Decision Problems in Information Security:
Methodologies and Quantitative Models

Dissertation zur Erlangung des Grades eines
Doktors der Wirtschaftswissenschaft

eingereicht an der Fakultät fär Wirtschaftswissenschaften
der Universität Regensburg

vorgelegt von: Emrah Yasasin

Berichterstatter: Prof. Dr. Guido Schryen, Prof. Dr. Günther Pernul

Tag der Disputation: 30. November 2018

University of Regensburg
Faculty of Business, Economics, and Management Information Systems
Department of Management Information Systems

Dissertation

Decision Problems in Information Security: Methodologies and Quantitative Models

---

submitted by
Emrah Yasasin M.Sc.
to
the Faculty of Business, Economics, and Management Information Systems
of the University of Regensburg
for the Degree of
Doctor rerum politicarum
in
Management Information Systems

Supervisors:
Prof. Dr. Guido Schryen
Prof. Dr. Günther Pernul

Regensburg, July 13, 2018

To my parents Habibe and Çetin Yaşasın

Preface

This dissertation was developed under the supervision of Prof. Dr. Guido Schryen. The thesis covers decision problems in information security and develops methodologies and quantitative models to address open issues in academia and to provide insights for practitioners. Framed in an adaptation of the process theory of Soh and Markus (1995) - from a thematic point of view - the dissertation comprises papers that cover decision problems in each phase[1] of the adapted theory. Within the first phase, the "*information security conversion process*", Paper 1 synthesizes research streams that explore firms' investments in information security and how these are transformed into resources. Paper 2 provides insights into how firms undertake information security investment actions, how firms evaluate the transformation of their information security investments into information security resources, and how they learn from past investments and transformations. Paper 3, which is situated in the second phase, the "*information security technologies / methods use process*", develops an optimization model to effectively allocate IT security incident tickets ("trouble tickets") to IT staff members under the consideration of capabilities and time constraints to ensure a smooth running of business operations. Next, Paper 4 introduces an innovative approach in the area of IT security vulnerabilities: It addresses the prediction of security vulnerabilities by applying forecasting methods in order to support managerial decisions. Lastly, Paper 5 addresses an important decision problem in the third phase, the "*information security competitive process*". This phase addresses the assessment of the impact of a firm's information security performance. These performance measurements are often carried out with the use of information security metrics; I therefore focus on the foundations of designing valid, objective and meaningful metrics by deriving a set of requirements and applying them to two metrics that are used in practice. The requirements target in particular decision makers who can evaluate herewith the applicability of their information security metrics.

The papers that build the core of my dissertation were made possible by the support I have received from many people over the years. I want to thank Prof. Dr. Guido Schryen for his

[1] The original phases of Soh and Markus (1995)'s process theory are "IT Conversion Process", "IT Use Process" and "Competitive Process", which I adapted as (1) "Information Security Conversion Process", (2) "Information Security Technologies / Methods Use Process" and (3) "Information Security Competitive Process" in the information security context.

outstanding support over the past years. Right from the beginning he motivated me by showing his lively interest in the progress of each paper, by expressing his commitment to my work, and by having faith in me to present our research at important conferences. I appreciate the inspiration for research that Prof. Dr. Guido Schryen continuously passes on to his research team. I also want to express my gratitude to Prof. Dr. Günther Pernul, in particular for the years in which I was part of his team as a student assistant: For me, this period was a decisive reason to embark upon a career in academia. I would also like to express my gratitude to my office colleagues Ms. Eva Szubartowicz (née Weishäupl) and Mr. Gerhard Rauchecker for the fruitful collaboration. A special chapter goes to Mr. Gerit Wagner: Thank you Gerit for scrupulously reviewing every single one of my documents. Your feedback has always been invaluable and I will miss your scholar's mind. I also want to extend my deepest gratitudes to Mr. Julian Prester for his excellent help regarding various aspects in research and teaching.

Financial support by the *Regionale Wettbewerbsfähigkeit und Beschäftigung*, Bavaria, 2007-2013 (EFRE) as part of the SECBIT project (http://www.secbit.de), the *Bavarian State Ministry for Education, Science and the Arts* as part of the FORSEC research association (https://www.bayforsec.de), the *German Academic Exchange Service* (DAAD) (https://www.daad.de), and the *Hanns Seidel Foundation* (http://www.hss.de) is gratefully acknowledged.

Finally, I would like to thank my parents, Habibe and Çetin Yaşasın, my brothers, Emin and Erdi Yaşasın, and my wife, İlknur Yaşasın. Completing this work would have been all the more difficult were it not for the support and love provided by them.

Regensburg, July 13, 2018 *Emrah Yasasin*

Table of Contents

Part I Dissertation Outline

1 Introduction . . . 3
- 1.1 Problem Relevance . . . 3
- 1.2 Decision Problems in Information Security: A Process Theory-Based Approach . . . 7
  - 1.2.1 Information Technology and Decision Problems: Soh and Markus (1995)'s Process Theory . . . 7
  - 1.2.2 A Process Theory-Based Approach to Decision Problems in Information Security . . . 9
- 1.3 Phases, Research Questions and Papers: An Overview . . . 16

Part II Research Papers

2 Phase 1: Information Security Conversion Process . . . 21
- 2.1 Paper 1: A Multi-Theoretical Literature Review on Information Security Investments using the Resource-Based View and the Organizational Learning Theory . . . 21
- 2.2 Paper 2: Information Security Investments: An Exploratory Multiple Case Study on Decision-Making, Evaluation and Learning . . . 22

3 Phase 2: Information Security Technologies / Methods Use Process . . . 23
- 3.1 Paper 3: A Decision Support System for IT Security Incident Management . . . 23
- 3.2 Paper 4: Forecasting IT Security Vulnerabilities - An Empirical Analysis . . . 24

4 Phase 3: Information Security Competitive Process . . . 25
- 4.1 Paper 5: Requirements for IT Security Metrics - An Argumentation Theory Based Approach . . . 25

Part III Additional Research Papers

5 List of Additional Research Papers . . . 29

Part IV Discussion and Conclusion

6 Summary, Critical Reflection and Outlook on Future Research . . . 33

Part V Bibliography

References . . . IX

Part I

Dissertation Outline

1

Introduction

The following thesis covers decision problems in information security[2] and develops methodologies and quantitative models to address open issues in academia and to provide insights for practitioners. Framed in an adaption of the process theory of Soh and Markus (1995), the dissertation comprises papers that address decision problems in each phase of the theory. From a methodological point of view, this thesis draws on different sources, such as a literature review, case study or mathematical models. The dissertation is structured as follows: Part I comprises an outline of and introduction to the dissertation. Here, in the first section, I present a motivation for the dissertation. In the second section, I first explain the process theory of Soh and Markus (1995) and adapt their theory to frame my research. Part II links to published versions of the papers that are part of the dissertation. Part III briefly lists additional papers that have been developed during the course of this dissertation. Finally, in Part IV, I discuss the findings of this thesis and conclude with an outline of future research.

1.1 Problem Relevance

Despite the attention information security and its strategic role in today's business operations receive, implementing information security effectively is still a key task enterprises face. For organizations - in particular those competing on a global scale - information security is a crucial strategic issue (Ezingeard et al. 2005, Hall et al. 2011) and it is constantly evolving. According to the "Threat Horizon" report of the Information Security Forum, a nonprofit association which analyzes security and risk management issues, current top threats include disruption caused by an over-reliance on fragile connectivity, disruption of the integrity of information, or

[2] The academic literature indicates that some authors distinguish between information security and IT security (e.g., von Solms (2001), von Solms and van Niekerk (2013)). It is pointed out that "*data security became computer security, and computer security became IT security and IT security became information security*" (von Solms and von Solms 2005, p. 272) because it provides an improved understanding of business impact and related threats in firms to which I concur. Throughout this dissertation, I use the terms information security and IT security synonymously and refer to them as "*protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability*" (Väyrynen et al. 2013, p. 35).

deterioration when controls are eroded by regulations and technology (CIO 2017, Information Security Forum 2017). These occurring threats can be classified as *internal* and *external threats* caused by *human*, *environmental*, or *technological* threats. Human threats include mistakes as well as intentional actions by, for example, insiders or hackers who cause harm to systems. Environmental threats are due to natural disasters, legislation, or disruptions of infrastructure. Finally, technological threats are caused by hardware or software failures (Jouini et al. 2014).

External attacks are one of the main threats: The extent, amount, severity, and diversity of external attacks on information systems are unprecedented (Lowry et al. 2015). For example, Yahoo was hacked in 2016 and announced the largest data breach in history, which affected more than one billion accounts (Yahoo! 2016) and had severe impacts on Yahoo's reputation. The Yahoo data breach enabled Verizon to demand a $1 billion discount on the original acquisition of Yahoo (CSO 2016b).

Similarly, insiders cause substantial security breaches as well, and they are very costly to mitigate (Lowry et al. 2015, Tripwire 2017). A recent study conducted by the SANS Institute surveyed respondents from a range of industries: The study revealed that 45% of the respondents did not know the potential of financial losses associated with an insider incident, while another 33% were unable to place a value on the losses and 38% admitted that their detection and prevention capabilities are ineffective (SANS Institute 2017). In 2016, the Ponemon Institute released a report providing figures of damages caused by insider attacks. The report shows that the average cost of just one single incident is $206,000, and, over a whole year, the costs averaged approximately $4.3 million (CSO 2017, Ponemon Institute 2016). In particular, "*in light of the recent wave of high visibility corporate breaches*" (Gordon et al. 2016, p. 49), such internal information security breaches can affect a firm's reputation (Safa et al. 2016, Shameli-Sendi et al. 2016). Given the importance of information security to the survival of an organization, investments in countermeasures are increasing (Böhme and Moore 2016).

The success of smooth organizational operations in demanding business environments relies in implementing information security efficiently (Hall et al. 2011). The worldwide spending on information security is steadily increasing and it is expected to reach $93 billion in 2018 (Gartner 2017) and predicted to grow to $143.3 billion in 2022 (Gartner 2018). These figures reveal that there is a high demand for suitable information security technologies, processes and methods. Further, organizations have started to focus on a variety of control mechanisms such as security processes, procedures, information security policies, and enforcement in addition to recurrent updates of their information security technologies (Bulgurcu et al. 2010, Chen et al. 2012, Dhillon and Backhouse 2000, Siponen and Vance 2010). In this climate, organizations are in need to deploy strategies to guide their security efforts and to optimize their limited (security) resources (Ahmad et al. 2014, Anderson and Choobineh 2008, Saydjari 2004). In order to ensure effective security measures and policies, organizations should implement multiple information security strategies (Richards and Davis 2010). Furthermore, an emerging view suggests that an

effective deployment of information security requires an interplay of processes that take into account information security investments for resources and how they impact the organizational performance (Al Hogail 2015, Boss et al. 2015, Burns et al. 2017, Hsu et al. 2015, Posey et al. 2013, Stanton et al. 2009, Vance et al. 2015). If suitable processes are to be implemented within an organization, questions in which resources to invest in, what technologies and methods to use and how they influence the organization itself can be answered fast and reliably (Dhillon and Torkzadeh 2006). The relationship between information technology (IT) and its impact on organizational performance is well researched (e.g., Bharadwaj (2000), Brynjolfsson and Hitt (2000), Henderson and Venkatraman (1993), Mahmood and Mann (1993), Melville et al. (2004)). However the "*information security trilogy*" - analogue to the "*information technology trilogy: business strategy, technological deployment and organizational performance*" (Croteau and Bergeron 2001, p. 77) - arguably merits more attention and research efforts. The *business strategy* is the alignment of investment decisions made by the organization to improve its organizational performance (Croteau and Bergeron 2001, Luftman and Brier 1999). The *technological deployment* refers to the strategic use of information technology, e.g., to provide a competitive advantage or meet other strategic organizational targets (Bergeron et al. 1991, Bergeron and Raymond 1995, Croteau and Bergeron 2001).

The information security trilogy is closely related to the emerging view of an interdependent process comprising the allocation of security investments, their implementation, as well as complementary measurement and optimization efforts (Humphreys 2008, Karyda et al. 2005). Regarding information security, the *business strategy* relates to information security investment decisions and researchers tended to be aware of the lack of studies on this aspect and made substantial progress in extending the understanding of organizations' information security investments (Xu et al. 2017). In terms of *technological deployment*, research focuses on updating the current information security technologies and deploying new either proactive or reactive technologies (Venter and Eloff 2003). The technological deployment also includes the analysis of vulnerability occurrences over time and the consideration of corresponding insights in managerial decisions. For example, vulnerability predictions may support software portfolio management practices, including acquisition or discontinuation decisions (Kraemer et al. 2009, Roumani et al. 2016). Concerning the evaluation of the organizational security performance, information security researchers developed taxonomies for metrics (Savola 2007), models (Wang 2005) or frameworks (Veiga and Eloff 2007). These trends reflect a rising interest in information security research in aligning information security to organizational objectives and thereby shifting from a technical issue towards a value-enabling role (Ezingeard et al. 2005, Huang and Hu 2007, Rathnam et al. 2005).

The backbone of this information security trilogy - *business strategy*, *technological deployment* and *organizational performance* - and the related decision problems can be instantiated and framed by the process theory of Soh and Markus (1995). They theorize that the impact

of IT investments on an organization's performance is the outcome of the interplay between three processes (Hu and Quan 2005): The *IT conversion process*, in which IT investments become IT resources[3]; the *IT use process*, in which IT resources form impacts; and the *competitive process*, in which IT impacts are transformed into organizational performance (Hu and Quan 2005, Scheepers and Scheepers 2008, Soh and Markus 1995, Srivastava and Teo 2007, Thiesse et al. 2009, Vermerris et al. 2014). The *IT conversion process* describes the transformation of IT investments into resources. It targets decision problems of investments and the "*right product*" (Saunders and Jones 1992, p. 74) for the firm. In the context of information security, I will address an instantiation of this decision problem: Based on a comprehensive review of the state-of-the-art, I examine how firms make their information security investment decisions in order to generate resources, and how they learn from past investments and their transformation into resources. The *IT use process* describes the information technology resources utilized in organizational environments and how they assure a smooth running of a firm's business operations. In my dissertation, I will address decision problems that relate to a smooth operation of business process which include an efficient incident management and the prediction of information security vulnerabilities. The *competitive process* describes the impact information technology has on an organization and covers the decision problem of measuring it (Bulchand-Gidumal and Melián-González 2011, Soh and Markus 1995). In my dissertation, I adapt this phase as the information security competitive process to address information security performances in an organizational setting. I provide requirements for information security metrics which are often used to measure the organizational security performance (Chapin and Akridge 2005).

These lines are further explored in the next section. I will explain the process theory of Soh and Markus (1995) and apply this model in the context of information security to frame my research.

[3] The original theory of Soh and Markus (1995) regards assets as valuable firm-specific resources so that I adopt the term "*assets*" as "*resources*" which is in alignment with the literature (cf. Grover et al. (2007), Melville et al. (2004), Nevo and Wade (2011), Piccoli and Ives (2005), Teece et al. (1997), Wade and Hulland (2004)). Accordingly, resources are *firm-specific, difficult to imitate, and often valuable, i.e., they enable the firm to improve efficiency*" (Melville et al. 2004, p. 289) and reflect the intention of Soh and Markus (1995). Therefore, I refer to the definition of Melville et al. (2004) and use the term resources as defined instead of assets throughout this dissertation.

1.2 Decision Problems in Information Security: A Process Theory-Based Approach

This section outlines the frame of my research. In the following, I present the adaptation of Soh and Markus (1995)'s process theory by applying it to the information security context as this allows information security to be aligned with its organizational information security performance. In particular, after having explained the process theory of Soh and Markus (1995), I will describe first the "*information security conversion process*", in which the conversion of information security investments to resources are represented and the underlying decision and evaluation processes are analyzed, second, the "*information security technologies / methods use process*", in which information security technologies and methods, forming operational information security impacts, are considered, and third, the *information security competitive process* in which organizational information security performance is examined.

1.2.1 Information Technology and Decision Problems: Soh and Markus (1995)'s Process Theory

Researchers have conducted several studies to examine the organizational impact of IT (Gholami and Kohli 2015), starting with seminal works of Weill and Olson (1989), Weill (1992) and followed by studies of Beath et al. (1994), Grabowski and Lee (1993), Lucas (1993), Markus and Soh (1993), Ross and Beath (2002), Sambamurthy and Zmud (1994). Soh and Markus (1995) integrated these works and formulated a process theory of information technology and the linkage with organizational performance.

The basic effects of IT investments on organizational performance are adopted from Markus and Soh (1993), IT resources and their linkage to IT impacts are derived from Markus and Soh (1993), Sambamurthy and Zmud (1994), Weill and Olson (1989), Weill (1992) and the appropriate use of IT are excerpted from Grabowski and Lee (1993) and Lucas (1993). The following figure illustrates the process theory (Soh and Markus 1995):

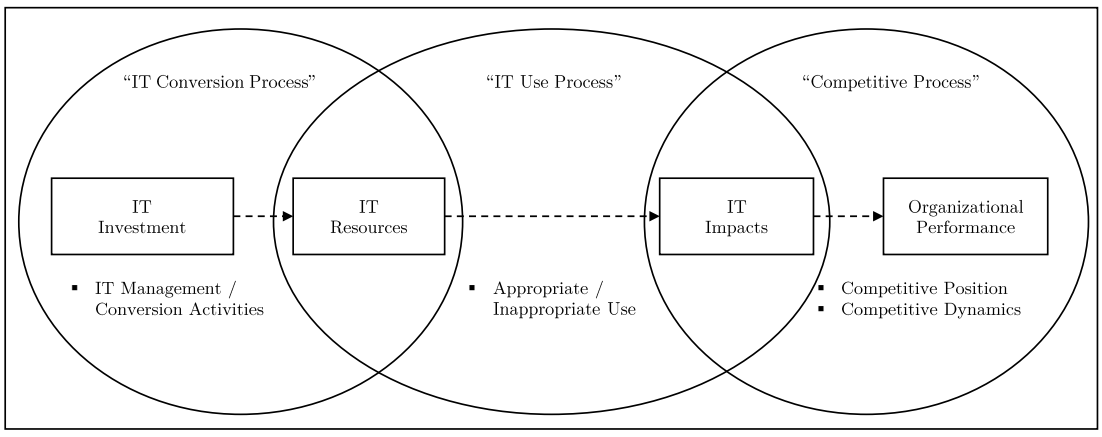

Fig. 1: Process Theory based on Soh and Markus (1995).

The process theory consists of three major phases, with the first one being the "*IT conversion process*": This process transforms IT investments into IT resources (Soh and Markus 1995). Although investment is necessary, it is not a sufficient condition to ensure the conversion into a resource which, in turn, has an impact (Smith and Crossland 2008). The outcome of an IT resource depends on its deployment, which involves solving decision problems such as establishing decision processes, developing an IT strategy, creating the necessary organizational structures, and focusing on initiatives and the effective management of IT projects (Banker et al. 2002, Queenan et al. 2011, Smith and Crossland 2008, Soh and Markus 1995).

According to the theory, IT resources exert IT impacts, which is depicted in the "*IT use process*": IT impacts are specified as new or improved products or services, transformed business processes, enriched organizational intelligence, as well as dynamic organizational structures (Sambamurthy and Zmud 1994, Soh and Markus 1995). These impacts occur when employees and organizational units use IT resources (i.e., technologies and skills) appropriately (Soh and Markus 1995). A precondition for "*appropriateness*" is to design and deploy useful applications, flexible IT infrastructures and high levels of user IT knowledge and skills (Peppard and Ward 2004, Soh and Markus 1995). If this is not given, the impact may not materialize since knowledge and data on their own are not sufficient to produce impacts (Sambamurthy and Zmud 1994, Soh and Markus 1995). Thus, organizations are challenged by decision problems such as deciding how to allocate their application portfolio, what technologies to update, which new technologies to launch, how technologies develop over time and how to train their employees to use information technology effectively.

The "*competitive process*" describes the effects of internal impacts on the organizational performance (Smith and Crossland 2008): It links the incorporation of IT in products and services as well as the effective redesign of business processes by means of IT, which results in better organizational performance (Bulchand-Gidumal and Melián-González 2011, Soh and Markus 1995). It also includes the enhancement, via IT, of the decision maker's ability to make decisions to increase organizational performance and the contribution of IT to enhance flexible organizational structures that are beneficial to the organization, to its customers, and its suppliers (Bulchand-Gidumal and Melián-González 2011, Kumar et al. 2003, Zhu et al. 2006). A main challenge for the organization is to measure the impact on organizational performance (Gholami and Kohli 2015, Kohli and Sherer 2002, Kohli and Devaraj 2003, Sabherwal and Jeyaraj 2015). Organizational performance refers to market-oriented and financial objectives within a competitive environment, which necessitates the measurement of the performance, the quantification of the transformation into resources and impact as well as the measurement of influence on the organization itself (Li et al. 2006, Schryen 2013, Yamin et al. 1999).

1.2.2 A Process Theory-Based Approach to Decision Problems in Information Security

In this subsection, I describe the adaption of Soh and Markus (1995)'s process theory in the context of information security and frame my research contributions within the theory. Figure 2 illustrates the adapted theory:

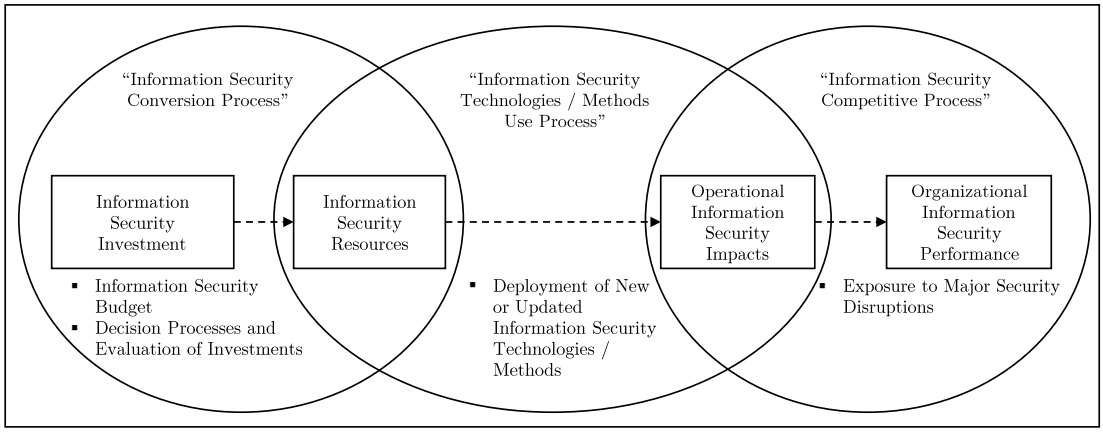

Fig. 2: Decision Problems in Information Security: A Process Theory based on Soh and Markus (1995).

Information Security Conversion Process

Analogously to the original theory, the first phase covers the "*information security conversion process*", which contains investments on information security resources. Information security resources can similarly be defined as IT resources, i.e., firm specific, challenging to copy, and often valuable (Grover et al. 2007, Nevo and Wade 2011, Piccoli and Ives 2005, Melville et al. 2004, Teece et al. 1997, Wade and Hulland 2004). In the security context, such resources might include "*security personnel, IT security applications, physical/technical equipment, or security procedures or policies*" (Kwon and Johnson 2013, p. 44) which "*enable the firm to improve efficiency*" (Melville et al. 2004, p. 289). One of the main challenges for transforming information security investments into information security resources is the nature of information security itself: "*Information security is intangible*" (Nosworthy 2000, p. 338), making it "*a difficult issue*" (Tsiakis and Stephanides 2005, p. 106) in terms of adequate measurement and quantification. Information security can be conceptualized as the security objectives of confidentiality, integrity, and availability of information[4] which ought to be ensured by information security resources (Bodin et al. 2005). Valuing investments in terms of these security objectives is difficult from

[4] Information confidentiality refers to the extent to which organizational information is kept from being disclosed, exposed or appropriated (Chang and Wang 2011, Lee et al. 2004, Schultz et al. 2001, Wang and Strong 1996); information integrity is the status that information has not been subjected to modification or forgery (Chang and Wang 2011, Lee et al. 2004, Shih and Wen 2003); and information availability refers to the extent to which information is readily accessible, whenever and wherever access is required (Chang and Wang 2011).

an accounting perspective unless there is a breach (Ruighaver et al. 2007) and if information security is regarded solely as an operational part of the IT, the intent to undertake information security investments may be difficult (Johnston and Hale 2009, Rhee et al. 2012, Tu et al. 2018). Furthermore, spending money on information security is not in itself sufficient to transform it into a resource: For example, the investment in a countermeasure such as a backup server is not effective when corresponding backup procedures and responsibilities are not established and when data recovery processes are not tested.

Information security investment research has gained attention since the early 2000s[5] and transformation processes of information security investments into information security resources are a fundamental part of these research efforts. The academic literature highlights three key issues (i.e., the optimal amount of information security investment, the allocation of this investment, and how to transform this investment effectively) that any organization needs to determine in order to turn their investments into information security resources (Huang et al. 2014). Concerning the optimal amount of information security investments, the academic literature has hereto provided a multitude of approaches (cf. e.g., Bodin et al. (2005), Bojanc and Jerman-Blažič (2012), Gordon and Loeb (2002), Hausken (2006), Willemson (2006), Wu et al. (2018)). These approaches commonly examine the optimal amount of investment, with security breach probability functions leading to guideline insights for decision makers to determine the optimal level of security investments (Huang et al. 2008). The second main issue, the allocation of information security investments, is addressed from the point of selecting and prioritizing security technologies as an allocation of the information security investment itself (Huang et al. 2014). The approaches range from the selection of network security countermeasures (Viduto et al. 2012) to the selection of optimal countermeasure portfolios in IT security planning (Sawik 2013). The third key subject is the effective transformation of information security investments, which is closely linked to the deployment of the resources (Ezhei and Tork Ladani 2018). The academic literature has, for example, examined how investments, such as the installment of IT security controls, become a resource: One of the key preconditions for such transformations is the know-how and technical knowledge created by a firm's employees via learning processes (Kwon and Johnson 2014). This is closely related to the claim that to achieve such transformations, information security practices should become tacit procedural knowledge (Merete Hagen et al. 2008, Thomson and von Solms 2006), and decision makers should determine security priorities and investment activities in the light of their business operations in order to turn them into resources (Rowe and Gallaher 2006).

As outlined, the objective of achieving such transformations effectively and economically has been an important research topic for a long time (Kwon and Johnson 2014). Synthesizing the insights of prior research, I pose therefore the following research question:

[5] For example, the Workshop on the Economics of Information Security (WEIS) which is the leading forum for information security economics research, has been initiated in 2002.

- **RQ 1:** *How has the academic literature contributed to information security investment research on transforming investments into information security resources?*

Paper 1 operationalizes and addresses this research question by synthesizing the information security investment research based on the resource-based view (Wernerfelt 1984, Melville et al. 2004) and the organizational learning theory (Argyris 1976, 1977, 1982, 1983, Argyris et al. 1985), both established theories in the information systems (IS) literature. Adopting this multi-theoretical view allows to cover research streams that explain the transformation of investments into resources. Therefore, this paper provides an overview of information security investment research, lays the foundation to answer RQ 1 and identifies aspects that have heretofore been underresearched.

As pointed out before, a crucial point of an information security resource is to ensure a maximum enforcement of the security objectives (i.e., confidentiality, integrity, and availability). However, given the fact that "*no organization can be completely secure without unlimited budget*" (Huang et al. 2014, p. 1), the greatest challenge is to determine the allocation of the information security budget. For the goal of defining an information security budget, it is important for an organization to determine the appropriate amount of investment before undertaking the investment itself (Huang et al. 2014). For this task, the academic literature suggests to use decision processes which are carried out as ongoing processes throughout the year, rather than an annual event or relying on past year's budget (Beebe et al. 2014). The academic literature offers multiple theoretical considerations and approaches assuming that all investments, and transforming these investments into resources have been accurately estimated and a rational decision process is followed (e.g., Cavusoglu et al. (2004a,b, 2008), Gal-Or and Ghose (2005), Herath and Herath (2008), Zafar and Clark (2009)).

However, these studies do not add to our understanding of how practitioners currently make security investment decisions, nor do they explain those decisions. Furthermore, these studies do not include learning strategies on how past investments were turned into information security resources (Young et al. 2012). All these studies of information security investment research, albeit extensive, adopted a normative philosophy and due to this, there is a lack of insights on understanding 1) the cognitive processes used by practitioners when making security investment decisions (Young et al. 2012), and 2) how these investments are turned into resources for the firm. In order to provide insights into what the basis of turning information security investments into resources is in practice, I pose the following research questions:

- **RQ 2:** *How do firms transform information security investments into information security resources?*
- **RQ 3:** *How do firms learn from these transformations of past information security resources?*

These two research questions are addressed in Paper 2 by developing a theory-based exploratory multiple case study using the resource-based view (Wernerfelt 1984, Melville et al. 2004) in addition to the organizational learning theory (Argyris 1976, 1977, 1982, 1983, Argyris et al. 1985). In this paper, insights into actual investment of firms and the transformation of these investments into resources, how firms evaluate these transformations and how they learn from past investments and transformations are outlined. The case study shows inter alia that 1) organizations in the sample do not use standardized decision processes for information security investments, 2) the impact of transformations, such as establishing security processes, on the business operations is perceived negatively, and that 3) learning from past investment decisions primarily arise at an ad-hoc basis.

Information Security Technologies / Methods Use Process

The second phase of the process theory of Soh and Markus (1995) attends to the information technology use, which, in the information security context, can be framed as "*information security technologies / methods use process*". In line with the original theory, the main objective of information security is to ensure uninterrupted business operations, which is achieved by the deployment of new, updated or improved technologies. The preconditions hold the same as in the original theory: The deployment of novel information security applications, flexible information security infrastructures, analysis and prediction of vulnerabilities or training employees in information security ought to be aimed at an operational information security impact. An operational information security impact can be, for example, the reduction of the number of security incidents, a quicker reaction to incidents, better authorization and access control, or improved monitoring of a firm's network traffic. It also can include the analysis of information security vulnerabilities in order to take decisions such as acquiring/deploying a new software or discontinuing a software due to security concerns (Kraemer et al. 2009, Roumani et al. 2016).

Although organizations invest in new information security technologies such as information security tools, establishing a security department or training employees, the amount of security incidents and breaches continues to be a significant problem (Safa et al. 2016, Ifinedo 2012). Organizations face various increasingly sophisticated and targeted cybercriminal attacks, which becomes evident when considering some of the more prominent security incidents of the last years; for example, data breaches have been reported at an array of companies including Tesco Bank, Yahoo, Target, Anthem, Ashley Madison, eBay, JP Morgan Chase, Home Depot, Sony Pictures Entertainment, Global Payments Inc., Tricare, Citibank and Heartland Payment Systems (Integrhythm 2017). In order to respond to these incidents, firms employ technological countermeasures, such as security information and event management systems, firewalls, security endpoints, identity and access management tools, as well as other network security systems (Bhatt et al. 2014, Senk 2013). A 2016 study by the IT analyst firm Enterprise Strategy Group

disclosed that firms in North America increase security automation and orchestration[6] for incident responses. The study is based on a survey of 100 IT professionals with knowledge or responsibility for their organizations' incident response processes and technologies (Business Wire 2016). The survey explored the drivers of this shift, identifying the shortage of qualified IT security experts and the reliance on manual resources as the main contributing factors (Business Wire 2016). The study further reports that 91 percent of the respondents think that incident response efficiency and effectiveness are limited by time and effort of manual processes. In addition, 91 percent also state they actively try to increase the size of their incident response staff as the security skills gap combined with heavy reliance on manual resources aggravate incident response issues (Business Wire 2016, Hexadite 2016). In line with our theory, an effective and efficient scheduling of corresponding tasks is one of the critical issues in order to reduce security incidents and it provides an important operational information security impact. Therefore, I pose the following research question:

- **RQ 4:** *How can security incidents be optimally assigned and scheduled to IT staff members in order to minimize the total completion time of security incidents?*

This research question is targeted in Paper 3 by drawing on methods of operations research. Specifically, the paper proposes an optimization model for assigning and scheduling security incidents to IT staff members. The work therefore contributes to decision analytics in the area of information security. First, the practical applicability of the proposed approach is shown by the development of efficient solution heuristics. Second, the research findings demonstrate that the newly developed heuristic improves the current best practice by up to 60% in terms of minimizing the total completion time of trouble tickets. At the same time, the algorithm's low execution time makes it suitable for application in practice.

In alignment with our theoretical backbone, another issue is the actual occurrence of incidents and their development over time which may have an impact on the operational information security performance. Information security incidents caused by vulnerabilities, as argued, consume time of employees (e.g., developers who fix the vulnerabilities) and also have severe financial impacts on firms. Although actual monetary costs of reputation damage is hard to quantify, the results of the 2015 global IT Security Risks survey conducted by Kaspersky Lab estimate the average losses of reputation damage as $8,653 for small and medium-sized businesses (SMB) and $204,750 for enterprises (Kaspersky Lab 2015). In particular, according to Cisco's 2016 Annual Security Report, SMBs are still less secure than enterprises (SolarWinds 2016). The reasons for this range from having no dedicated security team, using outdated hardware and security solutions to lacking the security protocols around intrusion and vulnerability protection, which leaves them prone to attacks (Cisco 2016). While firms invest in information security technologies in order to reduce susceptibility, an interesting finding is released by a report which found

[6] *Orchestration* refers to an information security response that aligns people, process, and technology involved in responding to and mitigating information security threats (IBM Resilient 2017).

that security products themselves are some of the most vulnerable software (CSO 2016a). The threats that arise from vulnerabilities are manifold, e.g., loss or theft of personal data, loss or theft of commercially sensitive information, inoperable IT systems, or making the business unable to function after being hacked, which all can lead to serious financial damages (Contractor UK 2016). Thus, given the substantial threat associated with these vulnerabilities, it is important to consider the history and development of vulnerabilities of a specific (system / software) product over time.

Vulnerability prediction models can be used to assess security threats and estimate the resources for handling potential security breaches over time. For instance, the expected number of vulnerabilities can be used as a measure of trustworthiness before a certain software product is acquired (Kim et al. 2007) or discontinued. Furthermore, assessing the expected number of vulnerabilities can provide valuable input for allocating and prioritizing limited resources to the inspection, patching and testing of an existing software portfolio (Kim et al. 2007, Shin et al. 2011, Walden et al. 2014). The overall impact of security vulnerabilities can be estimated based on the amount of their potential collateral damage and the frequency of their occurrences. Examining vulnerabilities over time shows that their structure is unique. Vulnerabilities are rare events (Shin et al. 2011) and there are several months in which no vulnerabilities are reported. Second, with respect to those months where vulnerabilities are observed, there are a few periods where a comparatively high number of vulnerabilities is reported. It is therefore necessary to examine how the development of vulnerabilities is affected by content-specific characteristics, i.e. the analyzed software as well as methodological properties, i.e. the applied forecasting technique. Consequently, this implies that the prediction accuracy can differ due to the characteristics of the forecasting methodology.

These line of thoughts regarding the impact of forecasting methodologies leads thus to the following research question:

- **RQ 5:** *How accurately can different forecasting methodologies predict IT security vulnerabilities?*

The research question is addressed by an empirical application of a broad set of prediction methodologies to a set of software and system packages, including Internet browsers, office solutions and operating systems (Paper 4). With this analysis, I contribute to the rising stream of research on information security vulnerability prediction by analyzing the effectiveness of prediction methodologies which take into account the uniqueness and rareness of vulnerability time series and by applying forecasting metrics that are suitable in this context. The obtained empirical results show that the choice of a forecasting methodology depends on the software or system package as some methods are not suitable in the context of IT security vulnerabilities. Furthermore, the study reviews the pros and cons of forecasting error metrics and argues for using absolute error forecasting metrics which have not been in the focus of prior research. It further outlines that absolute metrics can cover the actual prediction error precisely and

highlights that the accuracy results of the forecasting methodologies are robust in terms of the independence from the applied metrics.

Information Security Competitive Process

The original theory of Soh and Markus (1995) requires the measurement of the link of information technology and its impact on an organizational setting. In the context of information security, organizations need to assess the impact of their information security performance (Huang et al. 2006). I therefore instantiate this competitive process phase to measure the organizational security performance which includes, for example, the measurement of exposure to major security disruptions. Furthermore, a plethora of regulatory, financial and statutory requirements demand the measurement of information security itself (Ryan and Ryan 2008). Firms need to measure the effectiveness of their information security performance in order to make the right decisions and to align their security needs. Information security metrics[7] can provide insights with respect to the effectiveness of an organization's information security management system (ISO 2016). For example, from an economic perspective, measures that reveal success and failures of past actions can be used to justify additional budget to update or install new IT security countermeasures. From an organizational perspective, metrics can measure the maturity of a security program's overall efficiency (Merete Hagen et al. 2008). In general, information security metrics can enable the IT security department to quantify the effectiveness of the alignment with IT procedures or to explore the compliance with the firm's security policy. Information security metrics can further be applied to diagnose weaknesses and facilitate benchmark comparisons as well as to identify areas of improvements of information systems (Frankland 2008). Finally, not only from an economic perspective, the security department can show decision makers how existing and planned IT security programs align with business needs.

Regardless of the measures in place or applicable regulation (Ryan and Ryan 2008), the US National Institute of Standards and Technology (NIST) states that "*information security metrics must yield quantifiable information for comparison purposes, apply formulas for analysis, and track changes using the same points of reference*" (Chew et al. 2008, p. 9). However, the quantitative evaluation of the security controls within an organization is a task that has not been addressed sufficiently since the inception of information security as a research field (Pereira and Santos 2014). Nonetheless, the area has received attention lately (Jansen 2009). The academic literature struggles with information security metrics (Almasizadeh and Azgomi 2014, Fenz 2010) and highlights various factors that make the quantification of information security difficult. These include a deficiency of applicable estimators of security levels as well as the reliance on

[7] The terms "*IT security metric*", "*information security metric*" and "*security metric*" are often used equivalently in the academic literature (cf., e.g., Fenz (2010), Jansen (2011), Pereira and Santos (2014)) so that I also use the terms synonymously. I derive requirements and provide a definition in Paper 5 in Subsection 4.1.

subjective, human and qualitative input to obtain measurements (Jansen 2011). As there only exist best practice suggestions, this leads to the following research question:

- **RQ 6:** *Which requirements should IT security metrics fulfill?*

This research question is addressed in Paper 5 by adopting a methodological approach based on the argumentation theory and an accompanying literature review. In this study, I derive five key requirements against which IT security metrics can be evaluated and which can help decision makers when measuring the organizational security performance. In summary, I contend that IT security metrics should be (a) bounded, (b) metrically scaled, (c) reliable, valid and objective, (d) context-specific and (e) computed automatically. The study illustrates and discusses the context-specific instantiation of requirements by using two practically used IT security metrics as examples and derives implications that follow from the requirements.

1.3 Phases, Research Questions and Papers: An Overview

The subsequent table illustrates the mapping of the processes from the adapted process theory of Soh and Markus (1995), the papers and their publication outlets, and the corresponding research questions. The table also identifies the paper which is currently under review.

Table 1: An Overview of the Phases, Research Questions and Papers.

Phase 1: Information Security Conversion Process			
Research Questions		**Paper**	
RQ 1:	How has the academic literature contributed to information security investment research on transforming investments into information security resources?	Paper 1	A Multi-Theoretical Literature Review on Information Security Investments using the Resource-Based View and the Organizational Learning Theory Status: Published in the *Proceedings of the Thirty-Sixth International Conference on Information Systems (ICIS 2015)*
RQ 2:	How do firms transform information security investments into information security resources?	Paper 2	Information Security Investments: An Exploratory Multiple Case Study on Decision-Making, Evaluation and Learning Status: Published in *Computers & Security*
RQ 3:	How do firms learn from these transformations of past information security resources?		
Phase 2: Information Security Technologies / Methods Use Process			
Research Questions		**Paper**	
RQ 4:	How can security incidents be optimally assigned and scheduled to IT staff members in order to minimize the total completion time of security incidents?	Paper 3	A Decision Support System for IT Security Incident Management Status: Published in the *Proceedings of the Eleventh International Conference on Trust, Privacy and Security in Digital Business (TrustBus'14)*
RQ 5:	How accurately can different forecasting methodologies predict IT security vulnerabilities?	Paper 4	Forecasting IT Security Vulnerabilities - An Empirical Analysis Status: Under Review
Phase 3: Information Security Competitive Process			
Research Question		**Paper**	
RQ 6:	Which requirements should IT security metrics fulfill?	Paper 5	Requirements for IT Security Metrics - An Argumentation Theory Based Approach Status: Published in the *Proceedings of the Twenty-Third European Conference on Information Systems (ECIS 2015)*

Part II

Research Papers

2

Phase 1: Information Security Conversion Process

2.1 Paper 1: A Multi-Theoretical Literature Review on Information Security Investments using the Resource-Based View and the Organizational Learning Theory

---

Status:	Published
Conference:	Thirty-Sixth International Conference on Information Systems (ICIS 2015)
Acceptance Date:	17 September 2015
CORE Ranking:	A*
VHB-Jourqual 3:	A
Full citation:	Weishäupl, E., Yasasin, E., and Schryen, G (2015). A Multi-Theoretical Literature Review on Information Security Investments using the Resource-Based View and the Organizational Learning Theory. In Carte, T., Heinzl, A., and Urquhart, C., editors, *Proceedings of the Thirty-Sixth International Conference on Information Systems*, pages 1-22, December 13-16, Fort Worth, Texas, USA. Association for Information Systems.
Link:	https://aisel.aisnet.org/icis2015/proceedings/SecurityIS/16/
Abstract:	The protection of information technology (IT) has become and is predicted to remain a key economic challenge for organizations. While research on IT security investment is fast growing, it lacks a theoretical basis for structuring research, explaining economic-technological phenomena and guide future research. We address this shortcoming by suggesting a new theoretical model emerging from a multi-theoretical perspective adopting the Resource-Based View and the Organizational Learning Theory. The joint application of these theories allows to conceptualize in one theoretical model the organizational learning effects that occur when the protection of organizational resources through IT security countermeasures develops over time. We use this model of IT security investments to synthesize findings of a large body of literature and to derive research gaps. We also discuss managerial implications of (closing) these gaps by providing practical examples.

2.2 Paper 2: Information Security Investments: An Exploratory Multiple Case Study on Decision-Making, Evaluation and Learning

---

Status: Published
Journal: Computers & Security
Acceptance Date: 1 February 2018
CORE Ranking: B
VHB-Jourqual 3: N/A
Full citation: Weishäupl, E., Yasasin, E., and Schryen, G. (2017). Information Security Investments: An Exploratory Multiple Case Study on Decision-Making, Evaluation and Learning. *Computers & Security*, 77:807-823.
Link: https://www.sciencedirect.com/science/article/pii/S0167404818300555

Abstract: The need to protect resources against attackers is reflected by huge information security investments of firms worldwide. In the presence of budget constraints and a diverse set of assets to protect, organizations have to decide in which IT security measures to invest, how to evaluate those investment decisions, and how to learn from past decisions to optimize future security investment actions. While the academic literature has provided valuable insights into these issues, there is a lack of empirical contributions. To address this lack, we conduct a theory-based exploratory multiple case study. Our case study reveals that (1) firms' investments in information security are largely driven by external environmental and industry-related factors, (2) firms do not implement standardized decision processes, (3) the security process is perceived to impact the business process in a disturbing way, (4) both the implementation of evaluation processes and the application of metrics are hardly existent and (5) learning activities mainly occur at an ad-hoc basis.

3

Phase 2: Information Security Technologies / Methods Use Process

3.1 Paper 3: A Decision Support System for IT Security Incident Management

Status:	Published
Conference:	Eleventh International Conference on Trust, Privacy and Security in Digital Business (TrustBus'14)
Acceptance Date:	16 May 2014
CORE Ranking:	B
VHB-Jourqual 3:	N/A
Full citation:	Rauchecker, G., Yasasin, E., and Schryen, G. (2014). A Decision Support System for IT Security Incident Management. In Eckert, C., Katsikas, S.K., and Pernul, G., editors, *Proceedings of the Eleventh International Conference on Trust, Privacy and Security in Digital Business*, pages 36-47, September 2-3, Munich, Bavaria, Germany. Springer International Publishing.
Link:	https://link.springer.com/chapter/10.1007/978-3-319-09770-1_4
Abstract:	The problem of processing IT security incidents is a key task in the field of security service management. This paper addresses the problem of effectively assigning and scheduling security incidents to the members of the IT staff. To solve this problem, we propose an innovative approach to assign staff members to security incidents by applying mathematical programming to the field of IT security management. We formulate an optimization model and propose efficient solution methods. The numerical simulations show that our approach improves current best practice behaviour significantly.

3.2 Paper 4: Forecasting IT Security Vulnerabilities - An Empirical Analysis

---

Status: Under Review

Full citation: Yasasin, E., Prester, J., Wagner, G., and Schryen, G. (2018). Forecasting IT Security Vulnerabilities - An Empirical Analysis.

Link: https://epub.uni-regensburg.de/38099/1/Forecasting%20IT%20Security%20Vulnerabilities.pdf

Abstract: Organization have to deal with a plethora of IT security threats nowadays and to ensure smooth and uninterrupted business operations, firms are challenged to predict the volume of IT security vulnerabilities and to allocate resources for fixing them. This challenge requires decision makers to assess which system or software packages are prone to vulnerabilities, what impact exploits might have, and how many vulnerabilities can be expected to occur during a certain period of time. The academic literature has increasingly drawn attention to the need for predicting IT security vulnerabilities. However, only limited research has addressed the problem of forecasting IT security vulnerabilities based on time series that deal with the specific properties of IT security vulnerabilities, i.e., rareness of occurrence and high volatility. To address this shortcoming, we apply established methods which are capable of forecasting events characterized by rareness of occurrence and high volatility. Based on a dataset taken from the National Vulnerability Database (NVD), we use the Mean Absolute Error (MAE) and Root Mean Square Error (RMSE) to measure the forecasting accuracy of single, double and triple exponential smoothing methodologies, Crostons method, ARIMA, and a neural network-based approach. We analyze the impact of the applied forecasting methodology on the prediction accuracy with regard to its robustness along the dimensions of the examined system and software packages "operating systems", "browsers" and "office solutions" and the applied metrics. To the best of our knowledge, this study is the first that analyzes the effect of prediction techniques and applies forecasting metrics that are suitable in this context. Our results show that the optimal forecasting methodology depends on the software or system package as some methods perform poorly in the context of IT security vulnerabilities, that absolute metrics can cover the actual prediction error precisely and that the prediction accuracy is robust within the two applied forecasting-error metrics.

4

Phase 3: Information Security Competitive Process

4.1 Paper 5: Requirements for IT Security Metrics - An Argumentation Theory Based Approach

Status:	Published
Conference:	Twenty-Third European Conference on Information Systems (ECIS 2015)
Acceptance Date:	5 April 2015
CORE Ranking:	A
VHB-Jourqual 3:	B
Full citation:	Yasasin, E. and Schryen, G. (2015). Requirements for IT Security Metrics - An Argumentation Theory Based Approach. In Becker, J., vom Brocke, J., and de Marco, M., editors, *Proceedings of the Twenty-Third European Conference on Information Systems*, pages 1-16, May 26-29, Münster, North Rhine-Westphalia, Germany. Association for Information Systems.
Link:	https://aisel.aisnet.org/ecis2015_cr/208/
Abstract:	The demand for measuring IT security performance is driven by regulatory, financial, and organizational factors. While several best practice metrics have been suggested, we observe a lack of consistent requirements against which IT security metrics can be evaluated. We address this research gap by adopting a methodological approach that is based on argumentation theory and an accompanying literature review. As a result, we derive five key requirements: IT security metrics should be (a) bounded, (b) metrically scaled, (c) reliable, valid and objective, (d) context-specific and (e) computed automatically. We illustrate and discuss the context-specific instantiation of requirements by using the practically used "vulnerability scanning coverage" and "mean-time-to-incident discovery" metrics as examples. Finally we summarize further implications of each requirement.

Part III

Additional Research Papers

5

List of Additional Research Papers

During my research, I contributed to additional papers which are related to the outlined topics but do not directly contribute to the research questions raised in this thesis:

- Schryen, G., Benlian, A., Rowe, F., Shirley, G., Larsen, K., Petter, S., Paré, G., Wagner, G., Haag, S., and Yasasin, E. (2017). Literature Reviews in IS Research: What Can Be Learnt from the Past and Other Fields? *Communications of the Association for Information Systems*, 41:759-774. Paper 30.
- Weishäupl, E., Kunz, M., Yasasin, E., Wagner, G., Prester, J., Schryen, G., and Pernul, G. (2015). Towards an Economic Approach to Identity and Access Management Systems Using Decision Theory. In: Pernul, G., Schryen, G., and Schillinger, R., editors, *Proceedings of the Second International Workshop on Security in Highly Connected IT Systems*, pages 1-5, September 21-22, Vienna, Austria. FORSEC Research Association.
- Weishäupl, E., Yasasin, E., and Schryen, G. (2015)[8]. IT Security Investments Through the Lens of the Resource-Based View: A new Theoretical Model and Literature Review. In: Becker, J., vom Brocke, J., and de Marco, M., editors, *Proceedings of the Twenty-Third European Conference on Information Systems*, Paper 198, May 26-29, Münster, Germany. Association for Information Systems.
- Yasasin, E., Rauchecker, G., Prester, J., and Schryen, G. (2014). A Fuzzy Security Investment Decision Support Model for Highly Distributed Systems. In: Morvan, F., Wagner, R.R., and Tjoa, A.M., *Proceedings of the Twenty-Fifth International Workshop on Database and Expert Systems Applications*, pages 291-295, September 1-5, Munich, Germany. IEEE Computer Society.
- de Meer, H., Diener, M., Herkenhöner, R., Kucera, M., Niedermeier, M., Reisser, A., Schryen, G., Vetter, M., Waas, T., and Yasasin, E. (2013). Sicherheitsherausforderungen in hochverteilten Systemen. *PIK - Praxis der Informationsverarbeitung und Kommunikation*, 36(3):153-159.

[8] This paper contributes partly to RQ 1. As Paper 1 in Subsection 2.1 is an extension of it, this paper is therefore not part of the dissertation.

Part IV

Discussion and Conclusion

6

Summary, Critical Reflection and Outlook on Future Research

This dissertation addresses decision problems in information security and develops methodologies and quantitative models framed in the adapted process theory of Soh and Markus (1995) by developing research contributions within each of the phases. In this chapter, I summarize the key findings of my research, critically reflect on their limitations and provide an outlook on future research.

Regarding the first phase, the "*information security conversion process*", I first covered research streams that explain the transformation of investments into resources and identified research gaps driven by and organized along a new theoretical model for information security investments based on the integrative application of the resource-based view (Melville et al. 2004) and the organizational learning theory (Argyris 1976, 1977, 1982, 1983, Argyris et al. 1985). By doing so, open research issues were identified, each of which builds on either or both of the theories. For instance, the transformation of investments into resources primarily builds on the resource-based view as the theoretical backbone, whereas feedback mechanisms are mainly built upon the organizational learning theory. Regarding the latter theory, the study revealed that the academic literature lacks answers to the question of how past investments contribute to the transformation to information security resources. Thus, addressing the identified research gaps could provide new insights with practical and managerial implications for decision makers when undertaking information security investments. The literature review has therefore sought to contribute to information security investment research. Yet, the derived integrated model needs to be tested empirically which could be done in future research, e.g., by developing construct items and examining the investments and transformations into resources by an empirical experiment or by a longitudinal field study in a firm to track and examine the organizational changes.

As the literature revealed that it remains nebulous how firms allocate their budget, how they make their investment decisions to transform the undertaken investments into resources and how they use past investment activities in order to do so, an exploratory case study was carried out. Based on interviews conducted with both non-consulting and consulting firms, it was pointed out that organizations struggle to apply standardized decision processes for investment decisions, such as establishing security processes to achieve the targeted security objectives. Furthermore,

if some security controls are installed, they are perceived to have adverse effects on the business operations. The reason for this is that information security is regarded as not being part of the core business (Kayworth and Whitten 2012, Soomro et al. 2016). There is still a lack of clarity as to how to effect security improvements in the mindset that information security (in particular in SMEs) is a core issue in daily operations (Posey et al. 2014, Spillan and Hough 2003). To change this, senior management is in demand to stress the significance of information security (Esteves et al. 2017) and future research should concentrate on developing and accumulating human, relational, and security-related infrastructure issues to enhance the level of information security (Chang and Wang 2011). Plus, future research could also concentrate on how allocations of the budget can be achieved by considering different stakeholders' opinions, the context in which a firm operates as well as the firm's structure (Angst et al. 2017). Furthermore, there are new upcoming challenges: For instance, with the emergence of big data "*organizations are finding managing large amounts of data increasingly challenging*" (Demirkan et al. 2015, p. 735) and with the increasing volume of data, many organizations, especially corporate boards, are concerned about information security and how it impacts their business operations economically (Kayworth and Whitten 2012). Therefore, corporate IT executives steadily point out information security and privacy as an important economic factor (Kayworth and Whitten 2012, Luftman and Ben-Zvi 2009) as firms must protect not only their own information resources but also those of their customers, employees, and business partners (Lin et al. 2016). Future research might examine how information security investments will enable a firm to achieve a balance between the need for protecting their information resources against the need for enabling and improving the availability of their business processes while ensuring compliance (Albrechtsen 2015, Greenaway et al. 2015, Mehta and Bharadwaj 2015, Tvrdíková 2016). Finally, future research activities might study investments in information security and firms' performances to "*understand the extent to which information security investment leads to positive or negative firm performance*" (Bose and Luo 2014, p. 204).

The dissertation also contributed to decision problems regarding information security technologies and methods which falls into Phase 2 of the adapted process theory, the "*information security technologies / methods use process*". As pointed out in the corresponding part of Subsection 1.2.2, this phase deals with deployments of new technologies and methods aiming to achieve the security objectives and thus to enable an operational information security impact. In order to minimize the total completion time of incidents in a firm, a procedure to assign security incident tickets to members of the IT staff was developed. This optimization is intended to facilitate business operations as this ensures their smoother running. The aim of this research was to document the improvement of current best practice and the results showed that the current best practice behavior was improved by up to 60% in terms of completion time of incidents. The computational results reveal that, in the case of larger organizations which have a dedicated IT incident management team with more than 20 staff members, automatically scheduling reduced

the total completion time of an incident significantly. However, there are some limitations which can be addressed in future research. For instance, future research might consider the connection between incidents. To give a simple practical example: Think of a shutdown of an email server which will likely lead a firm's employees to open incident tickets. The root of this problem, however, lies in the restart of the email server and would solve all other trouble tickets that are related to this problem. This bundle of tickets can be grouped and solved by fixing one trouble ticket. Future research might consider these dependencies. Another improvement could be that the time for solving a ticket might be interrupted and resumed later on, e.g., when further help is needed. In the current model, each ticket was assigned to a single member of the IT staff. Yet, in practice, sometimes additional help is needed to solve a problem. And finally, as the optimization model could not be solved to optimality, other heuristics can be developed to achieve further benchmarks for the quality of their counterparts. Research activities in effective incident management during the last years include learning strategies as well. For instance, Bartnes et al. (2016) found that learning activities of IT staff members will improve incident response practices. The organizational learning theory of Argyris (1976, 1977, 1982, 1983) and Argyris et al. (1985), with its strategies of single and double-loop learning, might provide insights into training sessions and evaluations, thereby improving incident response practices (Bartnes et al. 2016). The learning aspect is also highlighted by He and Johnson (2017), who interviewed health care and IT professionals. Their study showed that firms struggle to structure the obtained incident knowledge and emphasize the need for "*double-loop organizational learning, dynamic security learning (DSL) process model, and security checklist to improve organizations' incident learning capabilities*" (He and Johnson 2017, p. 13).

The dissertation also comprises another study in Phase 2, as one of the main goals of the theory in this phase is to update or use new products. In the information security context, this aims at meeting the security objectives in order to have a positive impact on business operations. As a susceptible product might negatively effect the operational impact on a firm and given that cybercriminal activities are increasing, one of the main contributions was therefore to choose and apply suitable forecasting methods to predict IT security vulnerabilities for different software and system packages. This is essential, in particular regarding the acquisition of a new system or software, or its replacement when there are too many vulnerabilities (Mitra and Ransbotham 2015, Ruohonen et al. 2015). My research on the prediction of IT security vulnerabilities shows some significant implications including that the forecasting methodology depends on the software or system package and that absolute-error forecasting metrics can capture the actual prediction error. Regarding the results, from a managerial point of view, decision-makers can see what kind of software or system packages result in fewer vulnerabilities and which forecasting methodology is suitable for a specific product. In the context of time series analysis of IT security vulnerabilities, another area to examine in more depth might be the time between vulnerability disclosures: The research of Johnson et al. (2016) shows that the

prediction of the time between vulnerability disclosures on a per product basis is feasible. Besides including additional factors such as better version histories, future research could also examine how forecasting techniques in vulnerability assessment tools impact the vulnerability treatment and detection in organizations. And finally, in my study, published vulnerabilities were examined: Future work might also include vulnerabilities which were closed but not publicly announced by asking directly the developers of the software or system products.

In addition, the third and last phase, the "*information security competition process*", addresses the assessment of impacts of a firm's information security performance. Information security performance measurements are carried out by using metrics but there is still a "*lack of reliable metrics in measuring the security performance of organizations*" (Cavusoglu et al. 2015, p. 397). Therefore the focus was on the foundations of designing valid, objective and meaningful metrics in order to ease information security performance measurement. Security metrics are aimed at providing a quantitative and objective basis for strategic security decisions (Baker et al. 2007, Jansen 2011, Johnson and Goetz 2007), for example, by highlighting the required level of protection against threats and vulnerabilities, or by supporting the mechanisms to safeguard organizations' resources and knowledge (Fenz et al. 2014). Furthermore, security metrics can be used to bolster new projects (Ingalsbe et al. 2008). In order to support decision-making and to guide suitable metrics for the performance measurement, I developed requirements for IT security metrics and showed why they are needed theoretically. Plus, I illustrated the consequences of the lack thereof for an IT security metric that is used in practice and addressed hereby the question of how the criteria of valid, objective and meaningful metrics can be met. With this research, I hope to provide new insights through which researchers and practitioners have a starting point to construct reliable metrics on a sound basis. The study develops an approach for building a theoretical set of requirements to be fulfilled when IT security metrics are designed. To the best of my knowledge, this is the first systematic examination of the process of defining IT security metrics. Based on insights from this study, I conclude that metrics relying on the derived requirements are interpretable for decision makers. IT security metrics which meet the requirements are free from subjective estimations and based on robust quality criteria (objectivity, reliability and validity), the (automatic) computation of the metric's value is reproducible under the same test conditions. This lead to objective, valid, reliable and clearly interpretable IT security metrics and thereby decision makers can compare different IT security levels.

However, further research is still necessary. The developed requirements can be refined and/or extended by identifying additional requirements. Furthermore, in order to improve the proposed requirements, a detailed survey, with security experts as respondents, can be used to evaluate the requirements. In addition, the IT security metrics can be applied to different contexts (e.g., information security investment metrics or metrics used in IT security incident management). Hence, the identification and recognition of further research implications as well as the inclusion

of practitioners' insights should guide next steps in future research. In the information security metrics' research domain, metrics of system vulnerabilities, of defense power, of attack or threat severity, and metrics of situations were examined in a survey regarding their implementation, effectiveness, and impact (Pendleton et al. 2016). While the researchers discuss the advantages and disadvantages of those metrics, they point out "*that there are big gaps between the existing metrics and the desirable metrics*" (Pendleton et al. 2016, p. 23) and provide future directions, with which I concur: First, studies should point out the underlying definitions of the used security metrics; and second, security metrics research should be undertaken in close cooperation between industry and academia. While the latter often lacks data to validate the developed metric(s), the former is hindered in sharing information security data, which, by nature, is often sensitive (Skopik et al. 2016).

To conclude, I hope that the addressed decision problems in my dissertation will help both researchers and practitioners as starting points. For researchers, I suggest that the joint work with my colleagues can be extended by refining our approaches to make them more efficiently applicable in practice. For practitioners, I envision a higher awareness for information security-related decision problems and their managerial implications.

Part V

Bibliography

References

Ahmad, A., Maynard, S. B., and Park, S. (2014). Information Security Strategies: Towards an Organizational Multi-Strategy Perspective. *Journal of Intelligent Manufacturing*, 25(2):357–370.

Al Hogail, A. (2015). Design and Validation of Information Security Culture Framework. *Computers in Human Behavior*, 49:567–575.

Albrechtsen, E. (2015). Major Accident Prevention and Management of Information Systems Security in Technology-Based Work Processes. *Journal of Loss Prevention in the Process Industries*, 36:84–91.

Almasizadeh, J. and Azgomi, M. A. (2014). Mean Privacy: A Metric for Security of Computer Systems. *Computer Communications*, 52:47–59.

Anderson, E. E. and Choobineh, J. (2008). Enterprise Information Security Strategies. *Computers & Security*, 27(1):22–29.

Angst, C. M., Block, E. S., D'Arcy, J., and Kelley, K. (2017). When Do IT Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches. *MIS Quarterly*, 41(3):893–916.

Argyris, C. (1976). Single-Loop and Double-Loop Models in Research on Decision Making. *Administrative Science Quarterly*, 21(3):363–375.

Argyris, C. (1977). Organizational Learning and Management Information Systems. *Accounting, Organizations and Society*, 2(2):113–123.

Argyris, C. (1982). *Reasoning, Learning, and Action: Individual and Organizational.* Jossey-Bass, 2nd edition.

Argyris, C. (1983). Action Science and Intervention. *The Journal of Applied Behavioral Science*, 19(2):115–135.

Argyris, C., Putnam, R., and Smith, D. M. (1985). *Action Science: Concepts, Methods, and Skills for Research and Intervention.* Jossey-Bass, 1st edition.

Baker, W. H., Rees, L. P., and Tippett, P. S. (2007). Necessary Measures: Metric-Driven Information Security Risk Assessment and Decision Making. *Communications of the ACM*, 50(10):101–106.

Banker, R. D., Chang, H., and Kao, Y.-C. (2002). Impact of Information Technology on Public Accounting Firm Productivity. *Journal of Information Systems*, 16(2):209–222.

Bartnes, M., Moe, N. B., and Heegaard, P. E. (2016). The Future of Information Security Incident Management Training: A Case Study of Electrical Power Companies. *Computers & Security*, 61:32–45.

Beath, C., Goodhue, D., and Ross, J. (1994). Partnering for Business Value: The Shared Management of the IS Infrastructure. In Decross, J., Huff, S., and Munro, M., editors, *Proceedings of the Fifteenth International Conference on Information Systems*, pages 459–460, December 14-17, Vancouver, British Columbia, Canada. Association for Information Systems.

Beebe, N. L., Young, D. K., and Chang, F. (2014). Framing Information Security Budget Requests to Influence Investment Decisions. *Communications of the Association for Information Systems*, 35:133–143. Article 7.

Bergeron, F., Buteau, C., and Raymond, L. (1991). Identification of Strategic Information Systems Opportunities: Applying and Comparing Two Methodologies. *MIS Quarterly*, 15(1):89–103.

Bergeron, F. and Raymond, L. (1995). The Contribution of IT to the Bottom Line: A Contingency Perspective of Strategic Dimensions. In Leidner, D. and Ross, J., editors, *Proceedings of the Sixteenth International Conference on Information Systems*, pages 167–181, December 10-13, Amsterdam, The Netherlands. Association for Information Systems.

Bharadwaj, A. S. (2000). A Resource-Based Perspective on Information Technology Capability and Firm Performance: An Empirical Investigation. *MIS Quarterly*, 24(1):169–196.

Bhatt, S., Manadhata, P. K., and Zomlot, L. (2014). The Operational Role of Security Information and Event Management Systems. *IEEE Security & Privacy*, 12(5):35–41.

Bodin, L. D., Gordon, L. A., and Loeb, M. P. (2005). Evaluating Information Security Investments using the Analytic Hierarchy Process. *Communications of the ACM*, 48(2):78–83.

Böhme, R. and Moore, T. (2016). The "Iterated Weakest Link" Model of Adaptive Security Investment. *Journal of Information Security*, 7(2):81–102.

Bojanc, R. and Jerman-Blažič, B. (2012). Quantitative Model for Economic Analyses of Information Security Investment in an Enterprise Information System. *Organizacija*, 45(6):276–288.

Bose, R. and Luo, X. (2014). Investigating Security Investment Impact on Firm Performance. *International Journal of Accounting & Information Management*, 22(3):194–208.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., and Polak, P. (2015). What Do Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors. *MIS Quarterly*, 39(4):837–864.

Brynjolfsson, E. and Hitt, L. M. (2000). Beyond Computation: Information Technology, Organizational Transformation and Business Performance. *The Journal of Economic Perspectives*, 14(4):23–48.

Bulchand-Gidumal, J. and Melián-González, S. (2011). Maximizing the Positive Influence of IT for Improving Organizational Performance. *The Journal of Strategic Information Systems*, 20(4):461–478.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-based Beliefs and Information Security Awareness. *MIS Quarterly*, 34(3):523–548.

Burns, A., Posey, C., Roberts, T. L., and Lowry, P. B. (2017). Examining the Relationship of Organizational Insiders' Psychological Capital with Information Security Threat and Coping Appraisals. *Computers in Human Behavior*, 68:190–209.

Business Wire (2016). Nearly 100% of North American IT Professionals Surveyed by ESG Admit to Challenges with Incident Response. http://www.businesswire.com/news/home/20161006005128/en/100-North-American-Professionals-Surveyed-ESG-Admit. Retrieved: July 13, 2018.

Cavusoglu, H., Cavusoglu, H., and Raghunathan, S. (2004a). Economics of IT Security Management: Four Improvements to Current Security Practices. *Communications of the Association for Information Systems*, 14:65–75.

Cavusoglu, H., Cavusoglu, H., Son, J.-Y., and Benbasat, I. (2015). Institutional Pressures in Security Management: Direct and Indirect Influences on Organizational Investment in Information Security Control Resources. *Information & Management*, 52(4):385–400.

Cavusoglu, H., Mishra, M., and Raghunathan, S. (2004b). A Model for Evaluating IT Security Investments. *Communications of the ACM*, 47(7):87–92.

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

Chang, K.-C. and Wang, C.-P. (2011). Information Systems Resources and Information Security. *Information Systems Frontiers*, 13(4):579–593.

Chapin, D. A. and Akridge, S. (2005). How Can Security be Measured. *Information Systems Control Journal*, 2:1–6.

Chen, Y., Ramamurthy, K., and Wen, K.-W. (2012). Organizations' Information Security Policy Compliance: Stick or Carrot Approach? *Journal of Management Information Systems*, 29(3):157–188.

Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A., and Robinson, W. (2008). Performance Measurement Guide for Information Security. *National Institute of Standards and Technology (NIST)*.

CIO (2017). 9 Biggest Information Security Threats Through 2019. https://www.cio.com/article/3185725/security/9-biggest-information-security-threats-through-2019.html. Retrieved: July 13, 2018.

Cisco (2016). Annual Security Report. https://www.cisco.com/c/dam/assets/offers/pdfs/cisco-asr-2016.pdf. Retrieved: July 13, 2018.

Contractor UK (2016). IT Contractor Guide to Data Breach and Cyber Security Insurance. https://tinyurl.com/yd29saav. Retrieved: July 13, 2018.

Croteau, A.-M. and Bergeron, F. (2001). An Information Technology Trilogy: Business Strategy, Technological Deployment and Organizational Performance. *The Journal of Strategic Information Systems*, 10(2):77–99.

CSO (2016a). Security Products Among the Most Vulnerable Software. https://www.csoonline.com/article/3146046/security/security-products-are-among-the-most-vulnerability-riddled-software-products.html. Retrieved: July 13, 2018.

CSO (2016b). Verizon may want a $ 1 Billion Discount on Yahoo. http://www.csoonline.com/article/3129029/security/verizon-may-want-a-1-billion-discount-on-yahoo.html. Retrieved: July 13, 2018.

CSO (2017). Cost of Insider Threats vs. Investment in Proactive Education and Technology. http://www.csoonline.com/article/3215888/data-protection/cost-of-insider-threats-vs-investment-in-proactive-education-and-technology.html. Retrieved: July 13, 2018.

Demirkan, H., Bess, C., Spohrer, J., Rayes, A., Allen, D., and Moghaddam, Y. (2015). Innovations with Smart Service Systems: Analytics, Big Data, Cognitive Assistance, and the Internet of Everything. *Communications of the Association for Information Systems*, 37:733–752.

Dhillon, G. and Backhouse, J. (2000). Technical Opinion: Information System Security Management in the New Millennium. *Communications of the ACM*, 43(7):125–128.

Dhillon, G. and Torkzadeh, G. (2006). Value-Focused Assessment of Information System Security in Organizations. *Information Systems Journal*, 16(3):293–314.

Esteves, J., Ramalho, E., and De Haro, G. (2017). To Improve Cybersecurity, Think like a Hacker. *MIT Sloan Management Review*, 58(3):71–77.

Ezhei, M. and Tork Ladani, B. (2018). Interdependency Analysis in Security Investment against Strategic Attacks. *Information Systems Frontiers*, pages 1–15. In Press.

Ezingeard, J.-N., McFadzean, E., and Birchall, D. (2005). A Model of Information Assurance Benefits. *Information Systems Management*, 22(2):20–29.

Fenz, S. (2010). Ontology-Based Generation of IT-Security Metrics. In Shin, S. Y., Ossowski, S., and Schumacher, M., editors, *Proceedings of the 2010 ACM Symposium on Applied Computing*, pages 1833–1839, March 22-26, Sierre, Switzerland. Association for Computing Machinery.

Fenz, S., Heurix, J., Neubauer, T., and Pechstein, F. (2014). Current Challenges in Information Security Risk Management. *Information Management & Computer Security*, 22(5):410–430.

Frankland, J. (2008). IT Security Metrics: Implementation and Standards Compliance. *Network Security*, 2008(6):6–9.

Gal-Or, E. and Ghose, A. (2005). The Economic Incentives for Sharing Security Information. *Information Systems Research*, 16(2):186–208.

Gartner (2017). Gartner Says Worldwide Information Security Spending Will Grow 7 Percent to Reach $ 86.4 Billion in 2017. http://www.gartner.com/newsroom/id/3784965. Retrieved: July 13, 2018.

Gartner (2018). Forecast Analysis: Information Security, Worldwide, 1Q18 Update. https://www.gartner.com/doc/3878366/forecast-analysis-information-security-worldwide. Retrieved: July 13, 2018.

Gholami, R. and Kohli, R. (2015). Review of Information Technology Value Research: A Triple-Outcomes Perspective. In Cooper, C. L., Straub, D., and Welke, R., editors, *Wiley Encyclopedia of Management, Management Information Systems: Business Value of IT*, volume 7. John Wiley & Sons, Ltd, Hoboken, New Jersey.

Gordon, L. A. and Loeb, M. P. (2002). The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, 5(4):438–457.

Gordon, L. A., Loeb, M. P., and Zhou, L. (2016). Investing in Cybersecurity: Insights from the Gordon-Loeb Model. *Journal of Information Security*, 7(2):49–59.

Grabowski, M. and Lee, S. (1993). Linking Information Systems Application Portfolios and Organizational Strategy. In Banker, R., Kauffman, R., and Mahmood, M., editors, *Strategic Information Technology Management: Perspectives on Organizational Growth and Competitive Advantage*, pages 33–54, Hershey, Pennsylvania, USA. IGI Publishing.

Greenaway, K. E., Chan, Y. E., and Crossler, R. E. (2015). Company Information Privacy Orientation: A Conceptual Framework. *Information Systems Journal*, 25(6):579–606.

Grover, V., Henry, R. M., and Thatcher, J. B. (2007). Fix IT-Business Relationships through Better Decision Rights. *Communications of the ACM*, 50(12):80–86.

Hall, J. H., Sarkani, S., and Mazzuchi, T. A. (2011). Impacts of Organizational Capabilities in Information Security. *Information Management & Computer Security*, 19(3):155–176.

Hausken, K. (2006). 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.

He, Y. and Johnson, C. (2017). Challenges of Information Security Incident Learning: An Industrial Case Study in a Chinese Healthcare Organization. *Informatics for Health and Social Care*, 42(4):1–16.

Henderson, J. C. and Venkatraman, H. (1993). Strategic Alignment: Leveraging Information Technology for Transforming Organizations. *IBM Systems Journal*, 32(1):472–484.

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

Hexadite (2016). Security Orchestration and Automation: Closing the Gap in Incident Response.
http://secure.hexadite.com/security-orchestration-automation-survey. Retrieved: July 13, 2018.

Hsu, J. S.-C., Shih, S.-P., Hung, Y. W., and Lowry, P. B. (2015). The Role of Extra-Role Behaviors and Social Controls in Information Security Policy Effectiveness. *Information Systems Research*, 26(2):282–300.

Hu, Q. and Quan, J. (2005). Evaluating the Impact of IT Investments on Productivity: A Causal Analysis at Industry Level. *International Journal of Information Management*, 25(1):39–53.

Huang, C. D., Behara, R. S., and Goo, J. (2014). Optimal Information Security Investment in a Healthcare Information Exchange: An Economic Analysis. *Decision Support Systems*, 61:1–11.

Huang, C. D. and Hu, Q. (2007). Achieving IT-Business Strategic Alignment via Enterprise-Wide Implementation of Balanced Scorecards. *Information Systems Management*, 24(2):173–184.

Huang, C. D., Hu, Q., and Behara, R. S. (2008). An Economic Analysis of the Optimal Information Security Investment in the Case of a Risk-Averse Firm. *International Journal of Production Economics*, 114(2):793–804.

Huang, S.-M., Lee, C.-L., and Kao, A.-C. (2006). Balancing Performance Measures for Information Security Management: A Balanced Scorecard framework. *Industrial Management & Data Systems*, 106(2):242–255.

Humphreys, E. (2008). Information Security Management Standards: Compliance, Governance and Risk Management. *Information Security Technical Report*, 13(4):247–255.

IBM Resilient (2017). What is Incident Response Orchestration?
https://www.resilientsystems.com/cyber-resilience-knowledge-center/incident-response-blog/incident-response-orchestration/. Retrieved: July 13, 2018.

Ifinedo, P. (2012). Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory. *Computers & Security*, 31(1):83–95.

Information Security Forum (2017). Threat Horizon 2019: Disruption. Distortion. Deterioration.
https://www.securityforum.org/research/threat-horizon-2on-deterioration/. Retrieved: July 13, 2018.

Ingalsbe, J. A., Kunimatsu, L., Baeten, T., and Mead, N. R. (2008). Threat Modeling: Diving into the Deep End. *IEEE Software*, 25(1):28–34.

Integrhythm (2017). Security Incidents: Who is Coordinating a Response?
https://www.integrhythm.com/insights/security-incidents-response-with-servicenow-secops. Retrieved: July 13, 2018.

ISO (2016). How to Measure the Effectiveness of Information Security. https://www.iso.org/news/2016/12/Ref2151.html. Retrieved: July 13, 2018.

Jansen, W. (2009). Directions in Security Metrics Research. Technical report, National Institute of Standards and Technology Interagency Report. http://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7564.pdf. Retrieved: July 13, 2018.

Jansen, W. (2011). Research Directions in Security Metrics. *Journal of Information System Security*, 7(1):3–22.

Johnson, M. E. and Goetz, E. (2007). Embedding Information Security into the Organization. *IEEE Security & Privacy*, 5(3):16–24.

Johnson, P., Gorton, D., Lagerström, R., and Ekstedt, M. (2016). Time between Vulnerability Disclosures: A Measure of Software Product Vulnerability. *Computers & Security*, 62:278–295.

Johnston, A. C. and Hale, R. (2009). Improved Security through Information Security Governance. *Communications of the ACM*, 52(1):126–129.

Jouini, M., Rabai, L. B. A., and Aissa, A. B. (2014). Classification of Security Threats in Information Systems. *Procedia Computer Science*, 32:489–496.

Karyda, M., Kiountouzis, E., and Kokolakis, S. (2005). Information Systems Security Policies: A Contextual Perspective. *Computers & Security*, 24(3):246–260.

Kaspersky Lab (2015). Damage Control: The Cost of Security Breaches. https://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf. Retrieved: July 13, 2018.

Kayworth, T. and Whitten, D. (2012). Effective Information Security Requires a Balance of Social and Technology Factors. *MIS Quarterly Executive*, 9(3):163–175.

Kim, J., Malaiya, Y., and Ray, I. (2007). Vulnerability Discovery in Multi-Version Software Systems. In Cukic, B. and Dong, J., editors, *Proceedings of the Tenth IEEE High Assurance Systems Engineering Symposium*, pages 141–148, November 14-16, Plano, Texas, USA. IEEE Computer Society.

Kohli, R. and Devaraj, S. (2003). Measuring Information Technology Payoff: A Meta-Analysis of Structural Variables in Firm-Level Empirical Research. *Information Systems Research*, 14(2):127–145.

Kohli, R. and Sherer, S. A. (2002). Measuring Payoff of Information Technology Investments: Research Issues and Guidelines. *Communications of the Association for Information Systems*, 9(1):241–268.

Kraemer, S., Carayon, P., and Clem, J. (2009). Human and Organizational Factors in Computer and Information Security: Pathways to Vulnerabilities. *Computers & security*, 28(7):509–520.

Kumar, V., Maheshwari, B., and Kumar, U. (2003). An Investigation of Critical Management Issues in ERP Implementation: Emperical Evidence from Canadian Organizations. *Technovation*, 23(10):793–807.

Kwon, J. and Johnson, M. E. (2013). Health-Care Security Strategies for Data Protection and Regulatory Compliance. *Journal of Management Information Systems*, 30(2):41–66.

Kwon, J. and Johnson, M. E. (2014). Proactive Versus Reactive Security Investments in the Healthcare Sector. *MIS Quarterly*, 38(2):451–471.

Lee, Y. W., Pipino, L., Strong, D. M., and Wang, R. Y. (2004). Process-Embedded Data Integrity. *Journal of Database Management*, 15(1):87–103.

Li, S., Ragu-Nathan, B., Ragu-Nathan, T., and Rao, S. S. (2006). The Impact of Supply Chain Management Practices on Competitive Advantage and Organizational Performance. *Omega*, 34(2):107–124.

Lin, X., Zhang, D., and Li, Y. (2016). Delineating the Dimensions of Social Support on Social Networking Sites and their Effects: A Comparative Model. *Computers in Human Behavior*, 58:421–430.

Lowry, P. B., Dinev, T., and Willison, R. (2015). Call for Papers: European Journal of Information Systems (EJIS) Special Issue on Security and Privacy in 21st Century Organisations. https://perma.cc/53DS-TEMS. Retrieved: July 13, 2018.

Lucas, H. J. (1993). The Business Value of Information Technology: A Historical Perspective and Thoughts for Future Research. In Banker, R., Kauffman, R., and Mahmood, M., editors, *Strategic Information Technology Management: Perspectives on Organizational Growth and Competitive Advantage*, pages 359–374, Hershey, Pennsylvania, USA. IGI Publishing.

Luftman, J. and Ben-Zvi, T. (2009). Key Issues for IT Executives 2009: Difficult Economy's Impact on IT. *MIS Quarterly Executive*, 9(1):203–213.

Luftman, J. and Brier, T. (1999). Achieving and Sustaining Business-IT Alignment. *California Management Review*, 42(1):109–122.

Mahmood, M. A. and Mann, G. J. (1993). Measuring the Organizational Impact of Information Technology Investment: An Exploratory Study. *Journal of Management Information Systems*, 10(1):97–122.

Markus, M. L. and Soh, C. (1993). Banking on Information Technology: Converting IT Spending into Firm Performance. In Banker, R., Kauffman, R., and Mahmood, M., editors, *Strategic Information Technology Management: Perspectives on Organizational Growth and Competitive Advantage*, pages 375–403, Hershey, Pennsylvania, USA. IGI Publishing.

Mehta, N. and Bharadwaj, A. (2015). Knowledge Integration in Outsourced Software Development: The Role of Sentry and Guard Processes. *Journal of Management Information Systems*, 32(1):82–115.

Melville, N., Kraemer, K., and Gurbaxani, V. (2004). Review: Information Technology and Organizational Performance: An Integrative Model of IT Business Value. *MIS Quarterly*, 28(2):283–322.

Merete Hagen, J., Albrechtsen, E., and Hovden, J. (2008). Implementation and Effectiveness of Organizational Information Security Measures. *Information Management & Computer*

Security, 16(4):377–397.

Mitra, S. and Ransbotham, S. (2015). The Effects of Vulnerability Disclosure Policy on the Diffusion of Security Attacks. *Information Systems Research*, 26(3):565–584.

Nevo, S. and Wade, M. (2011). Firm-Level Benefits of IT-Enabled Resources: A Conceptual Extension and an Empirical Assessment. *The Journal of Strategic Information Systems*, 20(4):403–418.

Nosworthy, J. D. (2000). Implementing Information Security in the 21st Century - Do you have the Balancing Factors? *Computers & Security*, 19(4):337–347.

Pendleton, M., Garcia-Lebron, R., Cho, J.-H., and Xu, S. (2016). A Survey on Systems Security Metrics. *ACM Computing Surveys*, 49(4):1–35.

Peppard, J. and Ward, J. (2004). Beyond Strategic Information Systems: Towards an IS Capability. *The Journal of Strategic Information Systems*, 13(2):167–194.

Pereira, T. and Santos, H. (2014). Security Metrics to Evaluate Organizational IT Security. In Estevez, E., Janssen, M., and Soares Barbosa, L., editors, *Proceedings of the Eighth International Conference on Theory and Practice of Electronic Governance*, pages 500–501, October 27-30, Guimarães, Portugal. Association for Computing Machinery.

Piccoli, G. and Ives, B. (2005). IT-Dependent Strategic Initiatives and Sustained Competitive Advantage: A Review and Synthesis of the Literature. *MIS Quarterly*, 29(4):747–776.

Ponemon Institute (2016). 2016 Cost of Insider Threats. https://tinyurl.com/ybx7fjfg. Retrieved: July 13, 2018.

Posey, C., Roberts, T., Lowry, P. B., Bennett, B., and Courtney, J. (2013). Insiders Protection of Organizational Information Assets: Development of a Systematics-Based Taxonomy and Theory of Diversity for Protection-Motivated Behaviors. *MIS Quarterly*, 37(4):1189–1210.

Posey, C., Roberts, T. L., Lowry, P. B., and Hightower, R. T. (2014). Bridging the Divide: A Qualitative Comparison of Information Security Thought Patterns between Information Security Professionals and Ordinary Organizational Insiders. *Information & Management*, 51(5):551–567.

Queenan, C. C., Angst, C. M., and Devaraj, S. (2011). Doctors' Orders - If They're Electronic, Do They Improve Patient Satisfaction? A Complements / Substitutes Perspective. *Journal of Operations Management*, 29(7):639–649.

Rathnam, R., Johnsen, J., and Wen, H. J. (2005). Alignment of Business Strategy and IT Strategy: A Case Study of a Fortune 50 Financial Services Company. *Journal of Computer Information Systems*, 45(2):1–8.

Rhee, H.-S., Ryu, Y. U., and Kim, C.-T. (2012). Unrealistic Optimism on Information Security Management. *Computers & Security*, 31(2):221–232.

Richards, K. and Davis, B. (2010). Computer Security Incidents against Australian Businesses: Predictors of Victimisation. *Trends and Issues in Crime and Criminal Justice*, (399):1–6.

Ross, J. W. and Beath, C. M. (2002). Beyond the Business Case: New Approaches to IT Investment. *MIT Sloan Management Review*, 43(2):51–59.

Roumani, Y., Nwankpa, J. K., and Roumani, Y. F. (2016). Examining the Relationship between Firm's Financial Records and Security Vulnerabilities. *International Journal of Information Management*, 36(6):987–994.

Rowe, B. R. and Gallaher, M. P. (2006). Private Sector Cyber Security Investment Strategies: An Empirical Analysis. In Anderson, R., editor, *Proceedings of the Fifth Workshop on the Economics of Information Security*, pages 1–23, June 26-28, Cambridge, England, United Kingdom. Robinson College.

Ruighaver, A. B., Maynard, S. B., and Chang, S. (2007). Organisational Security Culture: Extending the End-User Perspective. *Computers & Security*, 26(1):56–62.

Ruohonen, J., Hyrynsalmi, S., and Leppänen, V. (2015). The Sigmoidal Growth of Operating System Security Vulnerabilities: An Empirical Revisit. *Computers & Security*, 55:1–20.

Ryan, J. J. C. H. and Ryan, D. J. (2008). Performance Metrics for Information Security Risk Management. *IEEE Security & Privacy*, 6(5):38–44.

Sabherwal, R. and Jeyaraj, A. (2015). Information Technology Impacts on Firm Performance: An Extension of Kohli and Devaraj (2003). *MIS Quarterly*, 39(4):809–836.

Safa, N. S., Von Solms, R., and Furnell, S. (2016). Information Security Policy Compliance Model in Organizations. *Computers & Security*, 56:70–82.

Sambamurthy, V. and Zmud, R. W. (1994). *IT Management Competency Assessment: A Tool for Creating Business Value through IT*. Financial Executives Research Foundation, Morristown, New Jersey, USA.

SANS Institute (2017). Defending Against the Wrong Enemy: 2017 SANS Insider Threat Survey. https://www.sans.org/reading-room/whitepapers/awareness/defending-wrong-enemy-2017-insider-threat-survey-37890. Retrieved: July 13, 2018.

Saunders, C. S. and Jones, J. W. (1992). Measuring Performance of the Information Systems Function. *Journal of Management Information Systems*, 8(4):63–82.

Savola, R. M. (2007). Towards a Taxonomy for Information Security Metrics. In Stølen, K., editor, *Proceedings of the 2007 ACM Workshop on Quality of Protection*, pages 28–30, October 29, Alexandria, Virginia, USA. Association for Computing Machinery.

Sawik, T. (2013). Selection of Optimal Countermeasure Portfolio in IT Security Planning. *Decision Support Systems*, 55(1):156–164.

Saydjari, O. S. (2004). Cyber Defense: Art to Science. *Communications of the ACM*, 47(3):52–57.

Scheepers, H. and Scheepers, R. (2008). A Process-Focused Decision Framework for Analyzing the Business Value Potential of IT Investments. *Information Systems Frontiers*, 10(3):321–330.

Schryen, G. (2013). Revisiting IS Business Value Research: What we already know, What we still need to know, and How we can get there. *European Journal of Information Systems*, 22(2):139–169.

Schultz, E. E., Proctor, R. W., Lien, M.-C., and Salvendy, G. (2001). Usability and Security an Appraisal of Usability Issues in Information Security Methods. *Computers & Security*, 20(7):620–634.

Senk, C. (2013). Adoption of Security as a Service. *Journal of Internet Services and Applications*, 4(11):1–16.

Shameli-Sendi, A., Aghababaei-Barzegar, R., and Cheriet, M. (2016). Taxonomy of Information Security Risk Assessment (ISRA). *Computers & Security*, 57:14–30.

Shih, S. C. and Wen, H. J. (2003). Building E-Enterprise Security: A Business View. *Information Systems Security*, 12(4):41–49.

Shin, Y., Meneely, A., Williams, L., and Osborne, J. (2011). Evaluating Complexity, Code Churn, and Developer Activity Metrics as Indicators of Software Vulnerabilities. *IEEE Transactions on Software Engineering*, 37(6):772–787.

Siponen, M. and Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly*, 34(3):487–502.

Skopik, F., Settanni, G., and Fiedler, R. (2016). A Problem Shared is a Problem Halved: A Survey on the Dimensions of Collective Cyber Defense through Security Information Sharing. *Computers & Security*, 60:154–176.

Smith, D. and Crossland, M. (2008). Realizing the Value of Business Intelligence. In Avison, D., Kasper, G. M., Pernici, B., Ramos, I., and Roode, D., editors, *Advances in Information Systems Research, Education and Practice*, pages 163–174, Milano, Italy. Springer.

Soh, C. and Markus, M. L. (1995). How IT Creates Business Value: A Process Theory Synthesis. In Ariav, G., Beath, C., DeGross, J. I., Hoyer, R., and Kemerer, C. F., editors, *Proceedings of the Sixteenth International Conference on Information Systems*, pages 29–41, December 10-13, Amsterdam, The Netherlands. Association for Information Systems.

SolarWinds (2016). Calculating the Real Dollar Cost of Risk for Small Business Owners. https://www.solarwindsmsp.com/blog/calculating-real-dollar-cost-risk-small-business-owners. Retrieved: July 13, 2018.

Soomro, Z. A., Shah, M. H., and Ahmed, J. (2016). Information Security Management Needs More Holistic Approach: A Literature Review. *International Journal of Information Management*, 36(2):215–225.

Spillan, J. and Hough, M. (2003). Crisis Planning in Small Businesses: Importance, Impetus and Indifference. *European Management Journal*, 21(3):398–407.

Srivastava, S. C. and Teo, T. S. (2007). E-Government Payoffs: Evidence from Cross-Country Data. *Journal of Global Information Management*, 15(4):20–40.

Stanton, J. M., Stam, K. R., Mastrangelo, P. M., and Jolton, J. A. (2009). Behavioral Information Security: An Overview, Results, and Research Agenda. In Zhang, P. and Galletta, D. F., editors, *Human-Computer Interaction and Management Information Systems: Foundations*, pages 262–280, Armonk, NY.

Teece, D. J., Pisano, G., and Shuen, A. (1997). Dynamic Capabilities and Strategic Management. *Strategic Management Journal*, 18(7):509–533.

Thiesse, F., Al-Kassab, J., and Fleisch, E. (2009). Understanding the Value of Integrated RFID Systems: A Case Study from Apparel Retail. *European Journal of Information Systems*, 18(6):592–614.

Thomson, K.-L. and von Solms, R. (2006). Towards an Information Security Competence Maturity Model. *Computer Fraud & Security*, 2006(5):11–15.

Tripwire (2017). Insider Threats as the Main Security Threat in 2017. https://www.tripwire.com/state-of-security/security-data-protection/insider-threats-main-security-threat-2017. Retrieved: July 13, 2018.

Tsiakis, T. and Stephanides, G. (2005). The Economic Approach of Information Security. *Computers & Security*, 24(2):105–108.

Tu, C. Z., Yuan, Y., Archer, N., and Connelly, C. E. (2018). Strategic Value Alignment for Information Security Management: A Critical Success Factor Analysis. *Information & Computer Security*, 26(2):150–170.

Tvrdíková, M. (2016). Increasing the Business Potential of Companies by Ensuring Continuity of the Development of their Information Systems by Current Information Technologies. *Journal of Business Economics and Management*, 17(3):475–489.

Vance, A., Lowry, P. B., and Eggett, D. L. (2015). A New Approach to the Problem of Access Policy Violations: Increasing Perceptions of Accountability through the User Interface. *MIS Quarterly*, 39(2):345–366.

Väyrynen, K., Hekkala, R., and Liias, T. (2013). Knowledge Protection Challenges of Social Media Encountered by Organizations. *Journal of Organizational Computing and Electronic Commerce*, 23(1-2):34–55.

Veiga, A. D. and Eloff, J. H. (2007). An Information Security Governance Framework. *Information Systems Management*, 24(4):361–372.

Venter, H. and Eloff, J. H. (2003). A Taxonomy for Information Security Technologies. *Computers & Security*, 22(4):299–307.

Vermerris, A., Mocker, M., and Van Heck, E. (2014). No Time to Waste: The Role of Timing and Complementarity of Alignment Practices in Creating Business Value in IT Projects. *European Journal of Information Systems*, 23(6):629–654.

Viduto, V., Maple, C., Huang, W., and López-Peréz, D. (2012). A Novel Risk Assessment and Optimisation Model for a Multi-Objective Network Security Countermeasure Selection Problem. *Decision Support Systems*, 53(3):599–610.

von Solms, B. (2001). Information Security - A Multidimensional Discipline. *Computers & Security*, 20(6):504–508.

von Solms, B. and von Solms, R. (2005). From Information Security to ... Business Security? *Computers & Security*, 24(4):271–273.

von Solms, R. and van Niekerk, J. (2013). From Information Security to Cyber Security. *Computers & Security*, 38:97–102.

Wade, M. and Hulland, J. (2004). Review: The Resource-Based View and Information Systems Research: Review, Extension, and Suggestions for Future Research. *MIS Quarterly*, 28(1):107–142.

Walden, J., Stuckman, J., and Scandariato, R. (2014). Predicting Vulnerable Components: Software Metrics vs Text Mining. In Cotroneo, D., editor, *Proceedings of the Twenty-Fifth IEEE International Symposium on Software Reliability Engineering*, pages 23–33, November 3-6, Naples, Italy. IEEE Computer Society.

Wang, A. J. A. (2005). Information Security Models and Metrics. In Guimaraes, M., editor, *Proceedings of the Forty-Third Annual Southeast Regional Conference - Volume 2*, pages 178–184, March 18-20, Kennesaw, Georgia, USA. Association for Computing Machinery.

Wang, R. Y. and Strong, D. M. (1996). Beyond Accuracy: What Data Quality means to Data Consumers. *Journal of Management Information Systems*, 12(4):5–33.

Weill, P. (1992). The Relationship between Investment in Information Technology and Firm Performance: A Study of the Valve Manufacturing Sector. *Information Systems Research*, 3(4):307–333.

Weill, P. and Olson, M. H. (1989). Managing Investment in Information Technology: Mini Case Examples and Implications. *MIS Quarterly*, 13(1):3–17.

Wernerfelt, B. (1984). A Resource-Based View of the Firm. *Strategic Management Journal*, 5(2):171–180.

Willemson, J. (2006). On the Gordon & Loeb Model for Information Security Investment. In Anderson, R., editor, *Proceedings of the Fifth Workshop on the Economics of Information Security*, pages 1–23, June 26-28, Cambridge, England, United Kingdom. Robinson College.

Wu, Y., Feng, G., and Fung, R. Y. (2018). Comparison of Information Security Decisions under Different Security and Business Environments. *Journal of the Operational Research Society*, 69(5):747–761.

Xu, F., Luo, X. R., Zhang, H., Liu, S., and Huang, W. W. (2017). Do Strategy and Timing in IT Security Investments Matter? An Empirical Investigation of the Alignment Effect. *Information Systems Frontiers*, pages 1–15. In Press.

Yahoo! (2016). Yahoo Security Notice December 14, 2016. https://help.yahoo.com/kb/SLN27925.html. Retrieved: July 13, 2018.

Yamin, S., Gunasekaran, A., and Mavondo, F. T. (1999). Relationship between Generic Strategies, Competitive Advantage and Organizational Performance: An Empirical Analysis. *Tech-*

novation, 19(8):507–518.

Young, D., Beebe, N., and Chang, F. (2012). Prospect Theory and Information Security Investment Decisions. In Joshi, K. and Yoo, Y., editors, *Proceedings of the Eighteenth Americas Conference on Information Systems*, pages 1–9, August 9-11, Seattle, Washington, USA. Association for Information Systems.

Zafar, H. and Clark, J. G. (2009). Current State of Information Security Research in IS. *Communications of the Association for Information Systems*, 24(34):557–596.

Zhu, K., Dong, S., Xu, S. X., and Kraemer, K. L. (2006). Innovation Diffusion in Global Contexts: Determinants of Post-Adoption Digital Transformation of European Companies. *European Journal of Information Systems*, 15(6):601–616.