care: A bibliometric analysis. *Operations Research for Health Care, 2*(1), 20-24. doi:https://doi.org/10.1016/j.orhc.2013.03.001

Dichev, I. D., & Janes, T. D. (2003). Lunar cycle effects in stock returns. *The Journal of Private Equity, 6*(4), 8-29.

Dipietro, B. (2013). International Data Breach Laws Are All Over The Map. *Wallstreet Journal.* Retrieved from http://blogs.wsj.com/riskandcompliance/2013/09/24/international-data-breach-laws-are-all-over-the-map/

Dlamini, M. T., Eloff, J. H. P., & Eloff, M. M. (2009). Information security: The moving target. *Computers & Security, 28*(3/4), 189-198. doi:10.1016/j.cose.2008.11.007

Dor, D., & Elovici, Y. (2016). A model of the information security investment decision-making process. *Computers & Security, 63*, 1-13. doi:http://dx.doi.org/10.1016/j.cose.2016.09.006

Drury, C. (2013). *Management accounting for business* (A. Cooke Ed. 5 ed.). Andover: Cengage Learning EMEA.

Dubner, S. J. (2011). The Folly of Predictions. *Freakonomics Radio Podcast*.

Durbach, I., & Calder, J. (2016). Modelling uncertainty in stochastic multicriteria acceptability analysis. *Omega, 64*, 13-23. doi:https://doi.org/10.1016/j.omega.2015.10.015

Durbach, I., & Davis, S. (2012). Decision support for selecting a shortlist of electricity-saving options: A modified SMAA approach. *ORiON, 28*(2), 99-116.

Dusart, P., Sauveron, D., & Tai-Hoon, K. (2008). Some limits of Common Criteria certification. *context, 2*(4).

Duso, T., Gugler, K., & Yurtoglu, B. (2010). Is the event study methodology useful for merger analysis? A comparison of stock market and accounting data. *International Review of Law and Economics, 30*(2), 186-192. doi:10.1016/j.irle.2010.02.001

Dutta, A., & McCrohan, K. (2002). Management's Role in Information Security in a Cyber Economy. *California Management Review, 45*(1), 67-87. doi:10.2307/41166154

Dyckman, T., Philbrick, D., & Stephan, J. (1984). A Comparison of Event Study Methodologies Using Daily Stock Returns: A Simulation Approach. *Journal of Accounting Research, 22*, 1-30. doi:10.2307/2490855

Eden, C. (2004). Analyzing cognitive maps to help structure issues or problems. *European Journal of Operational Research, 159*(3), 673-686. doi:https://doi.org/10.1016/S0377-2217(03)00431-4

Eisenga, A., Jones, T. L., & Rodriguez, W. (2012). Investing in IT Security: How to Determine the Maximum Threshold. *International Journal of information Security and Privacy, 6*(3), 75-87. doi:10.4018/jisp.2012070104

Ekenberg, L., Oberoi, S., & Orci, I. (1995). A cost model for managing information security hazards. *Computers & Security, 14*(8), 707-717. doi:10.1016/0167-4048(95)00021-6

ENISA. (2017). *ENISA Threat Landscape Report 2016*. Retrieved from Heraklion, Greece:

Eppler, M. J., & Mengis, J. (2004). The Concept of Information Overload: A Review of Literature from Organization Science, Accounting, Marketing, MIS, and Related Disciplines. *The Information Society, 20*(5), 325-344. doi:10.1080/01972240490507974

European Network and Information Security Agency. (2012). Introduction to Return on Security Investment, 18. Retrieved from https://www.enisa.europa.eu/activities/cert/other-work/introduction-to-return-on-security-investment

Faisst, U., Prokein, O., & Wegmann, N. (2007). Ein Modell zur dynamischen Investitionsrechnung von IT-Sicherheitsmaßnahmen. *Zeitschrift für Betriebswirtschaft, 77*(5), 511-538. doi:10.1007/s11573-007-0039-y

Falessi, N., Gavrila, R., Klejnstrup Ritter, M., & Moulinos, K. (2012). *Practical Guide on Development and Execution*. Retrieved from Heraklion: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide

Fama, E. F. (1970). EFFICIENT CAPITAL MARKETS - REVIEW OF THEORY AND EMPIRICAL WORK. *Journal of Finance, 25*(2), 383-423. doi:10.2307/2325486

Fama, E. F., Fisher, L., Jensen, M. C., & Roll, R. (1969). The Adjustment of Stock Prices to New Information. *International Economic Review, 10*(1), 1-21. doi:10.2307/2525569

Farrow, S., & Szanton, J. (2016). Cybersecurity Investment Guidance: Extensions of the Gordon and Loeb Model. *Journal of Information Security, 7*(02), 15.

Ferrara, E. (2013). Determine The Value Of Information Security Assets And Liabilities — Information Security Economics 102. Retrieved from http://www.forrester.com/Determine+The+Value+Of+Information+Security+Assets+And+Liabilities+8212+Information+Security+Economics+102/fulltext/-/E-RES94861

Fielder, A., Panaousis, E. A., Malacaria, P., Hankin, C., & Smeraldi, F. (2015). Comparing Decision Support Approaches for Cyber Security Investment. *CoRR, abs/1502.05532*.

Finkle, J. (2016). Exclusive: SWIFT discloses more cyber thefts, pressures banks on security. *Reuters*. Retrieved from http://uk.reuters.com/article/us-cyber-heist-swift-idUKKCN11600C

Forrest, C. (2016). Skyrocketing Android ransomware has quadrupled over past year. Retrieved from TechRepublic website: http://www.techrepublic.com/article/skyrocketing-android-ransomware-has-quadrupled-over-past-year-says-new-report/

Furnell, S., Fischer, P., & Finch, A. (2017). Can't get the staff? The growing need for cyber-security skills. *Computer Fraud & Security, 2017*(2), 5-10. doi:https://doi.org/10.1016/S1361-3723(17)30013-1

Gallaher, M. P., Link, A. N., & Rowe, B. (2008). *Cyber Security: Economic Strategies and Public Policy Alternatives*: Edward Elgar Publishing.

Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the financial impact of IT security breaches. *Information Management & Computer Security, 11*(2), 74-83. doi:10.1108/09685220310468646

Garvey, P. R., Moynihan, R. A., & Servi, L. (2013). A macro method for measuring economic-benefit returns on cybersecurity investments: The table top approach. *Systems Engineering, 16*(3), 313-328. doi:10.1002/sys.21236

Gatzert, N., Schmit, J. T., & Kolb, A. (2016). Assessing the risks of insuring reputation risk. *Journal of Risk and Insurance, 83*(3), 641-679.

Gatzlaff, K. M., & McCullough, K. A. (2010). The Effect of Data Breaches on Shareholder Wealth. *Risk Management and Insurance Review, 13*(1), 61-83. doi:10.1111/j.1540-6296.2010.01178.x

Gbanie, S. P., Tengbe, P. B., Momoh, J. S., Medo, J., & Kabba, V. T. S. (2013). Modelling landfill location using Geographic Information Systems (GIS) and Multi-Criteria Decision Analysis (MCDA): Case study Bo, Southern Sierra Leone. *Applied Geography, 36*, 3-12. doi:https://doi.org/10.1016/j.apgeog.2012.06.013

Geisser, S. (1974). A predictive approach to the random effect model. *Biometrika, 61*(1), 101-107.

Georgiou, I. (2011). Cognitive Mapping and Strategic Options Development and Analysis (SODA) *Wiley Encyclopedia of Operations Research and Management Science*.

Gibbs, S. (2016). Dropbox hack leads to leaking of 68m user passwords on the internet. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach

Giles, K., & Hagestad, W. (2013, 4-7 June 2013). *Divided by a common language: Cyber definitions in Chinese, Russian and English.* Paper presented at the Cyber Conflict (CyCon), 2013 5th International Conference on.

Gilsinan, K., & Krishnadev, C. (2017). Did Putin Direct Russian Hacking? And Other Big Questions. *TheAtlantic*. Retrieved from https://www.theatlantic.com/international/archive/2017/01/russian-hacking-trump/510689/

Glaser, B. G., Strauss, A. L., & Strutzel, E. (1968). The Discovery of Grounded Theory; Strategies for Qualitative Research. *Nursing Research, 17*(4), 364.

GlobalData. (2017). *UK Cyber Insurance 2017*. Retrieved from https://www.globaldata.com/store/report/gdf0002ia--uk-cyber-insurance-2017/

Godwin III, J. B., Kulpin, A., Rauscher, K. F., & Yaschenko, V. (2014). *Critical Terminology Foundations 2.* Retrieved from New York: http://www.ewi.info/idea/critical-terminology-foundations-2

Gomaa, W. H., & Fahmy, A. A. (2013). A survey of text similarity approaches. *International Journal of Computer Applications, 68*(13), 13-18.

Gonçalves Fontes, E. L., & José Balloni, A. (2007). Security In Information Systems: Sociotechnical Aspects. In T. Sobh (Ed.), *Innovations and Advanced Techniques in Computer and Information Sciences and Engineering* (pp. 163-166). Dordrecht: Springer Netherlands.

Goodin, D. (2017). Online databases dropping like flies, with >10,000 falling to ransomware. Retrieved from ArsTechnica website: https://arstechnica.co.uk/security/2017/01/more-than-10000-online-databases-taken-hostage-by-ransomware-attackers/

Goodman, S. E., & Ramer, R. (2007). Global sourcing of IT services and information security: Prudence before playing. *Communications of the Association for Information Systems, 20*(1), 50.

Gordon, L. A., & Loeb, M. P. (2002a). The economics of information security investment. *ACM Trans. Inf. Syst. Secur., 5*(4), 438-457. doi:10.1145/581271.581274

Gordon, L. A., & Loeb, M. P. (2002b). Return on Information Security Investment: Myths vs Realities. *Strategic Finance, 84*(5), 26-31.

Gordon, L. A., & Loeb, M. P. (2006). Budgeting Process for Information Security Expenditures. *Communications of the ACM, 49*(1), 121-125.

Gordon, L. A., Loeb, M. P., & Lei, Z. (2011). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security, 19*(1), 33-56. doi:10.3233/JCS-2009-0398

Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2003). Information security expenditures and real options: a wait-and-see approach. *Computer Security Journal, 19*(2), 1-7.

Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2003). Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy, 22*(6), 461-485. doi:10.1016/j.jaccpubpol.2003.09.001

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). The impact of information sharing on cybersecurity underinvestment: A real options perspective. *Journal of*

Accounting and Public Policy, 34(5), 509-519. doi:http://dx.doi.org/10.1016/j.jaccpubpol.2015.05.001

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2018). Empirical Evidence on the Determinants of Cybersecurity Investments in Private Sector Firms. *Journal of Information Security, Vol.09No.02*, 21. doi:10.4236/jis.2018.92010

Gordon, L. A., Loeb, M. P., Sohail, T., Tseng, C.-Y., & Zhou, L. (2008). Cybersecurity, Capital Allocations and Management Control Systems. *European Accounting Review, 17*(2), 215-241. doi:10.1080/09638180701819972

Gordon, L. A., Loeb, M. P., & Tseng, C.-Y. (2006). Capital budgeting and informational impediments: a management accounting perspective'. *Contemporary Issues in Management Accounting*, 146-165.

Gordon, L. A., Loeb, M. P., & Zhou, L. (2016). Investing in Cybersecurity: Insights from the Gordon-Loeb Model. *Journal of Information Security, 7*(02), 49. doi:10.4236/jis.2016.72004

Government of Montenegro. (2013). *National Cyber Security Strategy for Montenegro 2013-2017*. Podgorica Retrieved from http://www.mid.gov.me/ResourceManager/FileDownload.aspx?rid=165416&rType=2&file=Cyber%20Security%20Strategy%20for%20Montenegro.pdf.

Graesser, A. C., Olney, A., Haynes, B. C., & Chipman, P. (2005). AutoTutor: A Cognitive System That Simulates a Tutor Through Mixed-Initiative Dialogue. *Cognitive systems: Human cognitive models in systems design*, 177.

Grama, J. (2010). *Legal issues in information security*: Jones & Bartlett Publishers.

Greco, S., Ehrgott, M., & Figueira, J. R. (2016). *Multiple Criteria Decision Analysis: State of the Art Surveys* (Vol. 233). New York: Springer.

Greco, S., Ishizaka, A., Matarazzo, B., & Torrisi, G. (2017). Stochastic multi-attribute acceptability analysis (SMAA): an application to the ranking of Italian regions. *Regional Studies*, 1-16. doi:10.1080/00343404.2017.1347612

Griffiths, T. L., & Steyvers, M. (2004). Finding scientific topics. *Proceedings of the National Academy of Sciences, 101*(suppl 1), 5228-5235.

Gu, G., Zhang, J., & Lee, W. (2008). BotSniffer: Detecting botnet command and control channels in network traffic.

Gupta, R. A., & Chow, M. Y. (2008, 10-13 Nov. 2008). *Performance assessment and compensation for secure networked control systems.* Paper presented at the 2008 34th Annual Conference of IEEE Industrial Electronics.

Guyatt, G. H., Townsend, M., Berman, L. B., & Keller, J. L. (1987). A comparison of Likert and visual analogue scales for measuring change in function. *Journal of Chronic Diseases, 40*(12), 1129-1133. doi:https://doi.org/10.1016/0021-9681(87)90080-4

Hagen, J. M., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security, 16*(4), 377-397.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a Silver Bullet. *Journal of Marketing Theory and Practice, 19*(2), 139-152. doi:10.2753/MTP1069-6679190202

Hair Jr, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2016). *A primer on partial least squares structural equation modeling (PLS-SEM)*: Sage Publications.

Halaweh, M., & Fidler, C. (2008, 20-22 Oct. 2008). *Security perception in e-commerce: Conflict between customer and organizational perspectives.* Paper presented at the 2008 International Multiconference on Computer Science and Information Technology.

Hall, J., Sarkani, S., & Mazzuchi, T. (2011). Impacts of organizational capabilities in information security. *Information Management & Computer Security, 19*(3), 155-176. doi:10.1108/09685221111153546

Harford, T. (2016). Why predictions are a lot like Pringles. Retrieved from http://timharford.com/2016/01/why-predictions-are-a-lot-like-pringles/

Harkins, M. W. (2016a). Looking to the Future: Emerging Security Capabilities *Managing Risk and Information Security: Protect to Enable* (pp. 117-128). Berkeley, CA: Apress.

Harkins, M. W. (2016b). A New Security Architecture to Improve Business Agility *Managing Risk and Information Security: Protect to Enable* (pp. 99-116). Berkeley, CA: Apress.

Harzing, A. W. (2007). Publish or Perish. Retrieved from http://www.harzing.com/pop.htm

Hausken, K. (2006a). Income, interdependence, and substitution effects affecting incentives for security investment. *Journal of Accounting and Public Policy, 25*(6), 629-665. doi:10.1016/j.jaccpubpol.2006.09.001

Hausken, K. (2006b). Returns to information security investment: The effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability. *Information Systems Frontiers, 8*(5), 338-349. doi:10.1007/s10796-006-9011-6

Hausken, K. (2007). Information sharing among firms and cyber attacks. *Journal of Accounting and Public Policy, 26*(6), 639-688. doi:10.1016/j.jaccpubpol.2007.10.001

Hawkins, N. (2018). Resistance, response and recovery. *Computer Fraud & Security, 2018*(2), 10-13. doi:https://doi.org/10.1016/S1361-3723(18)30014-9

Hayes, J., & Bodhani, A. (2013). Cyber security: small firms under fire [InformatIon Technology Professionalism]. *Engineering & Technology, 8*(6), 80-83. doi:10.1049/et.2013.0614

Hearst, M. A. (1999). *Untangling text data mining*. Paper presented at the Proceedings of the 37th annual meeting of the Association for Computational Linguistics on Computational Linguistics, College Park, Maryland.

Henseler, J., Dijkstra, T. K., Sarstedt, M., Ringle, C. M., Diamantopoulos, A., Straub, D. W., . . . Calantone, R. J. (2014). Common beliefs and reality about PLS: Comments on Rönkkö and Evermann (2013). *Organizational Research Methods, 17*(2), 182-209.

Henseler, J., Hubona, G., & Ray, P. A. (2016). Using PLS path modeling in new technology research: updated guidelines. *Industrial Management & Data Systems, 116*(1), 2-20. doi:doi:10.1108/IMDS-09-2015-0382

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science, 43*(1), 115-135. doi:10.1007/s11747-014-0403-8

Herath, H. S. B., & Herath, T. C. (2008). Investments in Information Security: A Real Options Perspective with Bayesian Postaudit. *Journal of Management Information Systems, 25*(3), 337-375.

Herath, H. S. B., & Herath, T. C. (2011). Copula-based actuarial model for pricing cyber-insurance policies. *Insurance Markets and Companies: Analyses and Actuarial Computations, 2*(1), 7-20.

Herath, H. S. B., & Herath, T. C. (2014). IT security auditing: A performance evaluation decision model. *Decision Support Systems, 57*, 54-63. doi:http://dx.doi.org/10.1016/j.dss.2013.07.010

Herath, T. C., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154-165. doi:https://doi.org/10.1016/j.dss.2009.02.005

Hertz, D. B. (1979). Risk analysis in capital investment. *Harvard Business Review, 57*(5), 169-181.

Hess, A. (2015). Inside the Sony Hack. *Slate*. Retrieved from http://www.slate.com/articles/technology/users/2015/11/sony_employees_on_the_hack_one_year_later.html

Higuchi, K. (2015). KH_Coder (Version 2). Retrieved from http://khc.sourceforge.net/

Hitchings, J. (1995). Deficiencies of the traditional approach to information security and the requirements for a new methodology. *Computers & Security, 14*(5), 377-383. doi:https://doi.org/10.1016/0167-4048(95)97088-R

HM Government. (2016). *National Security Strategy and Strategic Defence and Security Review 2015: annual report 2016*. Retrieved from London: https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015-annual-report-2016

Hokkanen, J., Lahdelma, R., & Salminen, P. (1999). A multiple criteria decision model for analyzing and choosing among different development patterns for the Helsinki cargo harbor. *Socio-Economic Planning Sciences, 33*(1), 1-23. doi:https://doi.org/10.1016/S0038-0121(98)00007-X

Home Office Science Advisory Council. (2018). *Understanding the costs of cyber crime*. (Research Report 96). London Retrieved from https://www.gov.uk/government/publications/understanding-the-costs-of-cyber-crime.

Hoo, K. J. S. (2000). How Much Is Enough? A Risk-Management Approach to Computer Security.

Hovav, A., & Gray, P. (2014). The Ripple Effect of an Information Security Breach Event: A Stakeholder Analysis. *Communications of the Association for Information Systems, 34*.

Huang, C. D., & Behara, R. S. (2013). Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints.

International Journal of Production Economics, 141(1), 255-268. doi:http://dx.doi.org/10.1016/j.ijpe.2012.06.022

Hulisi, Ö., Srinivasan, R., & Nirup, M. (2011). Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection. *Risk Analysis, 31*(3), 497-512. doi:doi:10.1111/j.1539-6924.2010.01478.x

Hurtaud, S., Flamand, T., de la Vaissiere, L., & Hounka, A. (2015). *Cyber Insurance as one element of the Cyber risk management strategy*. Retrieved from

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research, 1*(1), 80.

Hyman, P. (2013). Cybercrime: it's serious, but exactly how serious? *Communications of the ACM, 56*(3), 18-20.

Iheagwara, C., Blyth, A., Kevin, T., & Kinn, D. (2004). Cost effective management frameworks: the impact of IDS deployment technique on threat mitigation. *Information and Software Technology, 46*(10), 651-664. doi:10.1016/j.infsof.2003.11.004

Imache, R., Izza, S., & Ahmed-Nacer, M. (2012). An enterprise information system agility assessment model. *Computer Science and Information Systems, 9*(1), 107-133.

Ince, O. S., & Porter, R. B. (2006). INDIVIDUAL EQUITY RETURN DATA FROM THOMSON DATASTREAM: HANDLE WITH CARE! *Journal of Financial Research, 29*(4), 463-479. doi:10.1111/j.1475-6803.2006.00189.x

Information Security Forum. (2016). The ISF Standard of Good Practice for Information Security. London: ISF.

International Standards Organisation. (2014). ISO/IEC DIS 27040 (Draft) *Information technology* (pp. 115). London: BSI.

International Telecommunication Union. (2008). Overview of cybersecurity *SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY* (pp. 64).

Internet Society. (2012). Some Perspectives on Cybersecurity, 22. Retrieved from Internet Society website: http://www.internetsociety.org/doc/some-perspectives-cybersecurity-2012

ISACA. (2014). *European Cybersecurity Implementation: Overview*. Retrieved from Rolling Meadows: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/European-Cybersecurity-Implementation-Series.aspx

Ishaq, S. K. (2016). Cyberinsurance Value Generator or Cost Burden? *ISACA Journal, 5*.

Jarvis, C. B., MacKenzie, S. B., & Podsakoff, P. M. (2003). A Critical Review of Construct Indicators and Measurement Model Misspecification in Marketing and Consumer Research. *Journal of Consumer Research, 30*(2), 199-218. doi:10.1086/376806

Jensen, M., Schwenk, J., Gruschka, N., & Iacono, L. L. (2009, 21-25 Sept. 2009). *On Technical Security Issues in Cloud Computing*. Paper presented at the 2009 IEEE International Conference on Cloud Computing.

Jiang, J. J., & Conrath, D. W. (1997). *Semantic similarity based on corpus statistics and lexical taxonomy.* Paper presented at the In the Proceedings of ROCLING X, Taiwan.

Jingyue, L., & Xiaomeng, S. (2007). Making cost effective security decision with real option thinking. *2007 International Conference on Software Engineering Advances*, 1-9. doi:10.1109/test.2007.4437622

Joo, D., Hong, T., & Han, I. (2003). The neural network models for IDS based on the asymmetric costs of false negative errors and false positive errors. *Expert Systems with Applications, 25*(1), 69-75. doi:https://doi.org/10.1016/S0957-4174(03)00007-1

Kallus, N. (2014). *Predicting crowd behavior with big public data.* Paper presented at the Proceedings of the 23rd International Conference on World Wide Web.

Kang, J. (2016). Oracle's Big Data Breach Highlights Growing Security Risks of the Cloud. Retrieved from TheStreet website: https://www.thestreet.com/story/13669745/1/oracle-s-data-breach-highlights-growing-security-risks-of-the-cloud.html

Kankanhalli, A., Teo, H.-H., Tan, B. C. Y., & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management, 23*(2), 139-154. doi:https://doi.org/10.1016/S0268-4012(02)00105-6

Kannan, K., Rees, J., & Sridhar, S. (2007). Market reactions to information security breach announcements: An empirical analysis. *International Journal of Electronic Commerce, 12*(1), 69-91. doi:10.2753/jec1086-4415120103

Kantarcıoğlu, M., & Clifton, C. (2005, 2005//). *Security Issues in Querying Encrypted Data.* Paper presented at the Data and Applications Security XIX, Berlin, Heidelberg.

Kaufmann, L., & Gaeckler, J. (2015). A structured review of partial least squares in supply chain management research. *Journal of Purchasing and Supply Management, 21*(4), 259-272.

Keen, P. G. W. (1980). Adaptive design for decision support systems. *ACM SIGOA Newsletter, 1*(4-5), 15-25. doi:10.1145/1017672.1017659

Keeney, R. L. (1994). Creativity in decision making with value-focused thinking. *Sloan Management Review, 35*(4), 33.

Keeney, R. L., & Raiffa, H. (1976). Decision analysis with multiple conflicting objectives. *Wiley& Sons, New York.*

Kesswani, N., & Kumar, S. (2015). *Maintaining Cyber Security: Implications, Cost and Returns*. Paper presented at the Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research, Newport Beach, California, USA.

Khansa, L., & Liginlal, D. (2009). Valuing the flexibility of investing in security process innovations. *European Journal of Operational Research, 192*(1), 216-235. doi:10.1016/j.ejor.2007.08.039

Kindervag, J., Shey, H., & Mak, K. (2015). *Understand The Business Impact and Cost Of A Breach.* Retrieved from https://www.forrester.com/report/Understand+The+Business+Impact+And+Cost+Of+A+Breach/-/E-RES60563

Kitchenham, B., & Charters, S. (2007). *Guidelines for performing Systematic Literature Reviews in Software Engineering*. Retrieved from http://www.dur.ac.uk/ebse/resources/Systematic-reviews-5-8.pdf

Kizza, J. M. (2015). Standardization and Security Criteria: Security Evaluation of Computer Products *Guide to Computer Network Security* (pp. 345-357). London: Springer London.

Kock, N. (2011). Using WarpPLS in e-collaboration studies: An overview of five main analysis steps. *Advancing Collaborative Knowledge Environments: New Trends in E-Collaboration: New Trends in E-Collaboration, 180*.

Kock, N. (2014a). Advanced Mediating Effects Tests, Multi-Group Analyses, and Measurement Model Assessments in PLS-Based SEM. *International Journal of e-Collaboration (IJeC), 10*(1), 1-13. doi:10.4018/ijec.2014010101

Kock, N. (2014b). Stable P value calculation methods in PLS-SEM. *Laredo, TX: ScriptWarp Systems*.

Kock, N. (2017). *WarpPLS User Manual: Version 6.0* (pp. 121). Retrieved from http://cits.tamiu.edu/WarpPLS/UserManual_v_6_0.pdf

Kock, N., & Hadaya, P. (2016). Minimum sample size estimation in PLS-SEM: The inverse square root and gamma-exponential methods. *Information Systems Journal*, n/a-n/a. doi:10.1111/isj.12131

Kolari, J. W., & Pynnönen, S. (2010). Event Study Testing with Cross-sectional Correlation of Abnormal Returns. *Review of Financial Studies, 23*(11), 3996-4025. doi:10.1093/rfs/hhq072

Kong, H.-K., Kim, T.-S., & Kim, J. (2012). An analysis on effects of information security investments: a BSC perspective. *Journal of Intelligent Manufacturing, 23*(4), 941-953. doi:10.1007/s10845-010-0402-7

Kong, H., Jung, S., Lee, I., & Yeon, S.-J. (2015). Information Security and Organizational Performance: Empirical Study of Korean Securities Industry. *ETRI Journal, 37*(2), 428-437. doi:10.4218/etrij.15.0114.1042

Kothari, S., & Warner, J. (2004). The econometrics of event studies. In B. E. Eckbo (Ed.), *Handbook of Corporate Finance: Empirical Corporate Finance* (pp. 558). Amsterdam: Elsevier.

Kraemer, S., & Carayon, P. (2005). Computer and Information Security Culture: Findings from two Studies. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 49*(16), 1483-1488. doi:10.1177/154193120504901605

Krymkowski, D. H., Manning, R. E., & Valliere, W. A. (2009). Norm Crystallization: Measurement and Comparative Analysis. *Leisure Sciences, 31*(5), 403-416. doi:10.1080/01490400903199443

Kulikova, O., Heil, R., van den Berg, J., & Pieters, W. (2012, 14-16 Dec. 2012). *Cyber Crisis Management: A Decision-Support Framework for Disclosing Security Incident Information*. Paper presented at the 2012 International Conference on Cyber Security.

Kwon, J., & Johnson, M. E. (2014). Proactive versus reactive security investments in the healthcare sector. *MIS Q., 38*(2), 451-472.

Lahdelma, R., Hokkanen, J., & Salminen, P. (1998). SMAA - Stochastic multiobjective acceptability analysis. *European Journal of Operational Research, 106*(1), 137-143. doi:https://doi.org/10.1016/S0377-2217(97)00163-X

Lahdelma, R., & Salminen, P. (2010). Stochastic Multicriteria Acceptability Analysis (SMAA). In M. Ehrgott, J. R. Figueira, & S. Greco (Eds.), *Trends in Multiple Criteria Decision Analysis* (pp. 285-315). Boston, MA: Springer US.

Lahdelma, R., & Salminen, P. (2016). SMAA in Robustness Analysis. In M. Doumpos, C. Zopounidis, & E. Grigoroudis (Eds.), *Robustness Analysis in Decision Aiding, Optimization, and Analytics* (pp. 1-20). Cham: Springer International Publishing.

Layton, R., & Watters, P. A. (2014). A methodology for estimating the tangible cost of data breaches. *Journal of Information Security and Applications, 19*(6), 321-330. doi:https://doi.org/10.1016/j.jisa.2014.10.012

Leacock, C., Miller, G. A., & Chodorow, M. (1998). Using corpus statistics and WordNet relations for sense identification. *Computational Linguistics, 24*(1), 147-165.

Lee, M., & Lee, J. (2012). The impact of information security failure on customer behaviors: A study on a large-scale hacking incident on the internet. *Information Systems Frontiers, 14*(2), 375-393. doi:10.1007/s10796-010-9253-1

Lee, M. C. (2011). A novel sentence similarity measure for semantic-based expert systems. *Expert Systems with Applications, 38*(5), 6392-6399. doi:http://dx.doi.org/10.1016/j.eswa.2010.10.043

LeMay, E., Ford, M. D., Keefe, K., Sanders, W. H., & Muehrcke, C. (2011, 5-8 Sept. 2011). *Model-based Security Metrics Using ADversary VIew Security Evaluation (ADVISE).* Paper presented at the 2011 Eighth International Conference on Quantitative Evaluation of SysTems.

Leoni, P. (2008). Market power, survival and accuracy of predictions in financial markets. *Economic Theory, 34*(1), 189-206.

Lepak, D. P., Smith, K. G., & Taylor, M. S. (2007). Value Creation and Value Capture: A Multilevel Perspective. *Academy of Management Review, 32*(1), 180-194. doi:10.5465/amr.2007.23464011

Lin, D. (1998). *An information-theoretic definition of similarity.* Paper presented at the 15th International Conference on Machine Learning, Madison, WI.

Lintean, M. C. (2011). *Measuring semantic similarity: representations and methods.* The University of Memphis.

Liou, J. J. H., & Tzeng, G.-H. (2012). Comments on "Multiple criteria decision making (MCDM) methods in economics: an overview". *Technological and Economic Development of Economy, 18*(4), 672-695. doi:10.3846/20294913.2012.753489

Liu, B., & Sundar, S. S. (2018). Microworkers as research participants: Does underpaying Turkers lead to cognitive dissonance? *Computers in Human Behavior, 88*, 61-69. doi:https://doi.org/10.1016/j.chb.2018.06.017

Liu, Y., Sarabi, A., Zhang, J., Naghizadeh, P., Karir, M., Bailey, M., & Liu, M. (2015). *Cloudy with a Chance of Breach: Forecasting Cyber Security Incidents.* Paper presented at the 24th USENIX Security Symposium, Washington, D.C.

Lo, A., & MacKinlay, A. (1988). Stock market prices do not follow random walks: evidence from a simple specification test. *Review of Financial Studies, 1*(1), 41-66. doi:10.1093/rfs/1.1.41

Loch, C. H., DeMeyer, A., & Pich, M. (2011). *Managing the unknown: A new approach to managing high uncertainty and risk in projects*: John Wiley & Sons.

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems - todays reality, yesterdays understanding. *MIS Quarterly, 16*(2), 173-186. doi:10.2307/249574

Lockwood, D., & Ansari, A. (1999). Recruiting and retaining scarce information technology talent: a focus group study. *Industrial Management & Data Systems, 99*(6), 251-256. doi:10.1108/02635579910253805

Lucas, C. (2014). Identifying the Business Value of Information Security. In T. Theodosios, K. Theodoros, & K. Panagiotis (Eds.), *Approaches and Processes for Managing the Economics of Information Systems* (pp. 157-180). Hershey, PA, USA: IGI Global.

Luiijf, E., Besseling, K., & de Graaf, P. (2013). Nineteen national cyber security strategies. *International Journal of Critical Infrastructures, 9*(1), 3-31. doi:10.1504/IJCIS.2013.051608

Lv, J. J., Zhou, Y. S., & Wang, Y. Z. (2011, 15-19 April 2011). *A Multi-criteria Evaluation Method of Information Security Controls.* Paper presented at the 2011 Fourth International Joint Conference on Computational Sciences and Optimization.

MacKinlay, A. C. (1997). Event studies in economics and finance. *Journal of Economic Literature, 35*(1), 13-39.

Mahmood, T., & Afzal, U. (2013, 11-12 Dec. 2013). *Security Analytics: Big Data Analytics for cybersecurity: A review of trends, techniques and tools.* Paper presented at the 2013 2nd National Conference on Information Assurance (NCIA).

Malkiel, B. G. (2003). The efficient market hypothesis and its critics. *Journal of Economic Perspectives, 17*(1), 59-82. doi:10.1257/089533003321164958

Mäntylä, M. V., Adams, B., Khomh, F., Engström, E., & Petersen, K. (2014). On rapid releases and software testing: a case study and a semi-systematic literature review. *Empirical Software Engineering, 20*(5), 1384-1425. doi:10.1007/s10664-014-9338-4

Mardani, A., Jusoh, A., Md Nor, K., Khalifah, Z., Zakwan, N., & Valipour, A. (2015). Multiple criteria decision-making techniques and their applications – a review of the literature from 2000 to 2014. *Economic Research-Ekonomska Istraživanja, 28*(1), 516-571. doi:10.1080/1331677X.2015.1075139

Martin, D. I., & Berry, M. W. (2007). Mathematical foundations behind latent semantic analysis. *Handbook of latent semantic analysis*, 35-56.

Marttunen, M., Lienert, J., & Belton, V. (2017). Structuring problems for Multi-Criteria Decision Analysis in practice: A literature review of method combinations. *European Journal of Operational Research, 263*(1), 1-17. doi:https://doi.org/10.1016/j.ejor.2017.04.041

Mathews, L. (2017). 2016 Saw An Insane Rise In The Number Of Ransomware Attacks. *Forbes*. Retrieved from Forbes website: https://www.forbes.com/sites/leemathews/2017/02/07/2016-saw-an-insane-rise-in-the-number-of-ransomware-attacks/#2215c9c258dc

Matsuura, K. (2009). Productivity Space of Information Security in an Extension of the Gordon-Loeb's Investment Model *Managing Information Risk and the Economics of Security* (pp. 99-119): Springer US.

McGoogan, C. (2016). Yahoo hack: What you need to know about the biggest data breach in history. *The Telegraph*. Retrieved from http://www.telegraph.co.uk/technology/2016/12/15/yahoo-hack-need-know-biggest-data-breach-history/

McHugh, M. L. (2013). The chi-square test of independence. *Biochemia medica, 23*(2), 143-149.

McLellan, C. (2016). Cybersecurity predictions for 2016: How are they doing? *Cyberwar and the Future of Cybersecurity*. Retrieved from ZDNet website: http://www.zdnet.com/article/cybersecurity-predictions-for-2016-how-are-they-doing/

McNiff, J., & Whitehead, A. J. (2011). *All You Need to Know About Action Research*: Sage Publications Ltd.

Meho, L. I., & Yang, K. (2006). A new era in citation and bibliometric analyses: Web of Science, Scopus, and Google Scholar. *arXiv preprint cs/0612132*.

Merton, R. (1994). Influence of mathematical models in finance on practice: past, present and future. *Philosophical Transactions of the Royal Society of London. Series A: Physical and Engineering Sciences, 347*(1684), 451.

Meyer, D., Hornik, K., & Feinerer, I. (2008). Text mining infrastructure in R. *Journal of Statistical Software, 25*(5), 1-54.

Miaoui, Y., Boudriga, N., & Abaoub, E. (2015). *Insurance versus investigation driven approach for the computation of optimal security investment.* Paper presented at the Pacific Asia Conference on Information Systems Singapore.

Michaud, S. R. (2017). *Examining the Negative Impact of Information Security on Worker Performance.* Northcentral University.

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook*: Sage.

Miller, G. A. (1995). WordNet: a lexical database for English. *Commun. ACM, 38*(11), 39-41. doi:10.1145/219717.219748

Miller, L. T., & Park, C. S. (2002). Decision Making Under Uncertainty—Real Options to the Rescue? *The Engineering Economist, 47*(2), 105-150. doi:10.1080/00137910208965029

Mishra, S. (2015). Organizational objectives for information security governance: a value focused assessment. *Information and Computer Security, 23*(2), 122-144. doi:10.1108/ics-02-2014-0016

Mitroff, I. I., & Featheringham, T. R. (1974). On systemic problem solving and the error of the third kind. *Behavioral Science, 19*(6), 383-393. doi:doi:10.1002/bs.3830190605

Mizzi, A. (2010). Return on Information Security Investment-The Viability Of An Anti-Spam Solution In A Wireless Environment. *IJ Network Security, 10*(1), 18-24.

Moore, T., Dynes, S., & Chang, F. R. (2015). Identifying How Firms Manage Cybersecurity Investment, 32. Retrieved from http://blog.smu.edu/research/files/2015/10/SMU-IBM.pdf

Moretti, S., Öztürk, M., & Tsoukiàs, A. (2016). Preference Modelling. In S. Greco, M. Ehrgott, & J. R. Figueira (Eds.), *Multiple Criteria Decision Analysis: State of the Art Surveys* (pp. 43-95). New York, NY: Springer New York.

Morgan, L. (2016, 2016-12-19). List of data breaches and cyber attacks in 2016 – 3.1 billion records leaked. Retrieved from https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2016-1-6-billion-records-leaked/

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2013). Cyber-risk decision models: To insure IT or not? *Decision Support Systems, 56*, 11-26. doi:http://dx.doi.org/10.1016/j.dss.2013.04.004

Muncaster, P. (2017). Cyber Insurance Adoption Soared 50% in 2016. *InfoSecurity Magazine*. Retrieved from https://www.infosecurity-magazine.com/news/cyber-insurance-adoption-soared-50/

Murgia, M., & Ralph, O. (2016). Boom in cyber attack insurance predicted to gather pace. *Financial Times*. Retrieved from https://www.ft.com/content/a767e518-c91e-11e6-8f29-9445cac8966f

Murray, M. (2017). The top mobile threats of 2016. Retrieved from ITProPortal website: http://www.itproportal.com/features/the-top-mobile-threats-of-2016/

Nakov, P., Popova, A., & Mateev, P. (2001). Weight functions impact on LSA performance. *EuroConference RANLP*, 187-193.

National Institute of Standards and Technology. (2012). *Computer Security Incident Handling Guide*. Gaithersburg.

Nepal, R., & Jamasb, T. (2015). Incentive regulation and utility benchmarking for electricity network security. *Economic Analysis and Policy, 48*, 117-127. doi:https://doi.org/10.1016/j.eap.2015.11.001

Neubauer, T., & Hartl, C. (2009, 1-3 June 2009). *On the Singularity of Valuating IT Security Investments.* Paper presented at the Computer and Information Science, 2009. ICIS 2009. Eighth IEEE/ACIS International Conference on.

Neumann, J. v., & Morgenstern, O. (1964). Theory of games and economic behaviour. *Theory of games and economic behaviour.*(3rd edition), 641 pp.

Nordrum, A. (2016). What Is a Distributed Denial-of-Service Attack and How Did It Break Twitter? *IEEE Spectrum*. Retrieved from IEEE.com website: http://spectrum.ieee.org/tech-talk/telecom/security/what-is-a-distributed-denialofservice-attack-and-how-did-it-break-twitter

Olifer, D., Goranin, N., Kaceniauskas, A., & Cenys, A. (2017). Controls-based approach for evaluation of information security standards implementation costs. *Technological and Economic Development of Economy, 23*(1), 196-219. doi:10.3846/20294913.2017.1280558

Ou Yang, Y.-P., Shieh, H.-M., Leu, J.-D., & Tzeng, G.-H. (2009). A VIKOR-based multiple criteria decision method for improving information security risk. *International Journal of Information Technology & Decision Making, 08*(02), 267-287. doi:10.1142/s0219622009003375

Pandey, P., & Snekkenes, E. A. (2014, 1-5 Sept. 2014). *Applicability of Prediction Markets in Information Security Risk Management.* Paper presented at the 2014 25th International Workshop on Database and Expert Systems Applications.

Paolacci, G., & Chandler, J. (2014). Inside the Turk:Understanding Mechanical Turk as a Participant Pool. *Current Directions in Psychological Science, 23*(3), 184-188. doi:10.1177/0963721414531598

Parker, M. M., Benson, R. J., & Trainor, H. E. (1988). *Information economics: linking business performance to information technology*. Englewood Cliffs, NJ: Prentice-Hall

Passeri, P. (2013). 2013 Top 20 Breaches. Retrieved from http://hackmageddon.com/2013/12/30/2013-top-20-breaches/

Patell, J. M. (1976). Corporate Forecasts of Earnings Per Share and Stock Price Behavior: Empirical Test. *Journal of Accounting Research, 14*(2), 246-276. doi:10.2307/2490543

Pawlak, P., & Wendling, C. (2013). Trends in cyberspace: can governments keep up? *Environment Systems and Decisions, 33*(4), 536-543. doi:10.1007/s10669-013-9470-5

Pearson, K. (1900). X. On the criterion that a given system of deviations from the probable in the case of a correlated system of variables is such that it can be reasonably supposed to have arisen from random sampling. *Philosophical Magazine Series 5, 50*(302), 157-175. doi:10.1080/14786440009463897

Pettigrew, J., & Ryan, J. (2012). Making Successful Security Decisions: A Qualitative Evaluation. *IEEE Security & Privacy, 10*(1), 60-68. doi:10.1109/MSP.2011.128

Phillips, P. P., & Phillips, J. J. (2010). Return on Investment *Handbook of Improving Performance in the Workplace: Volumes 1-3* (pp. 823-846): John Wiley & Sons, Inc.

Pinder, P. (2006). Preparing Information Security for legal and regulatory compliance (Sarbanes–Oxley and Basel II). *Information Security Technical Report, 11*(1), 32-38. doi:https://doi.org/10.1016/j.istr.2005.12.003

Pinsonneault, A., & Kraemer, K. (1993). Survey Research Methodology in Management Information Systems: An Assessment. *Journal of Management Information Systems, 10*(2), 75-105. doi:10.1080/07421222.1993.11518001

Ponemon Institute. (2014). *Cost of Data Breach Study*. Retrieved from Michigan: http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/

Ponemon Institute. (2017). *Cost of Cyber Crime Study 2017*. Retrieved from https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

Pons, P., & Latapy, M. (2005). Computing Communities in Large Networks Using Random Walks. In p. Yolum, T. Güngör, F. Gürgen, & C. Özturan (Eds.), *Computer and Information Sciences - ISCIS 2005* (Vol. 3733, pp. 284-293): Springer Berlin Heidelberg.

Ponweiser, M. (2012). *Latent Dirichlet Allocation in R.* University of Economics and Business, Vienna. Retrieved from http://epub.wu.ac.at/3558/

Porter, M. F. (1997). An algorithm for suffix stripping. In J. Karen Sparck & W. Peter (Eds.), *Readings in information retrieval* (pp. 313-316): Morgan Kaufmann Publishers Inc.

Post, G. V., & Kagan, A. (2007). Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computers & Security, 26*(3), 229-237. doi:https://doi.org/10.1016/j.cose.2006.10.004

Purser, S. A. (2004). Improving the ROI of the security management process. *Computers & Security, 23*(7), 542-546. doi:10.1016/j.cose.2004.09.004

R Core Team. (2018). R: A language and environment for statistical computing (Version 3.5.0). Vienna, Austria: R Foundation for Statistical Computing. Retrieved from https://www.R-project.org

Ramakrishnan, N., Butler, P., Muthiah, S., Self, N., Khandpur, R., Saraf, P., . . . Korkmaz, G. (2014). *'Beating the news' with EMBERS: forecasting civil unrest using open source indicators.* Paper presented at the Proceedings of the 20th ACM SIGKDD international conference on Knowledge discovery and data mining.

Rantapuska, T., & Ihanainen, O. (2008). Knowledge use in ICT investment decision making of SMEs. *Journal of Enterprise Information Management, 21*(6), 585-596. doi:doi:10.1108/17410390810911195

Rashid, A., Danezis, G., Chivers, H., Lupu, E., Martin, A., Lewis, M., & Peersman, C. (2018). Scoping the Cyber Security Body of Knowledge. *IEEE Security & Privacy, 16*(3), 96-102. doi:10.1109/MSP.2018.2701150

Rice, R. E., & Danowski, J. A. (1993). Is It Really Just Like a Fancy Answering Machine? Comparing Semantic Networks of Different Types of Voice Mail Users. *Journal of Business Communication, 30*(4), 369-397. doi:10.1177/002194369303000401

Richter, N. F., Sinkovics, R. R., Ringle, C. M., & Schlägel, C. (2016). A critical look at the use of SEM in international business research. *International Marketing Review, 33*(3), 376-404. doi:doi:10.1108/IMR-04-2014-0148

Riek, M., Böhme, R., & Moore, T. (2014). *Understanding the influence of cybercrime risk on the e-service adoption of European Internet users.* Paper presented at the Workshop on the Economics of Information Security (WEIS).

Rigdon, E. E. (2016). Choosing PLS path modeling as analytical method in European management research: A realist perspective. *European Management Journal, 34*(6), 598-605.

Ringle, C. M., Sarstedt, M., & Straub, D. (2012). A critical look at the use of PLS-SEM in MIS Quarterly.

Roeckle, H., Schimpf, G., & Weidinger, R. (2000). *Process-oriented approach for role-finding to implement role-based security administration in a large industrial organization*. Paper presented at the Proceedings of the fifth ACM workshop on Role-based access control, Berlin, Germany.

Roldán, J., L., & J. Sánchez-Franco, M. (2012). Variance-Based Structural Equation Modeling: Guidelines for Using Partial Least Squares in Information Systems Research. In M. Manuel, G. Ovsei, L. S. Annette, & R. Mahesh (Eds.), *Research Methodologies, Innovations and Philosophies in Software Systems Engineering and Information Systems* (pp. 193-221). Hershey, PA, USA: IGI Global.

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*. doi:10.1093/cybsec/tyw001

Romanosky, S., Hoffman, D., & Acquisti, A. (2014). Empirical analysis of data breach litigation. *Journal of Empirical Legal Studies, 11*(1), 74-104.

Rönkkö, M., & Evermann, J. (2013). A critical examination of common beliefs about partial least squares path modeling. *Organizational Research Methods, 16*(3), 425-448.

Ross, S. A. (1995). Uses, Abuses, and Alternatives to the Net-Present-Value Rule. *Financial Management, 24*(3), 96-102. doi:10.2307/3665561

Rowe, B. R., & Gallaher, M. P. (2006). *Private sector cyber security investment strategies: An empirical analysis.* Paper presented at the The fifth workshop on the economics of information security (WEIS06).

Rue, R., & Pfleeger, S. L. (2009). Making the Best Use of Cybersecurity Economic Models. *Security & Privacy, IEEE, 7*(4), 52-60. doi:10.1109/MSP.2009.98

Rus, V. (2014). *Opportunities and Challenges in Semantic Similarity.* Paper presented at the 2014.

Rus, V., & Lintean, M. (2012). *A comparison of greedy and optimal assessment of natural language student input using word-to-word similarity metrics*. Paper presented at the Proceedings of the Seventh Workshop on Building Educational Applications Using NLP, Montreal, Canada.

Rus, V., Lintean, M., Moldovan, C., Baggett, W., Niraula, N., & Morgan, B. (2012). *The similar corpus: A resource to foster the qualitative understanding of semantic similarity of texts.* Paper presented at the Semantic Relations II: Enhancing Resources and Applications, The 8th Language Resources and Evaluation Conference (LREC 2012), May.

Rus, V., Lintean, M. C., Banjade, R., Niraula, N. B., & Stefanescu, D. (2013). *SEMILAR: The Semantic Similarity Toolkit.* Paper presented at the ACL (Conference System Demonstrations).

Ryan, G. W., & Bernard, H. R. (2003). Techniques to Identify Themes. *Field Methods, 15*(1), 85-109. doi:10.1177/1525822x02239569

Saaty, T. L. (1994). How to Make a Decision: The Analytic Hierarchy Process. *Interfaces, 24*(6), 19-43. doi:doi:10.1287/inte.24.6.19

Saint-Hilary, G., Cadour, S., Robert, V., & Gasparini, M. (2017). A simple way to unify multicriteria decision analysis (MCDA) and stochastic multicriteria acceptability analysis (SMAA) using a Dirichlet distribution in benefit-risk assessment. *Biom J, 59*(3), 567-578. doi:10.1002/bimj.201600113

Salton, G. (1963). Associative Document Retrieval Techniques Using Bibliographic Information. *J. ACM, 10*(4), 440-457. doi:10.1145/321186.321188

Sanchez, G. (2015). The saga of PLS. Retrieved from http://sagaofpls.github.io

Sauper, C., & Barzilay, R. (2009). *Automatically generating Wikipedia articles: a structure-aware approach*. Paper presented at the Proceedings of the Joint Conference of the 47th Annual Meeting of the ACL and the 4th International Joint Conference on Natural Language Processing of the AFNLP: Volume 1 - Volume 1, Suntec, Singapore.

Sawik, T. (2013). Selection of optimal countermeasure portfolio in IT security planning. *Decision Support Systems, 55*(1), 156-164. doi:10.1016/j.dss.2013.01.001

SC Magazine. (2016). Payment fraud growth accelerates. Retrieved from SC Magazine website: https://www.scmagazineuk.com/payment-fraud-growth-accelerates/article/532167/

Schneier, B. (2016). Why you should side with Apple, not the FBI, in the San Bernardino iPhone case. Retrieved from Washington Post website: https://www.washingtonpost.com/posteverything/wp/2016/02/18/why-you-should-side-with-apple-not-the-fbi-in-the-san-bernardino-iphone-case/

Schneier, B. (2017, 2017-02-13). IoT Ransomware against Austrian Hotel. Retrieved from https://www.schneier.com/blog/archives/2017/01/iot_ransomware_.html

Scholes, M., & Williams, J. (1977). Estimating betas from nonsynchronous data. *Journal of Financial Economics, 5*(3), 309-327. doi:http://dx.doi.org/10.1016/0304-405X(77)90041-1

Schultz, E. E. (2002). A framework for understanding and predicting insider attacks. *Computers & Security, 21*(6), 526-531. doi:https://doi.org/10.1016/S0167-4048(02)01009-X

Schultz, E. E., Proctor, R. W., Lien, M.-C., & Salvendy, G. (2001). Usability and security an appraisal of usability issues in information security methods. *Computers & Security, 20*(7), 620-634.

Serrano, O., Dandurand, L., & Brown, S. (2014). *On the Design of a Cyber Security Data Sharing System*. Paper presented at the Proceedings of the 2014 ACM Workshop on Information Sharing &#38; Collaborative Security, Scottsdale, Arizona, USA.

Shapiro, S. S., & Wilk, M. B. (1965). An Analysis of Variance Test for Normality (Complete Samples). *Biometrika, 52*(3/4), 591-611. doi:10.2307/2333709

Sheen, J. N. (2010). Fuzzy Economic Decision-models for Information Security Investment. *Proceedings of the 9th WSEAS International Conference on Instrumentation Measurement Circuits and Systems (IMCAS 2010). Instrumentation, Measurement, Circuits and Systems*, 141-147.

Shetty, S., McShane, M., Zhang, L., Kesan, J. P., Kamhoua, C. A., Kwiat, K., & Njilla, L. L. (2018). Reducing Informational Disadvantages to Improve Cyber Risk Management†. *The Geneva Papers on Risk and Insurance - Issues and Practice, 43*(2), 224-238. doi:10.1057/s41288-018-0078-3

Shirtz, D., & Elovici, Y. (2011). Optimizing investment decisions in selecting information security remedies. *Information Management & Computer Security, 19*(2), 95-112. doi:10.1108/09685221111143042

Shuchih Ernest, C., & Chienta Bruce, H. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems, 106*(3), 345-361. doi:10.1108/02635570610653498

Sievert, C., & Shirley, K. E. (2014). *LDAvis: A method for visualizing and interpreting topics*. Paper presented at the Proceedings of the Workshop on Interactive Language Learning, Visualization, and Interfaces.

Siponen, M. T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *SIGMIS Database, 38*(1), 60-80. doi:10.1145/1216218.1216224

Smedinghoff, T. J. (2006). Where we're Headed–New Developments and Trends in the Law of Information Security. *Wildman Harrold News & Publications*. Retrieved from http://www.edwardswildman.com/Files/Publication/867dcafd-bdae-4c33-affe-68ea2ad688c0/Presentation/PublicationAttachment/2e55edad-c12b-4e47-8df8-e31faee30d1b/Where_We're_Headed_-_New_Developments_and_Trends_in_the_Law_of_Information_Securit.pdf

Snedaker, S., & Rogers, R. (2006). *IT Security Project Management Handbook*: Syngress Publishing.

SocioCultural Research Consultants LLC. (2016). Dedoose (Version 7.5.9). Los Angeles, CA. Retrieved from www.dedoose.com

Sonnenreich, W., Albanese, J., & Stout, B. (2006). Return on security investment (ROSI) - A practical quantitative model. *Journal of Research and Practice in Information Technology, 38*(1), 45-56.

Sowell, T. (2014). *Basic Economics* (5th ed.). New York: Basic Books.

Sparck Jones, K. (1972). A statistical interpretation of term specificity and its application in retrieval. *Journal of Documentation, 28*(1), 11-21. doi:doi:10.1108/eb026526

Srinidhi, B., Yan, J., & Tayi, G. K. (2008). *Firm-level Resource Allocation to Information Security in the Presence of Financial Distress*. Retrieved from http://ideas.repec.org/p/wsu/wpaper/yan-1.html

Srinidhi, B., Yan, J., & Tayi, G. K. (2015). Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors. *Decision Support Systems, 75*, 49-62. doi:http://dx.doi.org/10.1016/j.dss.2015.04.011

Stewart, T., & Durbach, I. (2016). Dealing with Uncertainties in MCDA. In S. Greco, M. Ehrgott, & J. R. Figueira (Eds.), *Multiple Criteria Decision Analysis: State of the Art Surveys* (pp. 467-496). New York, NY: Springer New York.

Steyvers, M., & Griffiths, T. (2007). Probabilistic topic models. *Handbook of latent semantic analysis, 427*(7), 424-440.

Straub, D. W., & Nance, W. D. (1990). Discovering and Disciplining Computer Abuse in Organizations: A Field Study. *MIS Quarterly, 14*(1), 45-60. doi:10.2307/249307

Straub, D. W., & Welke, R. J. (1998). Coping with Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly, 22*(4), 441-469. doi:10.2307/249551

Strauss, A., & Corbin, J. (1998). *Basics of qualitative research* (2nd ed.): Sage Publications, Inc.

Strotz, R. H. (1955). Myopia and Inconsistency in Dynamic Utility Maximization. *The Review of Economic Studies, 23*(3), 165-180. doi:10.2307/2295722

Stubley, D. (2013, 2013-06-07). What is Cyber Security? Retrieved from https://www.7elements.co.uk/resources/blog/what-is-cyber-security/

Suh, B., & Han, I. (2003). The Impact of Customer Trust and Perception of Security Control on the Acceptance of Electronic Commerce. *International Journal of Electronic Commerce, 7*(3), 135-161. doi:10.1080/10864415.2003.11044270

Symantec. (2016, 2016-12-14). What were the top trends in cybersecurity in 2016? Retrieved from https://medium.com/threat-intel/cybersecurity-ransomware-iot-2016-trends-fd4c45389cb

Takach, G. S. (2016). Chapter 9 - Preparing for Breach Litigation A2 - Fowler, Kevvie *Data Breach Preparation and Response* (pp. 217-230). Boston: Syngress.

Tang, J., Meng, Z., Nguyen, X., Mei, Q., & Zhang, M. (2014). *Understanding the Limiting Factors of Topic Modeling via Posterior Contraction Analysis.* Paper presented at the ICML.

Target Inc. (2013). response & resources related to Target's data breach. Retrieved from https://corporate.target.com/about/payment-card-issue.aspx

Tastle, W. J., & Wierman, M. J. (2007). Consensus and dissention: A measure of ordinal dispersion. *International Journal of Approximate Reasoning, 45*(3), 531-545. doi:http://dx.doi.org/10.1016/j.ijar.2006.06.024

Tatsumi, K.-i., & Goto, M. (2010). *Optimal Timing of Information Security Investment: A Real Options Approach.*

Telang, R., & Wattal, S. (2007). An empirical analysis of the impact of software vulnerability announcements on firm stock price. *Ieee Transactions on Software Engineering, 33*(8), 544-557. doi:10.1109/tse.2007.1015

Tervonen, T., & Figueira, J. R. (2008). A survey on stochastic multicriteria acceptability analysis methods. *Journal of Multi-Criteria Decision Analysis, 15*(1-2), 1-14. doi:10.1002/mcda.407

Tervonen, T., & Lahdelma, R. (2007). Implementing stochastic multicriteria acceptability analysis. *European Journal of Operational Research, 178*(2), 500-513. doi:https://doi.org/10.1016/j.ejor.2005.12.037

Tervonen, T., van Valkenhoef, G., Baştürk, N., & Postmus, D. (2013). Hit-And-Run enables efficient weight generation for simulation-based multiple criteria decision analysis. *European Journal of Operational Research, 224*(3), 552-559. doi:https://doi.org/10.1016/j.ejor.2012.08.026

Thaler, R. H., & Sunstein, C. R. (2003). Libertarian Paternalism. *The American Economic Review, 93*(2), 175-179.

The Economist. (2017). The world's most valuable resource is no longer oil, but data. *The Economist*. Retrieved from https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource

The White House. (2009). National Cybersecurity Awareness Month, 2009 [Press release]. Retrieved from https://www.whitehouse.gov/the_press_office/Presidential-Proclamation-National-Cybersecurity-Awareness-Month/

The White House. (2015). Executive Order -- Promoting Private Sector Cybersecurity Information Sharing [Press release]. Retrieved from https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari

Thomas, R. C. (2009). *Total cost of security: a method for managing risks and incentives across the extended enterprise*. Paper presented at the Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies, Oak Ridge, Tennessee, USA.

Thomson, K.-L., & von Solms, R. (2006). Towards an Information Security Competence Maturity Model. *Computer Fraud & Security, 2006*(5), 11-15. doi:https://doi.org/10.1016/S1361-3723(06)70356-6

Tong, A., Sainsbury, P., & Craig, J. (2007). Consolidated criteria for reporting qualitative research (COREQ): a 32-item checklist for interviews and focus groups. *International Journal for Quality in Health Care, 19*(6), 349-357. doi:10.1093/intqhc/mzm042

Torres, J. M., Sarriegi, J. M., Santos, J., & Serrano, N. (2006). *Managing Information Systems Security: Critical Success Factors and Indicators to Measure Effectiveness*, Berlin, Heidelberg.

Tosh, D. K., Molloy, M., Sengupta, S., Kamhoua, C. A., & Kwiat, K. A. (2015, 24-26 Aug. 2015). *Cyber-Investment and Cyber-Information Exchange Decision Modeling*. Paper presented at the 2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems.

Ungar, L., Mellers, B., Satopää, V., Tetlock, P., & Baron, J. (2012). *The Good Judgment Project: A Large Scale Test of Different Methods of Combining Expert Predictions*. Paper presented at the 2012 AAAI Fall Symposium Series.

Van Der Eijk, C. (2001). Measuring Agreement in Ordered Rating Scales. *Quality and Quantity, 35*(3), 325-341. doi:10.1023/a:1010374114305

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security, 29*(4), 476-486. doi:10.1016/j.cose.2009.10.005

Van Valkenhoef, G. (2018). smaa: Stochastic Multi-Criteria Acceptability Analysis (Version 0.3). CRAN. Retrieved from https://cran.r-project.org/package=smaa

van Wieren, M., Doerr, C., Jacobs, V., & Pieters, W. (2016). *Understanding Bifurcation of Slow Versus Fast Cyber-Attackers*, Cham.

Vargo, S. L., Maglio, P. P., & Akaka, M. A. (2008). On value and value co-creation: A service systems and service logic perspective. *European Management Journal, 26*(3), 145-152. doi:https://doi.org/10.1016/j.emj.2008.04.003

Vázquez, D. F., Acosta, O. P., Spirito, C., Brown, S., & Reid, E. (2012, 5-8 June 2012). *Conceptual framework for cyber defense information sharing within trust relationships*. Paper presented at the 2012 4th International Conference on Cyber Conflict (CYCON 2012).

von Solms, R. (1996). Information security management: The second generation. *Computers & Security, 15*(4), 281-288. doi:https://doi.org/10.1016/0167-4048(96)88939-5

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97-102. doi:http://dx.doi.org/10.1016/j.cose.2013.04.004

Walls, A., Perkins, E., & Weiss, J. (2013). Definition: Cybersecurity, 5. Retrieved from Gartner.com website: https://www.gartner.com/doc/2510116/definition-cybersecurity

Wamala, F. (2011). *ITU National Cybersecurity Strategy Guide*. Retrieved from Geneva: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-national-cybersecurity-guide.pdf

Wang, L., Jajodia, S., Singhal, A., Cheng, P., & Noel, S. (2014). k-Zero Day Safety: A Network Security Metric for Measuring the Risk of Unknown Vulnerabilities. *IEEE Transactions on Dependable and Secure Computing, 11*(1), 30-44. doi:10.1109/TDSC.2013.24

Wang, T., Rees, J., & Kannan, K. (2007). *Reading the Disclosures with New Eyes: Bridging the Gap between Information Security Disclosures and Incidents*. Paper presented at the Seventh Workshop on the Economics of Information Security, Hanover, NH.

Wei, L., Tanaka, H., & Matsuura, K. (2007). Empirical-analysis methodology for information-security investment and its application to reliable survey of Japanese firms. *Transactions of the Information Processing Society of Japan, 48*(9), 3204-3218.

Weir, C. S., Douglas, G., Carruthers, M., & Jack, M. (2009). User perceptions of security, convenience and usability for ebanking authentication tokens. *Computers & Security, 28*(1), 47-62. doi:https://doi.org/10.1016/j.cose.2008.09.008

Weir, C. S., Douglas, G., Richardson, T., & Jack, M. (2010). Usable security: User preferences for authentication methods in eBanking and the effects of experience. *Interacting with Computers, 22*(3), 153-164. doi:https://doi.org/10.1016/j.intcom.2009.10.001

Weishäupl, E., Yasasin, E., & Schryen, G. (2015). IT Security Investments through the Lens of the Resource-based View: A new theoretical Model and Literature Review.

Weiss, S., Indurkhya, N., Zhang, T., & Damerau, F. (2004). *Text Mining: Predictive Methods for Analyzing Unstructured Information*: SpringerVerlag.

West, B. (2016). Chapter 7 - Communicating Before, During and After a Breach A2 - Fowler, Kevvie *Data Breach Preparation and Response* (pp. 167-185). Boston: Syngress.

Wetzels, M., Odekerken-Schröder, G., & Van Oppen, C. (2009). Using PLS path modeling for assessing hierarchical construct models: Guidelines and empirical illustration. *MIS Quarterly*, 177-195.

Whitman, M. E. (2003). Enemy at the gate: threats to information security. *Commun. ACM, 46*(8), 91-95. doi:10.1145/859670.859675

Whittaker, B. (1999). What went wrong? Unsuccessful information technology projects. *Information Management & Computer Security, 7*(1), 23-30. doi:doi:10.1108/09685229910255160

Widup, S. (2012). Closing the Vault Door. *The Leaking Vault.* Retrieved from http://theleakingvault.com/closing-the-vault-door

Wilcoxon, F. (1945). Individual Comparisons by Ranking Methods. *Biometrics Bulletin, 1*(6), 80-83. doi:10.2307/3001968

Willemson, J. (2010). Extending the Gordon&Loeb Model for Information Security Investment. *Proceedings of the Fifth International Conference on Availability, Reliability, and Security (ARES 2010)*, 258-261. doi:10.1109/ares.2010.37

Wolcott, H. F. (1982). Differing styles of on-site research, or" If it isn't ethnography, what is it?". *Review Journal of Philosophy and Social Science, 7*(1), 154-169.

Wold, H. (1974). Causal flows with latent variables: partings of the ways in the light of NIPALS modelling. *European Economic Review, 5*(1), 67-86.

Wold, H. (1982). Models for Knowledge. In J. Gani (Ed.), *The Making of Statisticians* (pp. 189-212). New York, NY: Springer New York.

Wood, C. C., & Parker, D. B. (2004). Why ROI and similar financial tools are not advisable for evaluating the merits of security projects. *Computer Fraud & Security, 2004*(5), 8-10. doi:http://dx.doi.org/10.1016/S1361-3723(04)00064-8

Woolf, N. (2016). DDoS attack that disrupted internet was largest of its kind in history, experts say. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

World Economic Forum. (2015). *Towards the Quantification of Cyber Threats*. Retrieved from Geneva: http://www.weforum.org/reports/partnering-cyber-resilience-towards-quantification-cyber-threats

Wu, Z., & Palmer, M. (1994). *Verbs semantics and lexical selection*. Paper presented at the Proceedings of the 32nd annual meeting on Association for Computational Linguistics, Las Cruces, New Mexico.

Xue, Y., Liang, H., & Boulton, W. R. (2008). Information Technology Governance in Information Technology Investment Decision Processes: The Impact of Investment Characteristics, External Environment, and Internal Context. *MIS Quarterly, 32*(1), 67-96.

Yayla, A. A., & Hu, Q. (2011). The impact of information security events on the stock value of firms: the effect of contingency factors. *Journal of Information Technology, 26*(1), 60-77. doi:10.1057/jit.2010.4

Yong Jick, L., Kauffman, R. J., & Sougstad, R. (2011). Profit-maximizing firm investments in customer information security. *Decision Support Systems, 51*(4), 904-920. doi:10.1016/j.dss.2011.02.009

Yuhua, L., Bandar, Z. A., & McLean, D. (2003). An approach for measuring semantic similarity between words using multiple information sources. *Knowledge and Data Engineering, IEEE Transactions on, 15*(4), 871-882. doi:10.1109/TKDE.2003.1209005

Yuhua, L., McLean, D., Bandar, Z. A., O'Shea, J. D., & Crockett, K. (2006). Sentence similarity based on semantic nets and corpus statistics. *Knowledge and Data Engineering, IEEE Transactions on, 18*(8), 1138-1150. doi:10.1109/TKDE.2006.130

Zaini, M. K., & Masrek, M. N. (2013, 23-24 Dec. 2013). *Conceptualizing the Relationships between Information Security Management Practices and Organizational Agility.* Paper presented at the 2013 International Conference on Advanced Computer Science Applications and Technologies.

Zhou, L., Vasconcelos, A., & Nunes, M. (2008). Supporting decision making in risk management through an evidence-based information systems project risk checklist. *Information Management & Computer Security, 16*(2), 166-186. doi:doi:10.1108/09685220810879636

Zikai, W., & Haitao, S. (2008). Towards an optimal information security investment strategy. *2008 IEEE International Conference on Networking, Sensing and Control (ICNSC '08)*, 756-761.

Zimmerman, D. W. (1994). A Note on the Influence of Outliers on Parametric and Nonparametric Tests. *The Journal of General Psychology, 121*(4), 391-401. doi:10.1080/00221309.1994.9921213

Zionts, S. (1979). MCDM: If Not a Roman Numeral, then What? *Interfaces, 9*(4), 94-101.

APPENDICES

APPENDIX CHAPTER 3-1

This section provides details on authoritative definitions and their sources.

ID	source	title	year	definition
1	Committee on National Security Systems	National Information Assurance (IA) Glossary	2009	The ability to protect or defend the use of cyberspace from cyber attacks.
2	National Initiative for Cybersecurity Careers and Studies,	Explore Terms: A Glossary of Common Cybersecurity Terminology	n/a	Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure.
3	International Telecommunication Union	SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY	2008	Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and users assets. Organization and users assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and users assets against relevant security risks in the cyber environment. The general security objectives comprise the following: Availability Integrity, which may include authenticity and non-repudiation Confidentiality
4	Gartner	Definition: Cybersecurity	2013	Cybersecurity is the governance, development, management and use of information security, OT security, and IT security tools and techniques for achieving regulatory compliance, defending assets and compromising the assets of adversaries.

5	The Institution of Engineering and Technology	Resilience and Cyber Security of Technology in the Built Environment	2013	Cybersecurity strives to ensure the attainment and maintenance of the security objectives of the organisation and users assets against relevant security risks in the cyber environment
6	British Standards Institute	Guidelines for cybersecurity	2012	Preservation of confidentiality, integrity and availability of information in the Cyberspace. In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.
7	Australian Government	Cyber Security Strategy	2009	Measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means
8	Federal Chancellery of the Republic of Austria	Austrian Cyber Security Strategy	2013	Cybersecurity describes the protection of a key legal asset through constitutional means against actor-related, technical, organisational and natural dangers posing a risk to the security of cyber space (including infrastructure and data security) as well as the security of the users in cyber space. Cybersecurity helps to identify, assess and follow up on threats as well as to strengthen the ability to cope with interferences in or from cyber space, to minimise the effects as well as to restore the capacity to act and functional capabilities of the respective stakeholders, infrastructures and services.
9	Government of Belgium	Cyber Security Strategy	2012	Cybersecurity is the desired condition in which the security of cyberspace is in proportion to the cyber threat and the potential impact of cyber attacks. Cybersecurity is freedom from danger or damage caused by disruption or failure of IT or by abuse of ICT. The consequences by abuse, disruption or failure can include limiting the availability and reliability of IT, breach of confidentiality of information or damage to the integrity of that information (Change unlawful, delete or add).
10	Government of Finland	Finland's Cyber Security Strategy	2013	Cybersecurity means the desired end state in which the cyber domain is reliable and in which its functioning is ensured. In the desired end state the cyber domain will not jeopardise, harm or disturb the operation of functions dependent on electronic information (data) processing. Reliance on the cyber domain depends on its actors implementing appropriate and sufficient information security procedures (communal data security). These procedures can prevent the materialisation of cyber threats and, should they still materialise, prevent, mitigate or help tolerate

				their consequences. Cybersecurity encompasses the measures on the functions vital to society and the critical infrastructure which aim to achieve the capability of predictive management and, if necessary, tolerance of cyber threats and their effects, which can cause significant harm or danger to Finland or its population.
11	French Network and Information Security Agency	Information systems defence and security France's strategy	2011	The desired state of an information system in which it can resist events from cyberspace likely to compromise the availability, integrity or confidentiality of the data stored, processed or transmitted and of the related services that these systems offer or make accessible. Cybersecurity makes use of information systems security techniques and is based on fighting cybercrime and establishing cyber defence.
12	Federal Ministry of the Interior	Cyber Security Strategy for Germany	2011	Cybersecurity is the desired objective of the IT security situation, in which the risks of global cyberspace have been reduced to an acceptable minimum. Hence, cybersecurity in Germany is the desired objective of the IT security situation, in which the risks of the German cyberspace have been reduced to an acceptable minimum. Cybersecurity is the sum of suitable and appropriate measures. Civilian cybersecurity focuses on all IT systems for civilian use in German cyberspace. Military cybersecurity focuses on all IT systems for military use in German cyberspace.
13	Government of Hungary	National Cyber Security Strategy of Hungary	2013	The ongoing and systematic application of political, legal, economic, educational, awareness-raising and technical tools suitable for managing cyberspace risks, transforming the cyberspace into a reliable environment by ensuring an acceptable level of such risks for the smooth functioning and operation of social and economic processes
14	The Netherlands, Ministry of Security and Justice	The National Cyber Security Strategy (NCSS) 2	2013	The continuous and planned taking of political, legal, economic, educational, awareness-raising and technical measures to manage risks in cyberspace that transforms the cyberspace into a reliable environment for the smooth functioning and operation of societal and economic processes by ensuring an acceptable level of risks in cyberspace.
15	New Zealand Government	New Zealand's Cyber Security Strategy	2011	The practice of making the networks that constitute cyber space as secure as possible against intrusions, maintaining confidentiality, availability and integrity of information, detecting intrusions and incidents that do occur, and responding to and recovering from them.

16	Norwegian Ministries	Cyber Security Strategy for Norway	2012	Protection of data and systems connected to the Internet
17	Kingdom of Saudi Arabia	Developing National Information Security Strategy for the Kingdom of Saudi Arabia	2011	The ability to protect or defend the use of cyberspace from cyber-attacks.
18	Republic of South Africa	Cybersecurity Policy of South Africa	2010	Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and assets.
19	Republic of Turkey	National Cyber Security Strategy and 2013-2014 Action Plan	n/a	Protection of information systems that make up the cyber space from attacks, ensuring the confidentiality, integrity and accessibility of the information being processed in this space, detection of attacks and cybersecurity incidents, putting into force the countermeasures against these incidents and then putting these systems back to their states previous to the cybersecurity incident.
20	National Institute of Standards and Technology	Framework for Improving Critical Infrastructure Cybersecurity	2014	The process of protecting information by preventing, detecting, and responding to attacks
21	Spanish Cyber Security Institute	National Cyber Security, a commitment for everybody	2012	Cybersecurity consists of the application of an analysis and management process for risks associated with use, processing, storage and transmission of information and data, as well as risks associated with the systems and processes used, based on internationally accepted standards. The protection of goods, assets, services, rights and freedoms, within state jurisdiction.
22	Republic of Poland	CYBERSPACE PROTECTION POLICY OF THE REPUBLIC OF POLAND	2013	A set of organizational and legal, technical, physical and educational projects aimed at ensuring the uninterrupted functioning of cyberspace

23	Government of Jamaica	NATIONAL CYBER SECURITY STRATEGY	201 5	The implementation of measures to protect ICT infrastructure including critical infrastructure from intrusion, unauthorized access and includes the adoption of policies, protocols and good practices to better govern the use of cyberspace.
24	Craigen, Dan Diakun-Thibault, Nadia Purse, Randy	Defining Cybersecurit y	201 4	Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights.
25	Merriam-Webster	Definition of Cybersecurit y	201 5	Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack.
26	Oxford Dictionary	Definition of Cybersecurit y	201 5	The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this
27	Amoroso, Edward	Cyber Security	200 7	Cybersecurity involves reducing the risk of malicious attack to software, computers, and networks. This includes the tools used to detect break-ins, stop viruses, block malicious access, enforce authentication, enable encrypted communications, and on and on
28	EastWest Institute	Critical Terminology Foundations 2	201 4	Cybersecurity is a property of cyberspace that is an ability to resist intentional and/or unintentional threats and respond and recover
29	New Definition		201 5	The approach and actions associated with security risk management processes followed by organisations and states to protect confidentiality, integrity and availability of data and assets used in cyber space. The concept includes guidelines, policies and collections of safeguards, technologies, tools and training to provide the best protection for the state of the cyber environment and its users.”

APPENDIX CHAPTER 5-1

#	Question
1	How experienced would you say you are when it comes to Information Security investment decision processes?
2	What aspects or factors do you usually consider when making information security investment decisions? (e.g. legal, economic, cultural,…)
3	What are the value factors you're looking for in each area? i.e. what are attributes that add value to an investment from an InfoSec perspective?
4	How do you quantify the value of these investments to the organization?
5	What cost factors (direct or indirect) do you consider when making investment decisions for information security?
6	What are the key challenges when deciding which Information Security investment to go with? e.g. information on risk reduction, breach probability, etc.

7	If at all, how do you reduce uncertainty on those challenges to improve confidence in the investment decision?
8	Do you calculate/project cost of compromise? What cost components do you include?
9	Are you using any ‘return on investment’ type calculations for InfoSec spending? Which ones and why those?
10	Following from (9) – do you use them always or just sometimes? Are there any particularly useful aspects or challenges?
11	If you are using an Information Security Governance framework or ISMS - Does your framework cover economic aspects of InfoSec? E.g. does it provide guidance for financially sensible security investments?
12	Do you believe investment decisions in Information Security will come under greater scrutiny in future?

APPENDIX CHAPTER 7-1

Education

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	High school degree	4	1.6	1.6	1.6
	Some college without degree	36	14.4	14.4	16.0
	Associate degree	23	9.2	9.2	25.2
	Bachelor degree	149	59.6	59.6	84.8
	Graduate degree	38	15.2	15.2	100.0
	Total	250	100.0	100.0	

Job_Level

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Other	2	.8	.8	.8
	Owner/Executive	12	4.8	4.8	5.6
	Senior Management	52	20.8	20.8	26.4
	Middle Management	90	36.0	36.0	62.4

	Intermediate role	79	31.6	31.6	94.0
	Entry Level role	15	6.0	6.0	100.0
	Total	250	100.0	100.0	

InfoSec_knowledge

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Basic knowledge	20	8.0	8.0	8.0
	Moderate knowledge	144	57.6	57.6	65.6
	High knowledge	86	34.4	34.4	100.0
	Total	250	100.0	100.0	

Purchasing_knowledge

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Basic	20	8.0	8.0	8.0
	Intermediate	110	44.0	44.0	52.0
	Advanced	91	36.4	36.4	88.4
	Expert	29	11.6	11.6	100.0
	Total	250	100.0	100.0	

Industry

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Advertising	4	1.6	1.6	1.6
	Business Support	17	6.8	6.8	8.4
	Construction	6	2.4	2.4	10.8
	Education	18	7.2	7.2	18.0
	Entertainment	12	4.8	4.8	22.8
	Finance	34	13.6	13.6	36.4
	Government	14	5.6	5.6	42.0
	Healthcare & Pharma	21	8.4	8.4	50.4
	Insurance	3	1.2	1.2	51.6
	Manufacturing	25	10.0	10.0	61.6
	Nonprofit	1	.4	.4	62.0
	Retail	13	5.2	5.2	67.2
	Real Estate	6	2.4	2.4	69.6
	Telecoms	66	26.4	26.4	96.0
	Transportation	4	1.6	1.6	97.6
	Utilities	4	1.6	1.6	99.2
	Unemployed	2	.8	.8	100.0
	Total	250	100.0	100.0	

APPENDIX CHAPTER 7-2

Overview of latent variables and indicators

LV	**Indicator**	**Indicator Description**
Accnt	FA_EXP	The extent to which expenditure type considerations impact security investments
Accnt	FA_HUR	The extent to which hurdle rate considerations impact security investments
Accnt	FA_PRE	The extent to which insurance premium considerations impact security investments
BusProc	BP_CO	Impact considerations of communications in relation to security
BusProc	BP_CR	Conflicting business process requirements affecting security
BusProc	BP_OC	Conflict of security investments with other business opportunities
BusProc	BP_BP	Impact of security on business processes and user acceptance
BusProc	BP_SC	Impact on preexisting controls
BusProc	BP_TR	Conflicts in the underlying technical environment impacting security
CntrlCst	CC_IC	Consideration of the internal and external cost for implementation
CntrlCst	CC_OB	Consideration of the total budget available
CntrlCst	CC_OC	Consideration of the cost to operate a security control
CntrlCst	CC_PP	Consideration of the initial cost of the control
CntrlEff	CE_BR	Considerations on the extent to which the control can be bypassed
CntrlEff	CE_DF	Considerations on the deterrence benefits of the control
CntrlEff	CE_EC	Considerations on whether the control is working effectively
CntrlEff	CE_FP	Considerations on the accuracy of the control (false positive rate)
CntrlEff	CE_PV	Considerations of the velocity of security benefits

CntrlRsk	CR_CR	The extent to which the investment will address compliance requirements
CntrlRsk	CR_IR	The extent to which the investment will fix an immediate issue
CntrlRsk	CR_KR	The extent to which the investment will address known risks
CntrlRsk	CR_UR	The extent to which the investment will address yet unknown risks
CompEdge	CE_AG	The impact on business agility
CompEdge	CE_CA	The impact on competitive advantage
CompEdge	CE_CE	The impact on customer experience
IncCost	IC_CC	Considerations related to customer notifications and expenses
IncCost	IC_CL	Considerations related to the impact on customer retention
IncCost	IC_MS	Considerations related to the impact on market share
IncCost	IC_PR	Considerations related to public relations efforts and cost
IncCost	IC_RI	Considerations related to the impact on reputation
L&R	LR_CP	Considerations related to contractual penalties
L&R	LR_LC	Considerations related to legal counsel and proceedings
L&R	LR_LF	Considerations related to regulatory or legal fines
L&R	LR_SA	Considerations related to non-financial regulatory sanctions
PPLRes	PR_PM	Considerations on human resource requirements to deliver projects
PPLRes	PR_SC	Considerations on qualified staff overhead
PPLRes	PR_TC	Considerations on educational cost for human resources
Threats	T_AR	Consideration on how well a threat source is resourced
Threats	T_EFF	Consideration on the efficiency/time to impact of the threat
Threats	T_LH	Consideration on how likely an attack/event by a threat source is

APPENDIX CHAPTER 8-1

Criteria	**Direction**	**Measurement type**
FA_EXP	ascend	Likert type 1 - 5 (Not at all, Little, Somewhat, Much, A great amount)
FA_HUR	ascend	Likert type 1 - 5 (Not likely, Somewhat unlikely, Unsure, somewhat likely, very likely)
FA_PRE	ascend	Likert type 1 - 5 (considerably increase or no insurance possible, some increase, unaffected, some reduction, considerable reduction)
BP_CO	ascend	Likert type 1 - 5 (A great amount, Much, Somewhat, Little, Not at all)
BP_CR	ascend	Likert type 1 - 5 (A great amount, Much, Somewhat, Little, Not at all)
BP_OC	ascend	Likert type 1 - 5 (A great amount, Much, Somewhat, Little, Not at all)
BP_BP	ascend	Likert type 1 - 5 (Negative, slightly negative, No impact, slightly positive, Positive)
BP_SC	ascend	Likert type 1 - 5 (Strongly conflict, conflict, neither, complement, strongly complement)
BP_TR	ascend	Likert type 1 - 5 (Not at all, Little, Somewhat, Much, A great amount)
CC_IC	descend	Cardinal, e.g. 1000 - 3400, 45000 - 80000, …
CC_OB	descend	Cardinal, e.g. 6 or 25
CC_OC	descend	Cardinal, e.g. 1000 - 3400, 45000 - 80000, …
CC_PP	descend	Cardinal, e.g. 15400, 796000, …
CE_BR	ascend	Likert type 1 - 5 (Very Easy, Easy, Average, Difficult, Very Difficult)
CE_DF	ascend	Likert type 1 - 5 (Unlikely, Somewhat unlikely, Unsure, somewhat likely, very likely)
CE_EC	ascend	Likert type 1 - 5 (Not at all, Little, Somewhat, Much, A great amount)
CE_FP	ascend	Likert type 1 - 5 (Very High, High, Average, Low, Very Low)
CE_PV	ascend	Likert type 1 - 5 (Uncertain, Years, Months, Weeks, Days)
CR_CR	ascend	Likert type 1 - 5 (Not at all, Little, Somewhat, Much, A great amount)
CR_IR	ascend	Likert type 1 - 5 (Not at all, Little, Somewhat, Much, A great amount)

Criteria	**Directio n**	**Measurement type**
CR_KR	ascend	Likert type 1 - 5 (Not at all, Little, Somewhat, Much, A great amount)
CR_UR	ascend	Likert type 1 - 5 (Not at all, Little, Somewhat, Much, A great amount)
CE_AG	ascend	Likert type 1 - 5 (Very Negative, Negative, Neutral, Positive, Very Positive)
CE_CA	ascend	Likert type 1 - 5 (Not at all, Little, Somewhat, Much, A great amount)
CE_CE	ascend	Likert type 1 - 5 (Very negative, Negative, None, Positive, very positive)
IC_CC	ascend	Likert type 1 - 5 (Not at all, Little, Somewhat, Much, A great amount)
IC_CL	ascend	Likert type 1 - 5 (Not at all, Little, Somewhat, Much, A great amount)
IC_MS	ascend	Likert type 1 - 5 (Not at all, Little, Somewhat, Much, A great amount)
IC_PR	ascend	Likert type 1 - 5 (Not at all, Little, Somewhat, Much, A great amount)
LR_CP	ascend	Likert type 1 - 5 (Not at all, Little, Somewhat, Much, A great amount)
LR_LC	ascend	Likert type 1 - 5 (Not at all, Little, Somewhat, Much, A great amount)
LR_LF	ascend	Likert type 1 - 5 (Not at all, Little, Somewhat, Much, A great amount)
LR_SA	ascend	Likert type 1 - 5 (Not at all, Little, Somewhat, Much, A great amount)
PR_PM	ascend	Likert type 1 - 5 (A great amount, Much, Somewhat, Little, None)
PR_SC	ascend	Likert type 1 - 5 (Considerably higher specialist staff requirements, Higher staff requirements, Average staff requirements, Low staff requirements, No specialist staff required)
PR_TC	ascend	Likert type 1 - 5 (A great amount, Much, Somewhat, Little, None)
T_AR	ascend	Likert type 1 - 5 (No resistance, below adequate, Adequate resistance, above adequate, Well above required)
T_EFF	ascend	Likert type 1 - 5 (Not at all, Little, Somewhat, Much, A great amount)
T_LH	ascend	Likert type 1 - 5 (Not probable, somewhat improbable, neutral, somewhat probable, Very probable)

APPENDIX CHAPTER 8-2

ID	**AVSol1**	**AVSol2**	**AVSol3**	**AppWL**	**HIPS**	**Unchanged**
FA_EXP	5	4	4	4	4	5
FA_HUR	5	3	3	3	4	5
FA_PRE	3	4	4	4	4	1
BP_CO	4	3	3	2	2	5
BP_CR	3	3	2	2	2	5
BP_OC	5	4	4	4	4	5
BP_BP	3	3	3	2	3	4
BP_SC	4	4	4	4	4	3
BP_TR	2	3	2	3	3	5
CC_IC	5000 - 10000	15000 - 20000	15000 - 20000	20000 - 30000	20000 - 30000	0
CC_OB	0	8	12	10	3	0
CC_OC	0	35000 - 50000	80000 - 120000	55000 - 70000	5000 - 15000	0
CC_PP	0	70000 - 80000	80000 - 120000	900000 - 110000	0	0
CE_BR	3	4	4	5	3	1
CE_DF	2	3	4	5	4	1
CE_EC	3	4	3	4	3	1
CE_FP	4	4	3	2	3	5
CE_PV	5	5	4	4	4	1

CR_CR	4	5	4	5	4	1
CR_IR	4	4	4	4	4	1
CR_KR	5	5	5	5	5	1
CR_UR	2	3	4	4	4	1
CE_AG	3	3	3	3	3	2
CE_CA	3	3	4	4	4	1
CE_CE	3	3	3	2	2	3
IC_CC	2	2	2	2	2	1
IC_CL	2	2	2	2	2	1
IC_MS	2	2	2	2	2	1
IC_PR	2	3	3	3	3	1
LR_CP	2	3	3	3	3	1
LR_LC	2	2	2	2	2	1
LR_LF	3	3	3	3	3	1
LR_SA	3	3	3	3	3	1
PR_PM	4	3	3	2	2	5
PR_SC	4	3	2	2	2	5
PR_TC	4	3	3	2	2	5
T_AR	2	3	4	4	4	1
T_EFF	2	3	4	5	4	1
T_LH	3	4	4	5	4	1