Accepted Manuscript

Title: Information security investments: an exploratory multiple case study on decision-making, evaluation and learning

Author: Eva Weishäupl, Emrah Yasasin, Guido Schryen

PII: S0167-4048(18)30055-5
DOI: https://doi.org/10.1016/j.cose.2018.02.001
Reference: COSE 1286

To appear in: *Computers & Security*

Received date: 21-8-2017
Revised date: 9-1-2018
Accepted date: 1-2-2018

Please cite this article as: Eva Weishäupl, Emrah Yasasin, Guido Schryen, Information security investments: an exploratory multiple case study on decision-making, evaluation and learning, *Computers & Security* (2018), https://doi.org/10.1016/j.cose.2018.02.001.

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

Eva Weishäupl
University of Regensburg
Universitätsstraße 31
93053 Regensburg
eva.weishaeupl@wiwi.uni-regensburg.de

Emrah Yasasin
University of Regensburg
Universitätsstraße 31
93053 Regensburg
emrah.yasasin@wiwi.uni-regensburg.de

Guido Schryen[a]
University of Regensburg
Universitätsstraße 31
93053 Regensburg
guido.schryen@wiwi.uni-regensburg.de

About the Authors

Eva Weishäupl is a doctoral student and research assistant at the Professorship of Management Information Systems (Prof. Dr. Guido Schryen) at the University of Regensburg, Germany. She focused on the economics of information security, information security management, and information systems security. Ms. Weishäupl participates in the Bavarian research cooperation FORSEC (Security of highly-connected IT systems) where she researches about the economic impact of information security.

Emrah Yasasin is a doctoral student and research assistant at the Professorship of Management Information Systems (Prof. Dr. Guido Schryen) at the University of Regensburg, Germany. He has published literature reviews on information security investments. Mr. Yasasin's main interests are focused on the economics of information security, information security management, and information systems security. He specializes in qualitative and exploratory research methods. His research has been published in conferences such as the International Conference on Information Systems or European Conference on Information Systems and in the international journal Communications of the AIS.

[a] **Corresponding author:** Prof. Dr. Guido Schryen, University of Regensburg, Universitätsstraße 31, 93053 Regensburg. E-mail: guido.schryen@wiwi.uni-regensburg.de

Guido Schryen is a Professor of Management Information Systems at the University of Regensburg, Germany. His research interests cover fields of quantitative decision support (operations research), benefits of information systems and services, and IT security. He has published both quantitative and qualitative research in international journals, including Computers & Security, European Journal of Information Systems, European Journal of Operational Research, OR Spectrum, Communications of the AIS, Communications of the ACM, and others. Prof. Schryen is member of the advisory board of the „Bavarian IT Security and Safety Cluster“ (member of The Kompetenznetze Deutschland initiative of the Federal Ministry of Economics and Technology) and member of the advisory board of the „Forum IT-Security“ of the „Bavarian IT Security and Safety Cluster“.

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.

Keywords: *Information Security Investments, Multiple Case Study, Organizations, Single Loop Learning, Double Loop Learning*

1

1. Introduction

More and more organizations are highly reliant on Information Technology (IT) for their business operations to the extent that failure of IT systems could even lead to bankruptcy (Kearns & Lederer 2004). Additionally, security threats have become more advanced and frequent in the past years (Ponemon Institute 2015b): According to a global survey of Grant Thornton, one in six businesses has been targeted by a cyber-attack in the past year (Grant Thornton 2015). This led to a blow up of the costs caused by security incidents which is shown, for instance, by the "2015 Cost of Data Breach Study" of the Ponemon Institute: According to a global study of 350 companies, the average total cost of all data breaches increased from $3.5 to $3.8 million (Ponemon Institute 2015a). In 2015, cybercrime is estimated to have caused $315 billion in damages worldwide (Grant Thornton 2015). To avoid these damages, organizations need to protect systems, data and processes by reducing vulnerabilities and by improving their monitoring capabilities (Gartner 2011). Specifically, they invest into various security technologies that protect systems, data and processes against technical failure, damage or attacks such as data loss prevention, spyware detection, removal applications and cryptographic techniques (Gartner 2016; Gartner 2011). Information security investments surpassed $75.4 billion worldwide in 2015 according to a report of Gartner (2015) and is expected to grow further in 2016 (eWeek 2016). As predicted by the SANS Institute's report "IT Security Spending Trends" both IT and security budgets for financial services (including banking and insurance), technology providers, government, education and health care are on the rise (SANS Institute 2016). These figures indicate large and rising investments of firms in IT security so that organizations are impelled to pay thorough consideration to planning and evaluation of their IT security spending.

In the presence of budget constraints and a large 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 the economic value of future security investment actions (Anderson & Schneier 2005; Demetz & Bachlechner 2013; Gordon & Loeb 2006b). We identified only a few studies that provide empirical insights in how organizations make decisions on IT security investments: For example, Dor & Elovici (2016) investigate up-to-date decision making practices regarding information security investment in organizations and Toivanen (2015) examine the affecting drivers why information security investment decisions fail. Our case study goes beyond the overall body of empirical knowledge on IT security investments, which we unfold in more detail in the succeeding section, by exploring in a multiple case study how organizations (1) make information security investment decisions depending on environmental factors, (2) evaluate their investment decisions, and (3) organizationally learn from past activities when they have to decide on further security investments.

The key contributions of our case study are as follows: We provide empirical insights that (1) firms' investments in information security are largely driven by external environmental and industry-related factors, such as legal regulations, industry-specific demands and requirements of partner firms, (2) standardized decision processes as provided by academic literature are not applied in practice, (3) security processes are perceived as having a troublesome and time-consuming effect on business processes, (4) both the implementation of evaluation processes and the application of metrics are hardly existent and (5) learning activities mainly occur on an ad-hoc basis.

The paper is structured as follows: In Section 2, we provide the theoretical background of our work. Afterwards, in Section 3, we present the research approach used for our case study. Within Section 3, we derive the interview question in a theory-based way (Subsection 3.1). In Subsection 3.2, we present the research sites and in Subsection 3.3, we describe the data collection and how we analyzed our collected data. Then, in Section 4, we synthesize the results of the case study. In particular, we specify how external factors influence decision to invest in information security resources (Subsection 4.1). In Subsection 4.2, we illustrate how investments in information security resources based on underlying decision processes are conducted in practice. While we show the influence of security processes on business processes with measuring performances in Subsection 4.3, we introduce metrics and evaluation processes used to measure the changes in organizational performance in Subsection 4.4. The usage of single and double loop learning strategies for information security investments is outlined in Subsection 4.5. These insights are discussed in Section 5 and key propositions are derived: This section is structured analogously to Section 4. Finally, we conclude in Section 6.

2. Research on Information Security Investment

The importance of information security investment has given rise to a growing stream of research. Financial analyses help to identify the assets, threats, vulnerabilities of information systems and provide an approach for the necessary investment (Bojanc & Jerman-Blažic 2012; Bojanc et al. 2012) and to evaluate the value of portfolios of various kinds of security countermeasures in the light of different threat and business environments (Kumar et al. 2008). Moreover, the effects that IT security investments have on reducing the incidence of data security breaches over time were analyzed (Angst et al. 2017). Methods and models for evaluation have

been suggested, for instance, by Bistarelli et al. (2012), Bodin et al. (2005), Cavusoglu et al. (2004), Chou et al. (2006), Cremonini & Martini (2005), Jing (2009), Locher (2005), Sheen (2010) and Wang et al. (2011). Several metrics have been introduced to measure improvements in the overall organizational performance rooted in information security investments, for example, metrics that quantify the Return On Security Investment (ROSI), e.g., Anderson et al. (2008), Gordon & Loeb (2002a), the Internal Rate of Return (IRR), e.g., Buck et al. (2008) and Wawrzyniak (2006), Net Present Value (NPV), e.g., Eisenga et al. (2012) and Sheen (2010), Annual Loss Expectancy (ALE), e.g., Cremonini & Martini (2005) and Tanaka et al. (2005) or Cumulated Abnormal Return (CAR), e.g., Andoh-Baidoo & Osei-Bryson (2007) and Campbell et al. (2003).

There are a few case study approaches which have been used to understand investment and implementation strategies, particularly focusing on the aspects which drive the level of security (Rowe & Gallaher 2006), to develop a risk management framework for evaluating information security spending by firms (Herath & Herath 2008) and to explore whether larger firms are making better security investments (Dynes et al. 2005). Moreover, case studies have been utilized to support security investment decision-making (Beresnevichiene et al. 2010) and to investigate the question in which security solutions it is worth investing (Fenz et al. 2011). In addition, a series of empirical analyses of information security investment has been presented to verify the relationship between the vulnerability and effects of information security investment (Liu et al. 2008). The ways in which corporations make decisions regarding information security investments has been examined with empirical studies: It was analyzed whether firms address the budgeting process in a rational economic manner (e.g., with cost-benefit analysis) (Gordon & Loeb 2006a). Moreover, Toivanen (2015) examines the information security investment decision

making process to understand why information security investment decisions fail. The goal of that study is to determine the influential drivers, which affect the information security investment decision-making. In another study, Dor & Elovici (2016) investigate the information security investment decision-making process focusing on different phases and concepts showing that the decision-making process is heavily depending on different organizational and psychological factors.

In this study, we intend to extend current research that has focused on decision-making with evaluation and learning strategies. The strength of our case study lies in our theory-based perspective on information security investments: We use a "Resource-based Learning Model for Information Security Investments" based on Argyris et al. (1985), Melville et al. (2004) and Weishäupl et al. (2015), which frames firm-characteristic components such as business processes and security resources and, additionally, accounts for the repeated reevaluation of information security investments by dynamically incorporating the feedback of different learning strategies.

3. Research Methodology

We conducted an exploratory multiple case study (Yin 2003) to gain insights into information security investment management, which is a "*deeper and more political problem than is usually realized*" (Anderson 2001, p.364). Case studies have been recognized as an established approach to examine such complex phenomena (Majchrzak et al. 2000; Yin 2003), that cannot be controlled by the researchers and which need to be investigated in their original settings (Dubé & Paré 2003; Liu et al. 2011; Paré 2004; Yin 2003). Several authors indicate that empirical approaches are well suited for the information security investment problem: For instance, Lederer et al. (1990) who used a case study for the management of cost estimation argues that the management of cost estimation is among those "*sticky, practice-based problems where the experi-*

ences of the actors are important and the context of action critical" (Bonoma & Wong 1985, p.15; Lederer et al. 1990).

The design of our exploratory case study is guided by the goal of understanding how information security investment decisions are made and evaluated in organizations. Analyzing several organizations allows us to perform an "'*analytic generalization', in which a […] theory is used as a template with which to compare the empirical results of the case study*" (Yin 2003, p.32). Our case study is interview-based, i.e. the results of our interviews are our data source and before the actual field visits, we developed a case study protocol as suggested by Yin (2003)**,** which contains the interview protocol and the open-ended interview questions.

3.1 Theory-based Derivation of Interview Questions

According to Procter et al. (1999, p.245), the use of theory in case studies is an "*immense aid in defining the appropriate research design and data collection*". The interview questions arise from the model shown in Figure 1, namely the Resource-based Learning Model for Information Security Investments based on Argyris et al. (1985), Melville et al. (2004) and Weishäupl et al. (2015). We apply this theoretical model, which is developed by Weishäupl et al. (2015) and used by the authors for structuring their literature review on information security investments, as the basis for deriving our interview questions. The model accounts for the repeated reevaluation of information security investments by dynamically incorporating the feedback of single and double loop learning to adjust corresponding action strategies. In addition, the theoretical model frames firm-characteristic components such as business processes and security resources. The model comprises three main constructs, namely *governing variables*, *action strategies* and *consequences* and two learning strategies, *single loop learning* and *double loop learning*. Governing variables are defined as objectives a firms aims to gain (e.g., in the security context it would be a se-

curity policy) including conformance to country- and industry-specific regulations and norms as well as demands from trading partners. Action strategies are steps to achieve the objectives (e.g., investment in resources such as an antivirus program) and are influenced by the security environment variables. Consequences include all results on processes and resources from the actions undertaken. The two learning strategies assure that there is a continuous process and alignment of an organization's governing variables and its action strategies.

Based on the Resource-based learning model l, we derive five research themes (RTs) shown in Table 1 and operationalize them to 35 interview questions (cf. Appendix), which were open in order to stimulate a discussion.

In general, the developed research themes cover how firms make their decisions when investing in IT security resources regarding external factors and underlying decision processes, and how security processes and business processes are influenced thereby with respect to their performances. It also includes what kind of metrics and evaluation processes firms apply and how firms learn from the results of those for future investments. The impact of the governing variables in the resource-based learning model, including country characteristics, industry characteristics and trading partner resources & business processes on action strategies, is theorized in the first research theme: In the context of information security, an organization's goal is guaranteeing a suitable security level, which is influenced by compliance with country characteristics, industry characteristics and trading partner resources & business processes that force organizations to implement new information security measures. For instance, an organization's goal to align

with country-specific governmental regulations[1] results in investments to pass IT security audits and obligatory requests of the general data protection regulation (GDPR) force organizations to value data protection.

The second research theme covers action strategies which include managerial decisions to invest in various information security resources. In particular, it includes in which information security resources organizations invest in based on which underlying decision process. Regarding decision processes, IT security investment action strategies pertain to different resources, conceptualized in the theoretical model as technological and human security resources. The decisions to invest in various IT security resources impact the security processes within the firm, which in turn have a direct influence on the business processes – yet the kind of impact and the measurement remains nebulous.

The third research theme deals with the implemented security processes and how business processes are influenced thereby. According to the model, the IT business value generation process, including the processes, their performance, and the non-security resources, theorizes the influence on the overall organizational performance. The changes in the organizational performance achieved through information security investments, can be measured with metrics and assessed with evaluation processes.

Research theme 4 copes thus with measurement of the efficiency and effectiveness of past information security investment decisions and the fifth research theme deals with learning strategies – in particular how the results of evaluation processes of past investment decisions influence

[1] For instance, acts such as the *Gramm-Leach-Bliley Act* (GLBA) for financial firms, the *Sarbanes-Oxley* (SOX) act for accounting firms and the *health insurance portability and accountability act* (HIPAA) for healthcare providers (Khansa and Liginlal 2009).

the investment decisions in the future and which learning strategy is used under specific circumstances. We address the organization's learning strategy: Single loop and double loop learning with single loop being the more routine and double loop the more radical way of learning (Easterby-Smith et al. 2000). Since single and double loop learning are intertwined strategies, an isolated consideration of single loop and double loop learning is not advisable.

Based on the developed research themes, we specified 35 interview questions which do not differ semantically and syntactically for consulting firms and non-consulting firms (cf. Appendix).

3.2 Research Sites

We conducted interviews with 12 organizations: Seven consulting firms which consult their clients with regard to information security investments and five non-consulting firms. By interviewing non-consulting firms, we gain insights into their information security investments, in particular their decision making, evaluation and learning strategies from past investment decisions. As firms tend to be reluctant to disclose security-related inadequacies for fear of attacks and harm of reputation (Turoff & Plotnick 2012) and might not have deep expertise and complete comprehension in information security, we additionally chose consulting firms as interview partners which consult their clients about information security investments. With the combination of the consulting and non-consulting firms' answers, we benefit (1) from the consultants' know-how, experience and concentrated knowledge on the security management of many organizations, and (2) from the first-hand, comprehensive and detailed information from the non-consulting firms. Moreover, members of non-consulting firms have situated and longitudinal knowledge and insights. With not only interviewing non-consulting firms but also consulting firms, we can overcome the deficiency that firms might not want to disclose security-related inadequacies and mistakes to us for fear of attacks and harm of reputation (Turoff & Plotnick

2012). The combination of different interview partners offers knowledge about the research subject (Flick 2014; Flick 2008) and our case study aligns with similar studies which have also used the combination of different interview partners, e.g., A. W. Baur et al. (2015) and Krücken (2003).

3.3 Data Collection and Analysis

The data collection involved interviews conducted in February 2016 with seven consulting firms and five non-consulting firms which are located in Europe. Table 2 and 3 show the anonymized profiles of the firms; anonymization was necessary due to non-disclosure agreements. The types of interviewees as listed in row 2 (Interviewee(s)) in Table 2 and 3 show that they are "*elite*" (Yin 2011, p.56) as they are "*persons of high stature which fill a unique role and can provide distinctive insights*" (Yin 2011, p.56). For confidentiality reasons the consulting and non-consulting firms are referred to as CF 1 to CF 7 and NCF 1 to NCF 5 in this article. The participating companies represent a wide variety of firm sizes so that our multiple case study addresses issues of information security investments over different sectors of industry. Overall, our case study comprises insights of managers from different hierarchical levels, working for firms of several vertical levels of the industry, i.e., OEMs, suppliers and service providers, to form "*a holistic picture and mitigate the possibility of missing important insights*" (A. Baur et al. 2015, p.6).

All 12 interviews were conducted by two of the authors and had an average duration of 90 minutes. We conducted the in-person interviews at the interviewees' workplaces, a natural environment for discussing (Feldman & Horan 2011). Each interview was taped providing "*a more accurate rendition of any interview than any other method*" (Yin 2003, p.92), transcribed by a

third party, then reviewed by the authors for accuracy (Jones & Price 2001) and translated into English by the authors.

After the data collection phase, the analysis of the data was conducted in three steps as done by Silva & Hirschheim (2007): (1) We organized the transcripts of the interviews using NVivo, a software for the analysis of qualitative data; (2) in NVivo, we coded the files along the five research themes as introduced in the previous subsection; (3) we synthesized the interview results by structuring their presentation along the five research themes.

4. Empirical Findings

In this section, we present the results of our case study by describing the answers of the interviewees. The presentation is structured along the five research themes as they are derived in the previous section.

4.1 Influence of External Factors on Decisions to Invest in Information Security Resources

The main external drivers for decisions to invest in information security are country characteristics, including legal frameworks, regulations and acts which put high pressure on organizations. The same applies to obligatory industry-specific regulations and requirements of trading partners. Typical statements made by our interviewees are shown in Table 4, where they are grouped by the types of external factors. Since information security is a complex problem and investments in information security measures have no obvious return, organizations tend to neglect its importance and refuse to take actions except for when they are compelled by laws to invest which were criticized by some interviewees regarding compliance and content: It has been noted that the mandatory minimum level required by law tends to be below the actual protection needs.

Additionally, our study reveals that, in practice, there are laws which, albeit not being directly related to information security, have an impact on investments in information security (e.g., German Criminal Code when handling digital medical records). The influence of external pressure by the law has been confirmed by all interview partners, but the answers differed depending on industry and firm size. For instance, regulations are particularly important for the automotive industry and banks, and they become increasingly complex for organizations which operate internationally as several laws apply. It is notable that for many firms legal frameworks, regulations and acts are the only driver for their information security investment decisions, neglecting other country characteristics, such as a country's culture. Interestingly, most firms do not regard reputation as important unless there is a damage. However, few firms are driven in their information security investment decision by the location of the organization, their image and fear caused by recent incidents.

4.2 Investment in Information Security Resources based on Underlying Decision Processes

The resources in which a firm decides to invest are either technological or human: We found that organizations invest in "classical" technological and human security resources without any standardized decision processes. Most of the firms invest in "classical" technological resources (e.g., firewalls, antivirus programs) and "classical" human security resources (e.g., CISO, workshops) which is backed up with exemplarily statements of our interview partners in Table 5. All of the interviewees answered the corresponding interview questions by providing examples for technological and human security resources that are commonly invested in. However, the distinction between security and non-security IT resources and their allocation to different budgets is blurry in the daily business operations. The reason for that is that technological IT security re-

sources (e.g., firewall) are managed by the IT department. In contrast to technological security resources, the investment in human security resources depends on the industry and size of the firm: Large organizations and firms in critical industries (e.g., finance and telecommunication) employ a CISO and have dedicated departments for information security. This trend is extending to smaller firms and other industries due to a rising awareness of the importance of information security. Moreover, many firms that invest in external security consultants not only aim at benefiting from external know-how but they also intend to hand over the responsibility for security incidents.

Decisions to determine the optimal amount, time and allocation of security investments are made by the CISO in collaboration with the information security department (if it exists) and the CIO depending on the CISO's hierarchical position within the organization. Different opinions and preferences are discussed without using formal multi-stakeholder decision models, instead pilot tests or attack simulations are carried out as pointed out in statements (cf. Table 5). Overall, investments in technological and human information security resources are mostly made based on risk analyses or gut feeling.

4.3 Security Processes and their Influence on Business Processes and Measurement of Process Performances

With the help of various information security resources, firms often establish security processes to safeguard the confidentiality, integrity and availability of business operations, e.g., monitoring, password change and backup processes. The CISO is in charge of monitoring the security processes but it has been noted that this responsibility should not lie within the CISO as he controls the processes. Surprisingly, as indicated by the statements of our interview partners in Table

6, the impact of the security processes on the business processes was judged to be negative despite its effect of increased security and expected decrease of breaches as they slow down the business processes. This even goes so far that CISOs are hesitant to introduce new security processes because it could cause interruptions of business processes. Although security processes are regularly evaluated by external audits, the performance of security processes is rarely measured in practice because of its complexity. The effect of the security process performance on the business process performance is stated to be negative and not measured in numbers either. Overall, investments target various security processes in organizations despite its perceived negative impact on crucial business processes.

4.4 Metrics and Evaluation Processes Used to Measure the Changes in Organizational Performance

Similar to decision processes, evaluation processes are barely used in practice to evaluate the effectiveness and efficiency of information security investments. The lack of evaluation processes was stated by our interview partners as shown exemplarily in Table 7. This lack is rooted in the complexity and time expenditure of evaluating information security investment decisions. Industry specific differences could be observed, for instance, banks are required to audit their information security frequently. In general, firms are forced to evaluate their processes and systems when external pressure exists (audits), business processes do not run smoothly, or the IT budget is reallocated.

Considering the use of metrics for information security investments, such as ROSI, we noted that these are not used in practice as pointed out by the interviewees (cf. Table 7). An explanation, which was underpinned by the interview findings, is that the metrics include assumptions which

are difficult to assess in practice so that - although the metrics could provide a benefit for decision makers - in their current form their applicability is limited because the metrics do not adequately reflect the given facts embodied in practice. Therefore, evaluation processes, including metrics, are missing even though the academic literature provides various approaches. The connection between information security investments and organizational performance is not considered in practice.

4.5 Usage of Single and Double Loop Learning Strategy for Information Security Investments

From the two existing learning strategies, single loop and double loop learning, firms prefer, according to the interviews, single loop learning as a fast reaction to incidents rather than searching for a long lasting rectification later on. However, (single loop and double loop) learning is always triggered by incidents and not intrinsically motivated. Representative statements from our interviewees are shown in Table 8, where they are grouped by the types of learning strategies. The reason for the incident-triggered behavior might be that, according to interview partners from consulting firms, information security is regarded as an unpleasant task. It was stated that for human security resources learning takes place because firms consider the fluctuation of the employees and the fact that employees quickly forget lessons learned in past workshops. However, once technological security resources are installed, they are not reevaluated with regard to their suitability to changing environmental factors. Thus, for technological security resources, learning strategies are usually not applied.

Our results on how firms evaluate the effectiveness of their information security investments and how they learn from past experience shows large consensus of all interview partners that no sys-

tematic evaluation of information security investments occurs and no evaluation processes are implemented with the exception of those related to external pressure (e.g., external audits). The key reason of missing evaluation (processes) are unofficial "*never change a running system*" policies, many firms adhere to, i.e. improving has a lower priority than maintaining. As a consequence, once information security resources have been purchased and installed, they are not removed unless malfunctions or external pressure occur. The interview partners also agreed that although firms show some elements of learning, they have implement neither single loop learning (correcting errors in a routinely manner) nor double loop learning (fixing errors by aligning preferences and policies) strategies.

Table 9 summarizes the empirical findings structured along the five research themes.

5. Discussion

While we found some consistencies with the academic literature, for example regarding the influence governing variables have on information security investments, interesting mismatches have emerged between the perspectives of researchers and practitioners. Structured by our research themes, we discuss the results of our case study in comparison with the findings in academic literature and review the discrepancies in the statements between consulting and non-consulting firms. Subsequently, we propose a research agenda to provide guidance for future research by assessing what we know and formulating concrete propositions at the end of our discussion.

5.1 Influence of External Factors on Decisions to Invest in Information Security Resources

The three governing variables "Country Characteristics", "Industry Characteristics" and "Trading Partner Resources & Business Processes" are crucial in the information security investment context. Our results reveal that the first two have the strongest influence on the firm's information security investment actions. The findings are consistent with literature on how firms make information security investment decisions: The academic literature highlights the importance of standards, such as the ISO 27000 series and best practices (Chew et al. 2008), which is supported by our interviewees. The literature identified that a remarkably high percentage of companies are willing to implement the ISO27001 standard if they have not done already (Gillies 2011). Incentives for implementation are demonstrating to partner firms and customers that the organization has determined and measured its security threats and deployed a security policy in order to mitigate risks (Saint-Germain 2005) and lowering insurance costs (von Solms & von Solms 2004).

Regarding compliance with country and industry characteristic laws, there was a major difference of views between non-consulting and consulting firms: While the first indicated that firms comply with the legal requirements by all means, the latter one stated that fear of an imminent review for compliance is mandatory to trigger actions. From an interpretative perspective, we argue that there are two possibilities for this conflicting answer: First, there might be a lack of knowledge regarding information security-specific regulations in non-consulting firms, i.e. they might believe incorrectly that they cover all relevant factors until they get advised by information security specialists (e.g., consulting firms). Second, the non-consulting firms might embellish their current practice to us because of concerns regarding loss of reputation and embarrassment.

A surprising statement was given by some interviewees that reputation is not seen as very important which contradicts our assumptions and the academic literature: For example, Nguyen &

Leblanc (2001) found out that corporate reputation are acknowledged as having the potential to impact on customer loyalty toward the firm and therefore influence information security investment decisions. The reason for this mismatch might be that firms perceive that reputational loss is given if and only if an attack has happened and was successful. To prevent these attacks, firms would need investments in security countermeasures. In the hope not to be affected by attacks, firms rather use that money for other, non-security projects.

As the request for certification from the suppliers becomes more common in many sectors and complex due to globalization, the relationship of the certification need and its impact on investment decisions in information security of the suppliers has to be examined academically. In the academic literature, information sharing and outsourcing with trading partners is well researched (Anderson et al. 2008; Cezar et al. 2013; Gal-Or & Ghose 2005; Gao et al. 2015; Lacity et al. 2009). However, our case study indicates that information sharing and outsourcing is of secondary importance compared to the request of certification from trading partners.

5.2 Investment in Information Security Resources based on Underlying Decision Processes

Organizations invest in "classical" technological and human security resources without any standardized decision processes. In contrast to the technological security resources, the investment in human security resources highly depends on the industry and size of the consulted firm: Large organizations and firms in critical industries (e.g., finance and telecommunication) employ a CISO and have an own department for information security. This trend is extending to smaller firm sizes and other industries due to a rising awareness of the importance of information security.

While there is a clear differentiation from human non-security IT resources to human security IT resources, the distinction from technological non-security IT resources to technological security IT resources is blurry in practice. This lack of differentiation is problematic from an economic point of view because it is not possible to distinguish between an IT budget and an IT security budget. However, in literature, models and methods often require an IT security budget (Gordon & Loeb 2002b; Gordon & Loeb 2002a; Mukhopadhyay et al. 2013; Olifer et al. 2017). Literature often provides models which require the IT security budget as a precondition: For example, game-theoretical models use IT security budget constraints and are evaluated with fictitious firm data (Liu et al. 2014). We assume that as long as such models require specifying the IT security budget, they are difficult to apply in firms. This assumption was backed up by our interview partners. Academic literature should provide explicit guidelines for the distinction of IT budget and IT security budget.

The employment of a person who is in charge of information security is quite prevalent, whether he is named Security Director, Security Manager, Information Security Officer or Chief Information Security Officer. The variety of notation was named during our interviews and is backed up in literature (Fitzgerald 2007). The exact title is not as important as the appointed hierarchical position with respect to the CIO. With regard to our theoretical model, learning from past investments (employment of a CISO) should lead to an investment in a promotion of the CISO's hierarchy because of insufficient influence which had resulted in inadequate protection. The position of the CISO compared to the CIO has also been discussed in literature even whether he should "*have a chair at the board table*" (Klimoski 2016, p.15). With a chair at the board table, the CISO would be part of the organizations leadership members and in a better position to ensure that his security concerns have the full comprehension of the management team (Wylder

2003). In practice, there is a reluctance of including the CISO in the executive board. Reasons might be that security is still perceived as disruptive to business operations which are seen as top priority or information security is regarded as technical issue but not core business activities (Neubauer et al. 2006).

Regarding investments in information security awareness, training and workshops of a firm's employees, all interview partners acknowledged the importance which is backed up by the academic literature (Albrechtsen & Hovden 2010; McCrohan et al. 2010; Puhakainen & Siponen 2010; Stewart & Lacey 2012). There are several factors which need to be considered when it comes to information security awareness. Besides cultural diversity, one of the main factors which is not examined in depth is the varying knowledge level of employees: Some employees might be cautious inherently or because of private experiences while others are not. Based on this initial level of knowledge, the content of the security awareness trainings have to be adapted to reach a sufficient security awareness level for the specific firm and the employee's position.

All interview partners stated that no standardized decision processes have been established to determine the optimal amount, time and allocation of investments. This is in line with the findings of prior research that this decision-making process is biased and depends on organizational and psychological factors (Dor & Elovici 2016). Reasons for this might be that the lack of common language between decision-makers and information security experts (Toivanen 2015). There is discrepancy between the statements of the consulting and non-consulting firms: While, the non-consulting firms noted that methods such as risk analysis, business impact analysis, attack simulations, and cost-benefit and cost-effort analysis are conducted, the consulting firms took a more negative view. According to consulting firms, the decision to invest in technological and human information security resources are mostly based on gut feeling or are discussed be-

tween CISO and CIO without using formal multi-stakeholder decision models. A reason for this discrepancy might be that consultants do not have thorough insights in firms' internal decision processes whereas non-consulting firms can clearly report what kind of methods are implemented. An alternative explanation might be that non-consulting firms tend to embellish their current practices to hide their inexperience and lack of knowledge by saying they were doing far more than they actually were. Finally, we observe a large gap between decision models and methodologies suggested in the literature (Cavusoglu et al. 2008; Tsiakis & Stephanides 2005; Wang et al. 2008) and their use in practice. We assume that, due to the high complexity of information security investment decisions, practitioners tend to not apply them. Additionally, as confirmed by literature, "*it has been notoriously hard to justify investments in information security, […] since security investments to not generate any additional revenue*" (Dutta & Roy 2008, pp.367–369).

5.3 Security Processes and their Influence on Business Processes and Measurement of Process Performances

We find an interesting mismatch between the perspectives of researchers and practitioners on what makes firms implement security processes: While researchers claim that security processes are crucial and are intrinsically motivated (Ashenden 2008; Massacci et al. 2005) because they reduce risk and lead to an efficiently designed, implemented and deployed security architecture (Oppliger 2007), practitioners install security processes mainly because they have to. The assignment of the responsibility and control of the security process tend to be noticed as an important factor which should be researched in future. As an example, security processes should be controlled or reviewed externally to ascertain the CISO's proper installation of the security process. The security process is set to impact the business process in a disturbing way: We conclude that security processes are perceived as time-consuming and troublesome by the non-consulting

firms while the consulting firms state that this view is exactly the problem. However, the unimpeded execution of a business process is crucial for a firm's success (Neubauer & Heurix 2008; Wang et al. 2008). That is why a mind change has to take place and it must be emphasized that there is a trade-off. On the one hand, security processes protect the business processes, whereas on the other hand they should not be set too restrictive in order not to slow down productivity. The measurement of the quality of security processes is mainly implemented through external audits in practice which should be backed up with numbers resulting from metrics. Academic literature should provide those metrics to measure the quality of security processes.

5.4 Metrics and Evaluation Processes Used to Measure the Changes in Organizational Performance

Due to the complexity and time expenditure of evaluating information security investment decisions, evaluation processes are not applied in practice which contravenes the academic literature providing several methods, models and processes for evaluation (Barnard & von Solms 2000; Bistarelli et al. 2012; Bodin et al. 2005; Cremonini & Martini 2005; Eloff & Von Solms 2000; Knapp et al. 2009; Vroom & von Solms 2004). Academia provides several metrics (Jansen 2011; Tsiakis & Stephanides 2005) which are not applicable in practice due to lack of information or inaccurate assumptions. Evaluating information security investments is a challenging task because the return on investments in security resources whether tangible (e.g., firewalls) or intangible (e.g., workshops) is difficult to estimate as security incidents may be prevented or it could have been that there were no security incidents to be prevented. All of the interview partners agreed on this point whereas industry specific differences were described, for instance, for banks. However, firms are forced to evaluate when external pressure exists (audits), business processes do not run smoothly, or the IT budget is reallocated.

Evaluation processes, including metrics, are missing in practice even though the academic literature provides hereto a lot of various approaches (vom Brocke et al. 2007; Andoh-Baidoo & Osei-Bryson 2007; Böhme & Nowey 2008; Berinato 2002; Campbell et al. 2003; Cremonini & Martini 2005; Eisenga et al. 2012; Gordon & Loeb 2002b; Gordon & Loeb 2002a; Gordon et al. 2003; Kwon & Johnson 2014; Mizzi 2010; Rowe & Gallaher 2006; Sheen 2010; Sonnenreich et al. 2005; Tanaka et al. 2005).

5.5 Usage of Single and Double Loop Learning Strategy for Information Security Investments

In academia, the concept of single loop and double loop learning gains relevance (Hwang & Wang 2016; Reychav et al. 2016; Vallerand et al. 2017). With the increasing sophistication in attacks (Baskerville et al. 2014), the two types of learning have become essential in firms (Ahmad et al. 2012): Organizations need both single loop and double loop learning to secure their systems (Mattia & Dhillon 2003). In the literature, organizational learning in the information security context is present as described (Ahmad et al. 2015; Schlienger & Teufel 2005). In practice, from the two existing learning strategies firms prefer, according to the interviews, single loop learning as a fast reaction to incidents rather than searching for a long lasting rectification later on. However, (single loop and double loop) learning is always triggered by incidents and not intrinsically motivated.

Our empirical results reveal that no systematic evaluation of information security investments takes place and evaluation processes are only implemented when triggered by external pressure. All interview partners concurred that firms neither implement single loop learning nor double loop learning strategies.

We summarize the insights of our empirical study in Table 10, which aligns and contrasts our findings with those of prior research. Table 10 also contrasts findings regarding consulting firms with those regarding non-consulting firms.

As a research agenda to provide guidance for future research, we assess what we know and formulate the concrete key propositions derived from our discussion (Table 11):

Proposition 1 highlights the importance of external regulatory and industry-specific factors for organizational information security investment actions. The academic literature deals exhaustively with impacts of information security specific laws (Connolly & Lang 2013; Ghose & Rajan 2006; Kwon & Johnson 2014; Park et al. 2017), yet it is silent on laws which are not directly related to information security but do influence actions as one interviewee stated for the health care sector (cf. Table 4). For practice, this implicates the challenging task of including all relevant regulatory and industry-specific factors even if not directly related to information security at a first glance. Under the aspect of internationally operating organizations where data is distributed globally, these complex legal requirements should be in focus both for firms and for academic research.

Proposition 2 notes that standardized decision processes are not applied. The academic literature has proposed various analyses to address information security investment decision-making (Bojanc & Jerman-Blažic 2012; Bojanc & Jerman-Blažic 2008; Bojanc et al. 2012; Huang & Behara 2013; Huang et al. 2014; Qian et al. 2017). While these approaches provide crucial input to determine the optimal amount, time and allocation of investments, the embedding within an organization's decision process is not carried out. A practical implication might be that firms allocate too little financial resources in information security countermeasures which might lead

to higher risks of incidents. From an academic point of view, a potential approach might be the inclusion of standards such as ISO/IEC 27001 when developing information security models. From a practical view, such models could be better adopted within firms because as our interviews revealed, many firms already rely on this standard

Proposition 3 deals with the implications of security processes for business processes. In the academic literature, it was acknowledged that security processes may have a positive impact on the organizational performance if it leads to a reduction of potential risks (Böhme & Nowey 2008). With the rising number of security threats, security processes, which are - according to the literature - supposed to guarantee the proper operation of business processes, i.e., secure business processes, need to be discussed by organizations. The security of business processes has been addressed in the literature by modeling business processes with security elements through business process diagrams, for example, in a health care business process (Rodriguez et al. 2007). Jakoubi et al. (2009) examine scientific research efforts in the field of security- and risk-related business process/workflow management and provide a representative overview of the efforts in this field. They conclude that the research on the establishment of security processes and their effects on business processes is still a very young field. It has been recommended that security processes should be designed in the way that security experts have to effectively communicate security-related concerns to other stakeholders, who have different risk preferences and regard security not as a first priority within the firm (Werlinger et al. 2009).

Proposition 4 points out that metrics regarding information security investment, such as ROSI, are practically not used. In the literature, there are several approaches to measuring the impact of investment in IT security resources on the organizational performance with the help of ROSI (Buck et al. 2008; Mizzi 2010). However, one of the problems with ROSI for instance is that

there is no standardized computation and definition of it (vom Brocke et al. 2007): It is sometimes computed as an absolute value (Berinato 2002), or a quotient (Sonnenreich et al. 2005) but in most cases the computation as an absolute value is preferred (vom Brocke et al. 2007). Another problem is that these metrics require inputs which cannot be assessed or estimated by firms. This implicates that organizations rely on their managers' and experts' gut feelings which lead to rather subjective and unprecise results. In order to transparently plan and assign financial resources to information security countermeasures, academic models, which fulfill the requirements of availability of inputs, to measure the information security level are crucial.

Proposition 5 describes that firms prefer single loop learning as a fast reaction to incidents rather than searching for a long lasting rectification. In the context of information security, either double loop learning or a combination of single loop and double loop learning is advised in the academic literature: Single loop learning is not sufficient and organizations should focus on double loop learning (Rowe 1996; Van Niekerk & Solms 2004) because double loop learning is the more radical way of learning as it questions not only the action strategies but also the compliance with the governing variables. Implications for practice is that security-related problems and the underlying assumptions are not dealt the correct way (Mattia & Dhillon 2003; Van Niekerk & Solms 2004). A solution which can be applied by organizations is to deploy single and double loop learning to guarantee both short-term reaction and long-lasting rectifications. It would further help organizations to solve security problems that are complex: The combination of single and double loop learning strategy results in analyzing alterations in compliance with underlying governing variables and thus creates a mindset that consciously seeks out security problems in order to resolve them (Mattia & Dhillon 2003).

6. Conclusion

In this study, we examined firms' decision-making, evaluation and learning from past investment decisions. We extend current research (Dor & Elovici 2016; Toivanen 2015) by providing a thorough and theory-grounded look at how information security investments are undertaken in practice. Our case study reveals that (1) firms' investments in information security are largely driven by external environmental and industry-related factors, such as legal regulations, industry-specific demands and requirements of partner firms respectively, (2) standardized decision processes as provided by academic literature are not applied in practice, (3) security processes are perceived as having a troublesome and time-consuming effect on business processes, (4) both the implementation of evaluation processes and the application of metrics are hardly existent and (5) learning activities mainly occur on an ad-hoc basis.

However, our study is not without limitations: Although we strived to have a broad variety of different sectors and firm sizes, we cannot claim a generalization. Besides, the adoption of our theoretical view focusses on information security investments and activities of organizations. IS security phenomena at the individual level, for example learning of individuals, are out of our work's scope.

We hope that our case study encourages researchers to conduct new research on (1) how the interplay between the different external factors are considered in information security investment decisions and (2) how the implementation of evaluation processes and learning strategies can be supported in firms so that information security investments become more effective in practice.

Acknowledgments

We would like to thank the anonymous reviewers who have volunteered their time and expertise to improve this paper. The research leading to these results was supported by the 'Bavarian State Ministry of Education, Science and Arts', as part of the FORSEC research association and by the Hanns Seidel Foundation.

References

Ahmad, A., Hadgkiss, J. & Ruighaver, A.B., 2012. Incident Response Teams–Challenges in Supporting the Organisational Security Function. *Computers & Security*, 31(5), pp.643–652.

Ahmad, A., Maynard, S.B. & Shanks, G., 2015. A Case Analysis of Information Systems and Security Incident Responses. *International Journal of Information Management*, 35(6), pp.717–723.

Albrechtsen, E. & Hovden, J., 2010. Improving Information Security Awareness and Behaviour through Dialogue, Participation and Collective Reflection. An Intervention Study. *Computers & Security*, 29(4), pp.432–445.

Anderson, R. et al., 2008. *Security Economics and the Internal Market*, ENISA.

Anderson, R., 2001. Why Information Security is hard - An Economic Perspective. In D. Faigin, ed. *Proceedings of the Seventeenth Annual Computer Security Applications Conference*. New Orleans, LA, USA: IEEE Computer Society, pp. 358–365.

Anderson, R. & Schneier, B., 2005. Guest Editors' Introduction: Economics of Information Security. *IEEE Security & Privacy*, 3(1), pp.12–13.

Andoh-Baidoo, F.K. & Osei-Bryson, K.-M., 2007. Exploring the Characteristics of Internet Security Breaches that Impact the Market Value of Breached Firms. *Expert Systems with Applications*, 32(3), pp.703–725.

Angst, C.M. et al., 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), pp.893–916.

Argyris, C., 1977a. Double Loop Learning in Organizations. *Harvard Business Review*, 55(5), pp.115–125.

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

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

Argyris, C., Putnam, R. & Smith, D.M., 1985. *Action Science: Concepts, Methods, and Skills for Research and Intervention*, San Francisco, California: Jossey-Bass.

Ashenden, D., 2008. Information Security Management: A Human Challenge? *Information Security Technical Report*, 13(4), pp.195–201.

Barnard, L. & von Solms, R., 2000. A Formalized Approach to the Effective Selection and Evaluation of Information Security Controls. *Computers & Security*, 19(2), pp.185–194.

Baskerville, R., Spagnoletti, P. & Kim, J., 2014. Incident-Centered Information Security: Managing a Strategic Balance between Prevention and Response. *Information & Management*, 51(1), pp.138–151.

Baur, A. et al., 2015. A Novel Design Science Approach for Integrating Chinese User-Generated Content in Non-Chinese Market Intelligence. In D. Leidner & J. Ross, eds. *Proceedings of the Thirty Sixth International Conference on Information Systems (ICIS 2015)*. Fort Worth, TX, USA: Association for Information Systems.

Baur, A.W., Bühler, J. & Bick, M., 2015. How Pricing of Business Intelligence and Analytics SaaS Applications can catch up with their Technology. *Journal of Systems and Information Technology*, 17(3), pp.229–246.

Beresnevichiene, Y., Pym, D. & Shiu, S., 2010. Decision Support for Systems Security Investment. In L. P. Gaspary et al., eds. *Proceedings of the 2010 IEEE/IFIP Network Operations and Management Symposium Workshops*. Osaka, Japan: IEEE Computer Society, pp. 118–125.

Berinato, S., 2002. Finally, a Real Return on Security Spending. *CIO*, 15(9), pp.42–50.

Bistarelli, S. et al., 2012. Evaluation of Complex Security Scenarios Using Defense Trees and Economic Indexes. *Journal of Experimental & Theoretical Artificial Intelligence*, 24(2), pp.161–192.

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

Böhme, R. & Nowey, T., 2008. Economic Security Metrics. In I. Eusgeld, F. Freiling, & R. H. Reussner, eds. *Dependability Metrics*. Berlin Heidelberg: Springer, pp. 176–187.

Bojanc, R., Jerman-Blaic, B. & Tekavcic, M., 2012. Managing the Investment in Information Security Technology by Use of a Quantitative Modeling. *Information Processing and Management*, 48(6), pp.1031–1052.

Bojanc, R. & Jerman-Blažic, B., 2008. An Economic Modelling Approach to Information Security Risk Management. *International Journal of Information Management*, 28(5), pp.413–422.

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

Bonoma, T.V. & Wong, K.B., 1985. *A Case Study in Case Research: Marketing Implementation*, HBS Case Service, Harvard Business School.

Buck, K., Das, P. & Hanf, D., 2008. Applying ROI Analysis to Support SOA Information Security Investment Decisions. In H. Cooper, ed. *Proceedings of the 2008 IEEE Conference on Technologies for Homeland Security*. Waltham, MA, USA: IEEE Computer Society, pp. 359–366.

Calder, A., 2009. *Information Security based on ISO 27001/ISO 27002: A Management Guide*, Van Haren.

Campbell, K. et al., 2003. The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market. *Journal of Computer Security*, 11(3), pp.431–448.

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

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

Cezar, A., Cavusoglu, H. & Raghunathan, S., 2013. Outsourcing Information Security: Contracting Issues and Security Implications. *Management Science*, 60(3), pp.638–657.

Chew, E. et al., 2008. *Performance Measurement Guide for Information Security*, National Institute of Standards and Technology.

Chou, T.-Y., Seng-cho, T.C. & Tzeng, G.-H., 2006. Evaluating IT/IS Investments: A Fuzzy Multi-Criteria Decision Model Approach. *European Journal of Operational Research*, 173(3), pp.1026–1046.

Connolly, L. & Lang, M., 2013. Information Systems Security: The Role of Cultural Aspects in Organizational Settings. In K. Hedström & G. Dhillon, eds. *Proceedings of the Third Workshop on Information Security and Privacy*. Milan, Italy: Association for Information Systems.

Cremonini, M. & Martini, P., 2005. Evaluating Information Security Investments from Attackers Perspective: the Return-On-Attack (ROA). In *Proceedings of the Fourth Annual Workshop on the Economics of Information Security*. Cambridge, MA, USA: Harvard University.

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

Dor, D. & Elovici, Y., 2016. A Model of the Information Security Investment Decision-Making Process. *Computers & Security*, 63, pp.1–13.

Dubé, L. & Paré, G., 2003. Rigor In Information Systems Positivist Case Research: Current Practices, Trends, and Recommendations. *MIS Quarterly*, 27(4), pp.597–636.

Dutta, A. & Roy, R., 2008. Dynamics of Organizational Information Security. *System Dynamics Review*, 24(3), pp.349–375.

Dynes, S., Brechbuhl, H. & Johnson, M.E., 2005. Information Security in the Extended Enterprise: Some Initial Results From a Field Study of an Industrial Firm. In *Proceedings of the Fourth Annual Workshop on the Economics of Information Security*. Cambridge, MA, USA: Harvard University.

Easterby-Smith, M., Crossan, M. & Nicolini, D., 2000. Organizational Learning: Debates Past, Present And Future. *Journal of Management Studies*, 37(6), pp.783–796.

Eisenga, A., Jones, T.L. & Rodriguez, W., 2012. Investing in IT Security: How to Determine the Maximum Threshold. *International Journal of Information Security and Privacy*, 6(3), pp.75–87.

Eloff, M.M. & Von Solms, S.H., 2000. Information Security Management: An Approach to Combine Process Certification and Product Evaluation. *Computers & Security*, 19(8), pp.698–709.

eWeek, 2016. Spending on Information Security Expected to Rise in 2016. Available at: http://www.eweek.com/it-management/spending-on-information-security-expected-to-rise-in-2016.html.

Feldman, S.S. & Horan, T.A., 2011. The Dynamics of Information Collaboration: A Case Study of Blended IT Value Propositions for Health Information Exchange in Disability Determination. *Journal of the Association for Information Systems*, 12(2), pp.189–207.

Fenz, S., Ekelhart, A. & Neubauer, T., 2011. Information Security Risk Management: In Which Security Solutions Is It Worth Investing? *Communications of the Association for Information Systems*, 28(1), pp.329–356.

Fitzgerald, T., 2007. Clarifying the Roles of Information Security: 13 Questions the CEO, CIO, and CISO must ask each other. *Information Systems Security*, 16(5), pp.257–263.

Flick, U., 2014. *An Introduction to Qualitative Research*, Los Angeles: Sage.

Flick, U., 2008. *Managing Quality in Qualitative Research*, London: Sage Publications.

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

Gao, X., Zhong, W. & Mei, S., 2015. Security Investment and Information Sharing under an Alternative Security Breach Probability Function. *Information Systems Frontiers*, 17(2), pp.423–438.

Gartner, 2011. Gartner Highlights Strategies for Dealing with the Increase in Advanced Targeted Threats. Available at: http://www.gartner.com/newsroom/id/1774514.

Gartner, 2015. Gartner Says Worldwide Information Security Spending Will Grow Almost 4.7 Percent to Reach 75.4 Billion in 2015. Available at: http://www.gartner.com/newsroom/id/3135617.

Gartner, 2016. Magic Quadrant for Enterprise Data Loss Prevention. Available at: https://www.gartner.com/doc/reprints?id=1-2X96R6A&ct=160128&st=sb.

Ghose, A. & Rajan, U., 2006. The Economic Impact of Regulatory Information Disclosure on Information Security Investments, Competition, and Social Welfare. In R. Anderson, ed. *Proceedings of the Fifth Annual Workshop on the Economics of Information Security*. Cambridge, England, UK: University of Cambridge.

Gillies, A., 2011. Improving the Quality of Information Security Management Systems with ISO 27000. *The TQM Journal*, 23(4), pp.367–376.

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

Gordon, L.A. & Loeb, M.P., 2006b. Economic Aspects of Information Security: An Emerging Field of Research. *Information Systems Frontiers*, 8(5), pp.335–337.

Gordon, L.A. & Loeb, M.P., 2002a. Return on Information Security Investments: Myths vs. Reality. *Strategic Finance*, 84(5), pp.26–31.

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

Gordon, L.A., Loeb, M.P. & Lucyshyn, W., 2003. Sharing Information on Computer Systems Security: An Economic Analysis. *Journal of Accounting and Public Policy*, 22(6), pp.461–485.

Grant Thornton, 2015. Cyber Attacks Cost Global Business 300bn+. Available at: http://www.grantthornton.global/insights/articles/cyber-attacks-cost-global-business-over-300bn-a-year/.

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

Huang, C.D. & Behara, R.S., 2013. Economics of Information Security Investment in the Case of Concurrent Heterogeneous Attacks with Budget Constraints. *International Journal of Production Economics*, 141(1), pp.255–268.

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

Humphreys, T., 2006. State-of-the-Art Information Security Management Systems with ISO/IEC 27001: 2005. *ISO Management Systems*, 6(1), pp.15–18.

Hwang, G.-J. & Wang, S.-Y., 2016. Single Loop or Double Loop Learning: English Vocabulary Learning Performance and Behavior of Students in Situated Computer Games with Different Guiding Strategies. *Computers & Education*, 102, pp.188–201.

Jakoubi, S. et al., 2009. A Survey of Scientific Approaches Considering the Integration of Security and Risk Aspects into Business Process Management. In *Proceedings of the 20th International Workshop on Database and Expert Systems Application (DEXA 2009)*. pp. 127–132.

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

Jing, L., 2009. Risk Evaluation Process Model of Information Security. In *International Conference on Measuring Technology and Mechatronics Automation*. pp. 321–324.

Jones, M. & Price, R.L., 2001. Organizational Knowledge Sharing in ERP Implementation: A Multiple Case Study Analysis. In J. I. D. Sumit Sarkar Veda C.

Storey, ed. *Proceedings of the Twenty-Second International Conference on Information Systems*. New Orleans, Louisiana, USA: Association for Information Systems.

Kearns, G.S. & Lederer, A.L., 2004. The Impact of Industry Contextual Factors on IT Focus and the Use of IT for Competitive Advantage. *Information & Management*, 41(7), pp.899–919.

Klimoski, R., 2016. Critical Success Factors for Cybersecurity Leaders: Not Just Technical Competence. *People and Strategy*, 39(1), pp.14–18.

Knapp, K.J. et al., 2009. Information Security Policy: An Organizational-Level Process Model. *Computers & Security*, 28(7), pp.493–508.

Krücken, G., 2003. Mission Impossible? Institutional Barriers to the Diffusion of the "Third Academic Mission" at German Universities. *International Journal of Technology Management*, 25(1-2), pp.18–33.

Kumar, R.L., Park, S. & Subramaniam, C., 2008. Understanding the Value of Countermeasure Portfolios in Information Systems Security. *Journal of Management Information Systems*, 25(2), pp.241–280.

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

Lacity, M.C., Khan, S.A. & Willcocks, L.P., 2009. A Review of the IT Outsourcing Literature: Insights for Practice. *The Journal of Strategic Information Systems*, 18(3), pp.130–146.

Lederer, A.L. et al., 1990. Information System Cost Estimating: A Management Perspective. *MIS Quarterly*, 14(2), pp.159–176.

Liu, C.Z., Zafar, H. & Au, Y.A., 2014. Rethinking FS-ISAC: An IT Security Information Sharing Network Model for the Financial Services Sector. *Communications of the Association for Information Systems*, 34, pp.15–36.

Liu, L. et al., 2011. From Transactional User to VIP: How Organizational and Cognitive Factors Affect ERP Assimilation at Individual Level. *European Journal of Information Systems*, 20(2), pp.186–200.

Liu, W., Tanaka, H. & Matsuura, K., 2008. Empirical-Analysis Methodology for Information-Security Investment and Its Application to Reliable Survey of Japanese Firms. *Information and Media Technologies*, 3(2), pp.464–478.

Locher, C., 2005. Methodologies for Evaluating Information Security. Investments - What Basel II Can Change in the. Financial Industry. In C. W. Federico Rajola Jannis Kallinikos David E. Avison Robert Winter Phillip Ein-Dor Jörg Becker Freimut Bodendorf Dieter Bartmann, ed. *Proceedings of the Thirteenth European Conference on Information Systems*. Regensburg, Germany: Association of Information Systems.

Majchrzak, A. et al., 2000. Technology Adaptation: The Case of a Computer-Supported Inter-Organizational Virtual Team. *MIS Quarterly*, 24(4), pp.569–600.

Massacci, F., Prest, M. & Zannone, N., 2005. Using a Security Requirements Engineering Methodology in Practice: The Compliance with the Italian Data Protection Legislation. *Computer Standards & Interfaces*, 27(5), pp.445–455.

Mattia, A. & Dhillon, G., 2003. Applying Double Loop Learning to Interpret Implications for Information Systems Security Design. In *Proceedings of the 2003 IEEE International Conference on Systems, Man and Cybernetics*. Washington, D.C., USA: IEEE Computer Society, pp. 2521–2526.

McCrohan, K.F., Engel, K. & Harvey, J.W., 2010. Influence of Awareness and Training on Cyber Security. *Journal of Internet Commerce*, 9(1), pp.23–41.

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

Mizzi, A., 2010. Return on Information Security Investment-The Viability of an Anti-Spam Solution in a Wireless Environment. *International Journal of Network Security*, 10(1), pp.18–24.

Mukhopadhyay, A. et al., 2013. Cyber-Risk Decision Models: To Insure IT or Not? *Decision Support Systems*, 56, pp.11–26.

Neubauer, T. & Heurix, J., 2008. Defining Secure Business Processes with Respect to Multiple Objectives. In S. Jakoubi, S. Tjoa, & E. R. Weippl, eds. *Proceedings of the Third International Conference on Availability, Reliability and Security*. Barcelona, Spain: IEEE Computer Society, pp. 187–194.

Neubauer, T., Klemen, M. & Biffl, S., 2006. Secure Business Process Management: A Roadmap. In M. Lanzenberger, ed. *Proceedings of the First International Conference on Availability, Reliability and Security*. Vienna, Austria: IEEE Computer Society, pp. 1–8.

Nguyen, N. & Leblanc, G., 2001. Corporate Image and Corporate Reputation in Customers' Retention Decisions in Services. *Journal of Retailing and Consumer Services*, 8(4), pp.227–236.

Van Niekerk, J. & Solms, R. von, 2004. Organisational Learning Models for Information Security. In *Proceedings of the 4th ISSA 2004 Enabling Tomorrow Conference (ISSA 2004)*.

Olifer, D. et al., 2017. Controls-Based Approach for Evaluation of Information Security Standards Implementation Costs. *Technological and Economic Development of Economy*, 23(1), pp.196–219.

Oppliger, R., 2007. IT Security: In Search of the Holy Grail. *Communications of the ACM*, 50(2), pp.96–98.

Paré, G., 2004. Investigating Information Systems with Positivist Case Research. *Communications of the Association for Information Systems*, 13(1), pp.233–264.

Park, E.H., Kim, J. & Park, Y.S., 2017. The Role of Information Security Learning and Individual Factors in Disclosing Patients' Health Information. *Computers & Security*, 65, pp.64–76.

Ponemon Institute, 2015a. *2015 Cost of Data Breach Study: Global Analysis*, Ponemon Institute.

Ponemon Institute, 2015b. Cost of Data Breach Grows as does Frequency of Attacks. Available at: http://www.ponemon.org/blog/cost-of-data-breach-grows-as-does-frequency-of-attacks.

Procter, S., Currie, G. & Orme, H., 1999. The Empowerment of Middle Managers in a Community Health Trust: Structure, Responsibility and Culture. *Personnel Review*, 28(3), pp.242–257.

Puhakainen, P. & Siponen, M., 2010. Improving Employees' Compliance through Information Systems Security Training: An Action Research Study. *MIS Quarterly*, 34(4), pp.757–778.

Qian, X. et al., 2017. A Game-Theoretic Analysis of Information Security Investment for Multiple Firms in a Network. *Journal of the Operational Research Society*, 68(10), pp.1290–1305.

Reychav, I. et al., 2016. Using Tablets in Medical Consultations: Single Loop and Double Loop Learning Processes. *Computers in Human Behavior*, 61, pp.415–426.

Rodriguez, A., Fernández-Medina, E. & Piattini, M., 2007. A BPMN Extension for the Modeling of Security Requirements in Business Processes. *IEICE Transactions on Information and Systems*, 90(4), pp.745–752.

Rowe, B.R. & Gallaher, M.P., 2006. Private Sector Cyber Security Investment Strategies: An Empirical Analysis. In R. Anderson, ed. *Proceedings of the Fifth Workshop on the Economics of Information Security*. Cambridge, England: Unversity of Cambridge.

Rowe, C., 1996. Evaluating Management Training and Development: Revisiting the Basic Issues. *Industrial and Commercial Training*, 28(4), pp.17–23.

Saint-Germain, R., 2005. Information Security Management Best Practice based on ISO/IEC 17799. *Information Management*, 39(4), pp.60–66.

SANS Institute, 2016. *IT Security Spending Trends*, SANS Institute.

Schlienger, T. & Teufel, S., 2005. Tool Supported Management of Information Security Culture. In R. Sasaki et al., eds. *Security and Privacy in the Age of Ubiquitous Computing*. IFIP Advances in Information and Communication Technology. Springer, pp. 65–77.

Sheen, J.N., 2010. Fuzzy Economic Decision-Models for Information Security Investment. In *Proceedings of the Ninth WSEAS International Conference on Instrumentation, Measurement, Circuits and Systems*. Hangzhou, China: Association for Computing Machinery, pp. 141–147.

Silva, L. & Hirschheim, R., 2007. Fighting Against Windmills: Strategic Information Systems and Organizational Deep Structures. *MIS Quarterly*, 31(2), pp.327–354.

Sonnenreich, W., Albanese, J. & Stout, B., 2005. Return On Security Investment (ROSI): A Practical Quantitative Model. *Journal of Research and Practice in Information Technology*, 38(1), pp.239–252.

Stewart, G. & Lacey, D., 2012. Death by a Thousand Facts: Criticising the Technocratic Approach to Information Security Awareness. *Information Management & Computer Security*, 20(1), pp.29–38.

Tanaka, H., Matsuura, K. & Sudoh, O., 2005. Vulnerability and Information Security Investment: An Empirical Analysis of E-Local Government in Japan. *Journal of Accounting and Public Policy*, 24(1), pp.37–59.

Toivanen, H., 2015. *Case Study of Why Information Security Investment Decision Fail?* Doctoral Thesis, University of Jyvaskyla, Finland.

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

Turoff, M. & Plotnick, L., 2012. The ISCRAM Future Threat Delphi: Nostradamus Revisited. In Z. F. Jozef Ristvej Leon Rothkrantz, ed. *Proceedings of Ninth International ISCRAM Conference*. Vancouver, Canada: Simon Fraser University, Vancouver, Canada.

Vallerand, J., Lapalme, J. & Moıse, A., 2017. Analysing Enterprise Architecture Maturity Models: A Learning Perspective. *Enterprise Information Systems*, 11(6), pp.859–883.

vom Brocke, J., Strauch, G. & Buddendick, C., 2007. Return on Security Investments–Towards a Methodological Foundation of Measurement Systems. In J. Xohmeier & S. Hayne, eds. *Proceedings of the Thirteenth Americas Conference on Information Systems*. Keystone, Colorado, USA: Association for Information Systems.

von Solms, B. & von Solms, R., 2004. The 10 Deadly Sins Of Information Security Management. *Computers & Security*, 23(5), pp.371–376.

Vroom, C. & von Solms, R., 2004. Towards Information Security Behavioural Compliance. *Computers & Security*, 23(3), pp.191–198.

Wang, J., Chaudhury, A. & Rao, H.R., 2008. A Value-at-Risk Approach to Information Security Investment. *Information Systems Research*, 19(1), pp.106–120.

Wang, S.-L. et al., 2011. Risk-Neutral Evaluation of Information Security Investment on Data Centers. *Journal of Intelligent Information Systems*, 36(3), pp.329–345.

Wawrzyniak, D., 2006. Information Security Risk Assessment Model for Risk Management. In C. L. Stevel Furnell Simone Fischer-Hübner, ed. *Proceedings of the Third international Conference on Trust, Privacy, and Security in Digital Business*. Wroclaw, Poland: Springer, pp. 21–30.

Weishäupl, E., Yasasin, E. & Schryen, G., 2015. A Multi-Theoretical Literature Review on Information Security Investments using the Resource-Based View and the Organizational Learning Theory. In D. Leidner & J. Ross, eds. *Proceedings of the Thirty Sixth International Conference on Information Systems*. Fort Worth, TX, USA: Association for Information Systems.

Werlinger, R., Hawkey, K. & Beznosov, K., 2009. An Integrated View of Human, Organizational, and Technological Challenges of IT Security Management. *Information Management & Computer Security*, 17(1), pp.4–19.

Wylder, J.O., 2003. Improving Security from the Ground Up. *Information Systems Security*, 11(6), pp.29–38.

Yin, R.K., 2011. *Applications of Case Study Research*, Los Angeles, London, New Delhi, Singapore, Washington DC: Sage Publications, Inc.

Yin, R.K., 2003. *Case Study Research: Design and Methods*, Los Angeles, London, New Delhi, Singapore, Washington DC: Sage Publications, Inc.

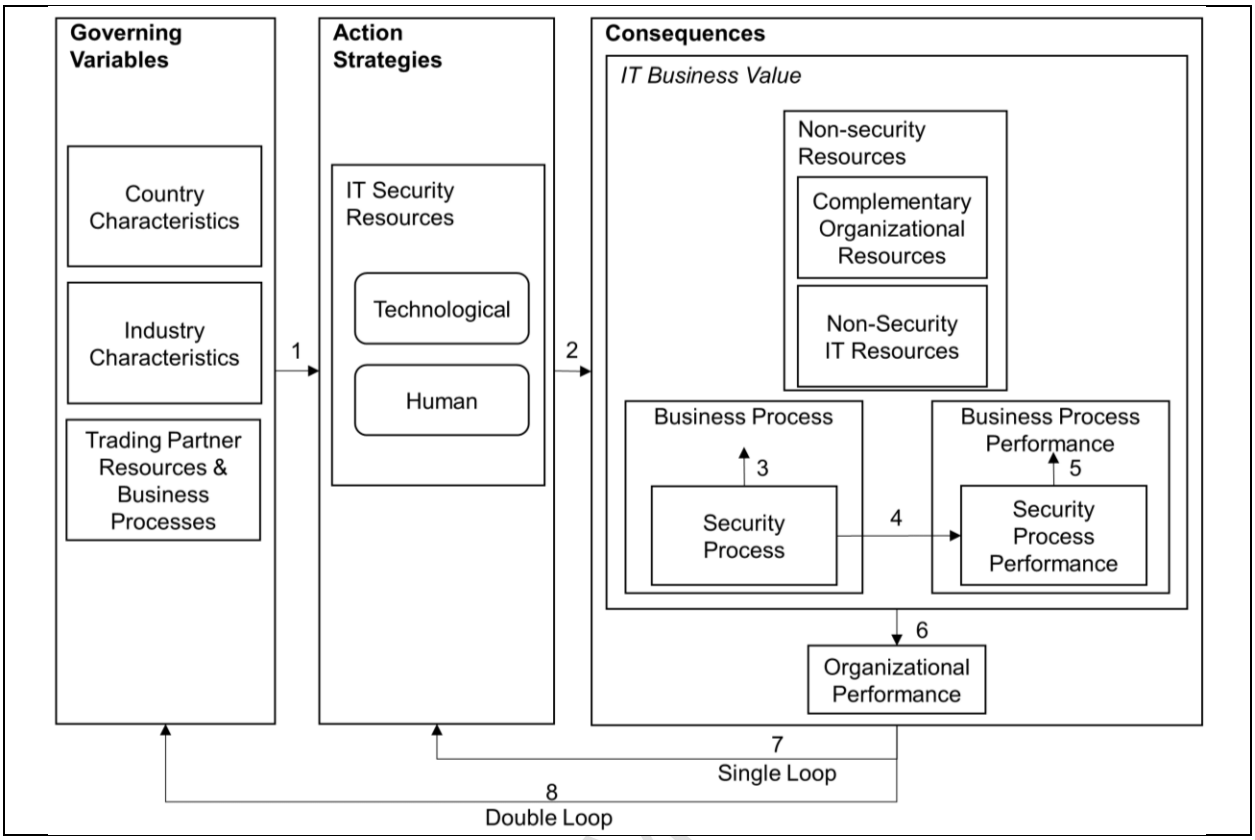

Figure 1. A Resource-based Learning Model for Information Security Investments based on Argyris et al. (1985)**,** Melville et al. (2004) **and** Weishäupl et al. (2015)

Table 1. Research Themes

RT 1:	Influence of External Factors on Decisions to Invest in Information Security Resources
RT 2:	Investment in Information Security Resources based on Underlying Decision Process
RT 3:	Security Processes and their Influence on Business Processes and Measurement of Process Performances
RT 4:	Metrics and Evaluation Processes Used to Measure the Changes in Organizational Performance
RT 5:	Usage of Single and Double Loop Learning Strategy for Information Security Investments

Table 2. Profiles of the Interviewed Consulting Firms

	CF 1	CF 2	CF 3	CF 4	CF 5	CF 6	CF 7
Interviewee(s)	Chief Executive Officer & Consultant	Chief Executive Officer	Sales Director & Director Marketing	Senior Manager & Consultant	Senior Manager	Senior Manager	Consultant
Number of employees	<100	<20	<100	<100,000	>100,000	< 5,000	<100,000

Table 3. Profiles of the Interviewed Non-Consulting Firms

	NCF 1	NCF 2	NCF 3	NCF 4	NCF 5
Sector of Industry	Tertiary sector	Secondary sector	Secondary sector	Tertiary sector	Quaternary sector
Interviewee(s)	CISO	CISO	Head of IT Governance and Head of IT Security Strategy	CEO	Head of Data Center
Number of employees	< 3,000	< 5,000	< 50,000	< 20	< 100

Table 4. Empirical Findings - Effect of External Factors

External Factors	Statements of Interview Partners
Country Characteristics	▪ "*We have to comply with the German Federal Data Protection Act and the IT Security Act. We are not allowed to do anything what violates data protection.*" (NCF 1) ▪ "*A big customer uses encryption because he is forced by the German Criminal Code, which contains regulations concerning medical confidentiality. The company physician keeps digital medical records which could otherwise be accessed by the IT staff.*" (CF 3) ▪ "*I need to consider why I have to invest in information security and, economically thinking there are only two possibilities: Either my reputation is damaged or I am forced externally by laws to act.*" (NCF 5)
Industry Characteristics	▪ "*If I want to operate a business in the credit card industry, I have to comply with PCI DSS.*" (CF 2) ▪ In the health care sector "*a data transmission standard enters into force when data is transmitted but it is rather a technical standard.*" (CF 3)
Trading Partner Resources & Business Processes	▪ "*A few OEMs designed their own standard which suppliers need to comply with.*" (NCF 2) ▪ "*Outsourcing is common in particular in large firms […]. For instance, those external partners are also involved in the security management of the firm*." (CF 7). ▪ "*We observe a trend in the area of application development that large customers demand certifications.*" (NCF 3) ▪ "*The construction sector is comparatively slow-moving when it comes to security awareness, meaning that they do not attach great importance to certifications. In comparison, industrial companies increasingly demand that we proof the security of our systems.*" (NCF 3)

Table 5. Empirical Findings – IT Security Resources based on Decision Processes

Resources and Processes	**Statements of Interview Partners**
Technological IT Security Resources	▪ "*Every company has basic technical equipment that the market has to* offer." (CF 7) ▪ "*The technological solutions require the least workload because they are the easiest to implement. Organizational countermeasures are more laborious.*" (NCF 2) ▪ "*The advantage of technological measures is that they are preventive and we always try to work preventively when it comes to security.*" (NCF 2)
Human IT Security Resources	▪ "*In particular, industries in which information is of critical importance, such as the finance and telecommunication industry, do have a CISO*" (CF 6) and "*in large automotive firms, you can expect to find CISO positions.*" (CF 7) ▪ "*If the CISO is located hierarchically below the CIO, which is very common, then he will not have significant influence*" (CF 6). ▪ "*Because of conflicts of interest, it would make sense to grant the CISO independence from the CIO.*" (CF 2) ▪ "*You will regularly find dedicated security departments in large organizations. In smaller organizations such a structure is less common.*" (CF 6) ▪ "*I have barely seen large [security] departments, even in bigshot companies. I am not aware of a core team which consists of more than 10 people and we are talking about a global company.*" (CF 3) ▪ "*Awareness is a complex issue that has not yet been discovered entirely. Influencing the behavior of 200,000 employees is a challenging task. In addition, IT security tends to be managed by technicians who are more knowledgeable in technology rather than in human behavior.*" (CF 3)
Underlying Decision Processes	▪ "*We use a two-dimensional matrix, either with costs-effort or cost-benefit. Sometimes, a strategy pyramid is of help.*" (NCF 2) ▪ Assets which need to be protected tend to be determined based on a risk analysis (CF 4) but "*risk depends on the probability of occurrence which is always a gut feeling. That's the problem of risk no matter which risk model you use.*" (CF 2)

Table 6. Empirical Findings – Analysis of Security Processes

Analysis of Security Processes	**Statements of Interview Partners**
Security Process and Influence on Business Process	▪ "*Most organizations have established security processes which determine access to buildings, departments and individual rooms or the interaction with visitors. The 'C' and 'A' in the PCDA cycle is missing in most organizations […]. Most firms regard it rather as a state than a process.*" (CF 3) ▪ "*The business process runs without the security process: That is exactly the problem: […] The business has to run and security is not part of what is necessary as the business also runs without any security precautions.*" (CF 3) ▪ "*Security disturbs the employees because of long passwords and requirements to change passwords regularly.*" (CF 3) ▪ "*IT security is at its best when it is unseen by employees.*" (CF 3) ▪ "*A mind change is necessary. Security is a core part of the business process otherwise it would not be needed.*" (CF 3)
Security Process Performance	▪ The quality of security processes "*can be measured by withstanding external audits, for instance ISO 27001. I do think that this is the only quality criterion.*" (CF 3) ▪ "*Audits are the classic tool for monitoring the efficiency and effectiveness of security processes.*" (CF 4)

Table 7. Empirical Findings – Security Metrics and Evaluation Processes

Metrics and Processes	**Statements of Interview Partners**
Security Metrics	▪ "*Key Performance Indicators (KPIs) and Key Goal Indicators (KGIs), for example uptimes, are mainly used in large organizations.*" (CF 2) ▪ "*ROSI is a very abstract and theoretical metric and includes a considerable element of uncertainty.*" (NCF 2) ▪ "*There are no metrics used on how many viruses have been stopped or whether a cheaper or better application is available.*" (CF 1)
Evaluation Processes	▪ "*At the end of the year, a retrospect takes place but there are no evaluation processes.*" (NCF 4) ▪ "*During my term in office, I have never found a single evaluation process established by a client.*" (CF 1) ▪ "*We evaluate information security investments based on gut feeling, not based on metrics.*" (NCF 3) ▪ It is more common that external and internal audits are carried out: "*External audits are conducted in order to check whether the processes are implemented properly*" (CF 7) and "*internal audits are conducted based on a standardized questionnaire. Moreover, our customers visit and perform an audit.*" (NCF 2) ▪ "*Firms know their revenue and how much they have invested in information security but quantifying the link is difficult because you do not know how many attacks and how much loss are prevented*." (CF 5)

Table 8. Empirical Findings – Learning Strategies

Learning Strategies	Statements of Interview Partners
Single Loop Learning	▪ "*When a firm is satisfied with their security measures, it tries to maintain the status quo as improving has a lower priority than maintaining. They only improve something if there is a problem. In practice, decisions to invest are always event-driven.*" (CF 3) ▪ "*As organizations are profit-driven, the objective is always to solve existing problems with minimal effort and costs*." (CF 2) ▪ "*In large firms in which fluctuation is high, the CEO is interested in increasing profit in this very year to benefit his reputation because he might be replaced soon and investing in security is a long-term investment.*" (CF 2)
Double Loop Learning	▪ "*First, we apply selective countermeasures where needed. Then we make a big fix when the budget plan is developed for the next year. During the year, there is no money for a big fix, only for little countermeasures.*" (NCF 2) ▪ "*We regularly gain an overview of the threat level and how we are prepared against these threats so that we can react quickly to changing situations.*" (NCF 2)

Table 9. Summary of Empirical Findings

Research Theme	Empirical Findings
RT 1: Influence of External Factors on Decisions to Invest in Information Security Resources	▪ Main external drivers are country characteristics, legal frameworks, regulations and acts which are mandatory and put pressure on organizations ▪ The influence of the external pressure by laws depends on industry and firm size ▪ Few firms are driven in their information security investment decision by their location, their image and fear caused by recent incidents ▪ Firms invest in "classical" technological (firewalls, antivirus programs etc.) and human security resources (e.g., CISO, workshops for employees) without any standardized decision processes ▪ The investment in human security resources depends on the industry and size – Large organizations and firms in critical industries employ a CISO and have dedicated departments for information security – This trend is extending to smaller firm sizes and other industries due to a rising awareness of the importance of information security
RT 2: Investment in Information Security Resources based on Underlying Decision Processes	▪ Decisions are made by the CISO in collaboration with the information security department (if it exists) and the CIO depending on the CISO's hierarchical position within the organization ▪ Different opinions and preferences are discussed without using formal multi-stakeholder decision models ▪ Investments in technological and human information security resources are mostly made based on risk analyses or gut feeling
RT 3: Security Processes and their Influence on Business Processes and Measurement of Process Performances	▪ Firms often establish security processes to safeguard the confidentiality, integrity and availability of business ▪ Impact of the security processes on the business processes was judged to be negative ▪ Security processes are regularly evaluated by external audits ▪ Performance of security processes is rarely measured in practice because of its complexity ▪ Effect of the security process performance on the business process performance is stated to be negative and not measured in numbers
RT 4: Metrics and Evaluation Processes Used to Measure the Changes in Organizational Performance	▪ Evaluation processes are barely used in practice to evaluate the effectiveness and efficiency of information security investments ▪ Firms are forced to evaluate when external pressure exists (audits), business processes do not run smoothly, or the IT budget is reallocated ▪ The usage of metrics for information security investments is absent: – Metrics include assumptions which are difficult to assess in practice – In their current form, metrics' applicability is limited because they do not adequately reflect the given facts embodied in practice
RT 5: Usage of Single and Double Loop Learning Strategy for Information Security Investments	▪ Learning strategy is always triggered by incidents and not motivated intrinsically ▪ Firms prefer single loop learning as a fast reaction to incidents rather than searching for a long lasting rectification ▪ For human security resources learning takes place because firms consider the fluctuation of the employees and the fact that employees quickly forget lessons learned in past workshops ▪ Once technological security resources are installed, they are not questioned any more with regard to their suitability to changing environmental factors

Table 10. Empirical Insights in the Light of Previous Findings and in the Light of Distinguishing Consulting and Non-consulting Firms

Research Themes	Aligning New Insights with the Literature	Distinguishing New Insights for Consulting Firms from those for Non-Consulting Firms
RT 1: Influence of External Factors on Decisions to Invest in Information Security Resources	Consensus regarding the importance of standards, e.g., ISO 27000 series (e.g., Calder 2009; Gillies 2011; Humphreys 2006)	Mismatch regarding compliance with legal requirements. While non-consulting firms indicate a compliance by all means, the consulting firms noted fear as a mandatory trigger for compliance.
RT 2: Investment in Information Security Resources based on Underlying Decision Process	Mismatch regarding distinction between IT budget and IT security budget: Models in literature require an IT security budget (e.g., Bojanc & Jerman-Blažic 2008; Bojanc et al. 2012; Gordon & Loeb 2006a), whereas in practice this distinction is blurry. Match regarding the absence of standardized decision-processes (Dor & Elovici 2016).	Mismatch regarding decision processes: According to consulting firms, decisions are based on gut feeling, non-consulting firms reported that methods (e.g., risk analysis) are used.
RT 3: Security Processes and their Influence on Business Processes and Measurement of Process Performances	Mismatch regarding motivation to implement security processes: In literature, security processes are motivated intrinsically (e.g., Ashenden 2008; Massacci et al. 2005), whereas in practice, the implementation of security processes is extrinsically motivated.	Mismatch regarding the impact of security processes on business processes: In non-consulting firms, security processes are perceived as slowing down the business processes. Consulting firms recognize this fact as the main problem and propose a mind change in the tradeoff between the importance of security processes and their negative impact on the business processes.
RT 4: Metrics and Evaluation Processes Used to Measure the Changes in Organizational Performance	Mismatch regarding evaluation processes: Evaluation processes are barely used in practice which contravenes academic literature providing several models, methods and processes for evaluation (e.g., Eloff & Von Solms 2000; Knapp et al. 2009; Vroom & von Solms 2004). We also found a mismatch regarding metrics: While academia provides several metrics (Jansen 2011; Tsiakis & Stephanides 2005), in practice none of them is applicable due to lack of information.	Consensus regarding evaluation processes: All of the interview partners stated that evaluating information security investments is difficult as the estimation of the return on investments is challenging.
RT 5: Usage of Single and Double Loop Learning Strategy for Information Security Investments	Mismatch regarding the opinion on double loop learning: In academic literature double loop	Consensus that in firms a “never change a running system” strategy / policy is applied, i.e. no

	learning is recommended and single loop learning is seen as inaccurate (e.g., Argyris 1977a; Argyris 1977b; Argyris 1976; Argyris et al. 1985). In practice, single loop learning is a fast re-action to incidents which is ap-propriate in case of attacks.	learning takes place.

Table 11. Derived Key Propositions

Proposition 1	The external regulatory and industry-specific factors have the strongest influence on the firm's information security investment actions.
Proposition 2	No standardized decision processes are applied to determine the optimal amount, time and allocation of investments.
Proposition 3	The security process impacts the business process in a disturbing way.
Proposition 4	Metrics regarding information security investment, such as ROSI, are practically not used.
Proposition 5	Firms prefer single loop learning as a fast reaction to incidents rather than searching for a long lasting rectification.

Appendix

Table 12. Research Themes and Corresponding Interview Questions

Research Theme	Interview Questions
RT 1: Influence of External Factors on Decisions to Invest in Information Security Resources	▪ Which external influences have to be considered when undertaking IT security investments? ▪ Do industry standards or norms exist? ▪ Are there any regulative frameworks? ▪ Are there any best practice approaches, which have to be considered? ▪ Are there any customer-specific or trading partner-specific demands that need to be considered? (e.g., necessary certifications)
RT 2: Investment in Information Security Resources based on Underlying Decision Processes	▪ Which IT security resources do exist? (personnel or material resources) ▪ Is there a distinction between non-security and security resources? ▪ How is the necessity of investment in IT security resources viewed? ▪ What are the IT security resources frequently invested in? ▪ Are there any decision processes when undertaking investments in IT security resources? If so, which are these? ▪ How are external influences included in IT security investment decision processes? ▪ How are objectives included in the decision processes? ▪ What kind of data or information are included in these decision processes? ▪ Are these processes standardized? ▪ Who are the process owners or decision makers? ▪ Are there various decision makers / stakeholders with different kind of preferences? (e.g., technical department, CIO, …) ▪ What are the different objectives of the stakeholders? ▪ Are these objectives at odds? ▪ How are these conflicting objectives treated or solved?
RT 3: Security Processes and their Influence on Business Processes and Measurement of Process Performances	▪ Are there any security processes which secure the confidentiality, availability and integrity of the firm (e.g., authentication processes which manage the access to firm's facilities)? If so, which are these? ▪ How is the impact of security processes on business processes viewed, treated and measured? ▪ How is the quality of security processes measured? ▪ Are these security processes standardized? ▪ Who is in charge of the security processes? ▪ How are the security processes evaluated?
RT 4: Metrics and Evaluation Processes Used to Measure the Changes in Organizational Performance	▪ What kind of evaluation processes take place in order to determine and to measure the improvement of the business processes and the overall organizational performance through IT security investments? ▪ Which data are included in these evaluation processes? ▪ How are external impacts included in these evaluation processes? ▪ Is a relation between IT security resources and revenue established? ▪ Are metrics to evaluate IT security investments used? If so, which are these? ▪ What kind of process metrics are used?
RT 5: Usage of Single and Double Loop Learning Strategy for Information Security Investments	▪ What is the frequency of evaluating the results from IT security investments? ▪ How are the results of evaluation processes from past investment decisions included in future investment decision processes? ▪ Is the focus on solving existing problems in order to improve the existing system without major modifications after having evaluated? If so, how? Are there any examples? ▪ Do the conclusions from evaluation processes result in changes, modifications of the framework conditions, objectives or assumptions? If so, how? Are there any examples?