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

Completed Research Paper

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
University of Regensburg
Universitätsstraße 31
93053 Regensburg
guido.schryen@wiwi.uni-regensburg.de

Abstract

The protection of information technology (IT) has become and is predicted to remain a key economic challenge for organizations. While research on IT security investment is fast growing, it lacks a theoretical basis for structuring research, explaining economic-technological phenomena and guide future research. We address this shortcoming by suggesting a new theoretical model emerging from a multi-theoretical perspective adopting the Resource-Based View and the Organizational Learning Theory. The joint application of these theories allows to conceptualize in one theoretical model the organizational learning effects that occur when the protection of organizational resources through IT security countermeasures develops over time. We use this model of IT security investments to synthesize findings of a large body of literature and to derive research gaps. We also discuss managerial implications of (closing) these gaps by providing practical examples.

Keywords: Information Security, Investment, Literature review, Resource-based View, Organizational Learning Theory, Multi-theoretical Perspective

Introduction

The protection of information technology (IT) has become and is predicted to remain a key challenge for organizations, which need to secure their IT systems, data, intellectual property, and business processes against attacks, misuse or technical failures (Anderson 2001; Frost & Sullivan 2013; Gartner 2011, 2012; Whitman 2003). IT threats can lead, for example, to the disruption of production and service processes (e.g., attack on MasterCard and Visa (The Guardian 2010)) and data theft (e.g., attack on Sony Pictures Entertainment (The Washington Post 2014)), which, in turn, result in economic damage, including losses in productivity and revenue, strategic disadvantages and loss of reputation (Bandyopadhyay et al. 2009). Many security incidents are attributable to cybercrime, which can be considered a growth industry (McAfee 2014).

Industries have responded to emerging IT security threats with high investments in IT security. According to Gartner (2014), the worldwide spending on IT security reached $71.1 billion in 2014, an increase of 7.9 percent over one year, and is expected to grow further 8.2 percent in 2015. A recent survey indicates that organizations will spend an average of $381 per employee on IT security (eWEEK 2014). In the 2016 budget proposal of the U.S. government, $14 billion are reserved for cybersecurity efforts to protect federal and private networks (Thomson Reuters 2015). These figures indicate that the IT security landscape is pervaded not only by technological challenges but also by financial issues. In the presence of budget constraints, key economic questions for organizations are which of their assets (processes, systems, etc.) need which level of protection, which security countermeasures (e.g., firewalls, intrusion detection systems, security education, or security policies) lead to this protection and how much should be spent on which countermeasure (Anderson and Schneier 2005; Gordon and Loeb 2006).

IT security researchers have responded to the economic challenges of IT security with hundreds of articles. A broad set of approaches from different disciplines, including micro-economics (e.g., Grossklags et al. (2008a), finance (e.g., Buck et al. (2008)), risk management (e.g., Hoo (2000)) and organization theory (e.g., Cohen (2006)) have been applied. However, the literature is still rather fragmented, and incoherent based on the isolated adoption of different approaches and lacks a unifying theoretical basis.

In order to address these deficiencies, we ask three research questions:

1. Why and how can a multi-theoretical perspective based on the "Resource-based View" and the "Organizational Learning Theory" be used to structure and guide research on information security investments?
2. To what extent has the literature contributed to key questions of information security investments?
3. What are gaps in information security investments research that still need to be addressed?

Our approach to draw on the widely accepted "Resource-based View" and the "Organizational Learning Theory" is driven by the goal to address both the static and dynamic (temporal) protection of an organization's resources at the firm level. Adopting only one theory necessarily leads to the neglect of either the static or the dynamic perspective. We use this multi-theoretical perspective to suggest a new theoretical model on information security investments. Our synthesis of literature findings is structured according to this model, which also allows us to identify research gaps. Adopting the typology of literature reviews suggested by Paré et al. (2015, p. 186), we conduct a "*theoretical review*".

With our literature review, we contribute to the literature on information security investments in several regards: (1) to the best of our knowledge, we provide the first multi-perspective theoretical model on information security investments; (2) we comprehensively synthesize literature findings using the theoretical model; (3) we identify research gaps to guide future research.

The remainder of this paper is structured as follows: In the following section, we provide a brief introduction to information security investment research. In Section 3, we present a multi-theoretical view by discussing the Resource-based View and the Organizational Learning Theory and we suggest an integrative model on information security investments. The literature search and selection is described in Section 4. Section 5 synthesizes the literature and identifies research gaps, before we discuss our results in Section 6. We conclude our paper in Section 7.

Information Security Investment Research

Effectiveness and economic efficiency of information security investments has been an important research topic for a long time (Kwon and Johnson 2014). Currently, there are three interdisciplinary streams of research related to information security investments: (1) Micro-economic approaches based on game theory (e.g., Grossklags et al. (2008a) and Sun et al. (2008)); (2) Financial analysis based on Return on Investment (ROI), Net Present Value (NPV) and Internal Rate of Return (IRR) (e.g., Bojanc and Jerman-Blažic (2008a) and Buck et al. (2008)); and (3) Management approaches based on decision theory (e.g., Huang and Goo (2009)), risk management (e.g., Bojanc and Jerman-Blažic (2008b) and Hoo (2000)) and organization theory (e.g., Cohen (2006) and Hagen et al. (2008)). In this article, we propose a multi-theoretical model that allows us to embed the literature on the three current research streams into a comprehensive model based on the Resource-based View and the Organizational Learning Theory. For instance, game-theoretical articles, such as the paper of Grossklags et al. (2008a), deal with the influences of attacks on the firm's decision to invest in security; these influences are covered in our model, more precisely in the Governing Variables. The proposed model extends the model proposed in Weishäupl et al. (2015) by considering the dynamic properties of information security.

However, the development of a theoretical model for information security investments is a challenging task because (1) the nature of countermeasures is diverse, covering strategic and operational issues with regard to the legal, technical and organizational perspectives. (2) Unlike other investments, information security investments are not intended to earn a return, but to reduce risk, i.e., they are successful if "*nothing happened*" and thus the potential outcomes (benefits or loss) are often intangible (Kwon and Johnson 2014, p. 452). Examples of intangible outcomes are benefits related to regulatory compliance and public credibility (Kwon and Johnson 2014). Investing into information security processes or products does not provide direct return but it may have a positive impact on the organizational performance if it leads to a reduction of potential risks (Böhme and Nowey 2008). (3) The complementarity between the "ex-ante" and the "ex-post" perspectives must be taken into account. First, the approaches which adopt an "ex-ante" perspective aim at providing decision support by estimating the costs and benefits of possible investments (Böhme and Nowey 2008). Second, approaches which adopt the "ex-post" perspective reflect on investments made in the past and evaluate whether the firm's budget allocation was effective and efficient (Böhme and Nowey 2008).

The first two of these challenges can be addressed by drawing on the Resource-based View because (a) diverse assets such as systems, data or processes, which need to be protected, can be modeled as resources and (b) both tangible and intangible resources, such as firewalls, and security knowledge, can be explicitly considered (Weishäupl et al. 2015). Organizational Learning Theory is particularly suitable to address the third challenge because it takes into account the firm's ability to learn and integrate temporal and dynamic feedback loops.

Overall, both the Resource-based View and the Organizational Learning Theory, which are established theories in the IS literature (Kwon and Johnson 2014; Wade and Hulland 2004), provide an appropriate theoretical basis to frame research on information security investments. We apply both perspectives in the next section in order to suggest a multi-theoretical lens on information security investments, including the provision of an integrative theoretical model.

A Multi-Theoretical Lens on Information Security Investments

In this section, we first discuss the advantages of adopting a multi-theoretical view on information security investments. Then we apply the theoretical lenses (Resource-based View and Organizational Learning Theory) and show in which regard they are appropriate for framing information security investments. Finally, we develop a new theoretical foundation for information security investments by integrating both of these theoretical lenses.

Multiple Lenses on Information Security Investments

According to Schryen (2015), literature can be framed from different perspectives in order to provide complementary views on the literature. The impact of drawing on multiple views is threefold: First, complementary views can be synthesized into a new theoretical model, which combines the advantages of multiple perspectives. Second, the interplay between multiple perspectives provides a more comprehensive account of the literature that can be used to classify studies. Third, a combined perspective gives rise to research questions which would otherwise have remained undetected. With regard to the IS literature, there are several articles which use multi-theoretical perspectives. For instance, Jasperson et al. (2002) analyze the

link between power on the one side and IT impacts or use on the other side with the help of technology lenses and power lenses. In the field of information security, Siponen et al. (2014) use the Protection Motivation Theory, the Theory of Reasoned Action, and the Cognitive Evaluation Theory to explain employees' adherence to security policies.

In our study, we view the information security investment literature through two lenses: the Resource-based View and the Organizational Learning Theory. These two lenses are suitable because they complement each other: (1) The Resource-based View is inherently static, focusing on the possession of resources and capabilities (Elsenhardt and Martin 2000; Kraaijenbrink et al. 2010). This means that it does not account for dynamics and temporal effects. In contrast, the Organizational Learning Theory considers such effects and theorizes on learning progress made from the organization's past errors over time which ensures that an organization transforms "*information into valued knowledge which in turn increases its long-run adaptive capacity*" (Schwandt and Marquardt 1999, p. 70). It thus enables an organization to react to dynamically changing environments. (2) The Resource-based View, as suggested by Melville et al. (2004), operationalizes and covers major factors (cf. Figure 1) which need to be considered in investment decisions (Weishäupl et al. 2015), for instance the macro, competitive and focal firm environment. An advantage of the Resource-based View is that it theorizes on various components of a firm, its environment and its relations to each other. In contrast, the Organizational Learning Theory does not focus on the organization and its components in detail.

Therefore, we examine the information security investment literature using these two lenses simultaneously to suggest a new integrative theoretical model, to gain a comprehensive view on the literature and to identify corresponding and otherwise undetected research gaps.

First Theoretical Lens: The Resource-Based View

The origins of the Resource-based View, one of the most influential theories in the history of management theorizing (Kraaijenbrink et al. 2010), can be traced back to the works of Chandler (1977), Coase (1937), Penrose (1959), Stigler (1961) and Wernerfelt (1984). The key proposition is that a firm must acquire and control valuable, rare, inimitable, and non-substitutable resources and capabilities to achieve sustained competitive advantage (Barney 1991, 1994, 1997; Kraaijenbrink et al. 2010). According to Barney (1991, p. 101), a firm's resources include "*all assets, capabilities, organizational processes, firm attributes, information, knowledge, etc. controlled by a firm that enable the firm to conceive of and implement strategies that improve its efficiency and effectiveness*.

According to Weishäupl et al. (2015), information security investments are a subtype of (general) IT investments and therefore the Resource-based View is appropriate for framing information security investments for three reasons: (1) Both, non-security IT resources or assets (IT systems, data, processes, etc.), which need protection, and IT security resources, which provide protection, can be modeled as resources, with both tangible resources, such as firewalls, and intangible resources, including security knowledge, being covered (Weishäupl et al. 2015). (2) The Resource-based View has been used in the IS literature to frame information security investments. For instance, Cavusoglu et al. (2004) draw on the Resource-based View to assess hypotheses related to organizational size, security breaches and discusses the Resource-based View's link to security investments. Central elements of the Resource-based View can also be found in the work of Demirhan (2005). (3) The Resource-based View has already served as a theoretical basis for literature reviews in the IS domain, such as the "IT Business Value Model" of Melville et al. (2004). In the following, we draw on the Resource-based View, which was adapted to the information security investment context (Weishäupl et al. 2015), as shown in Figure 1 and described in Table 1.

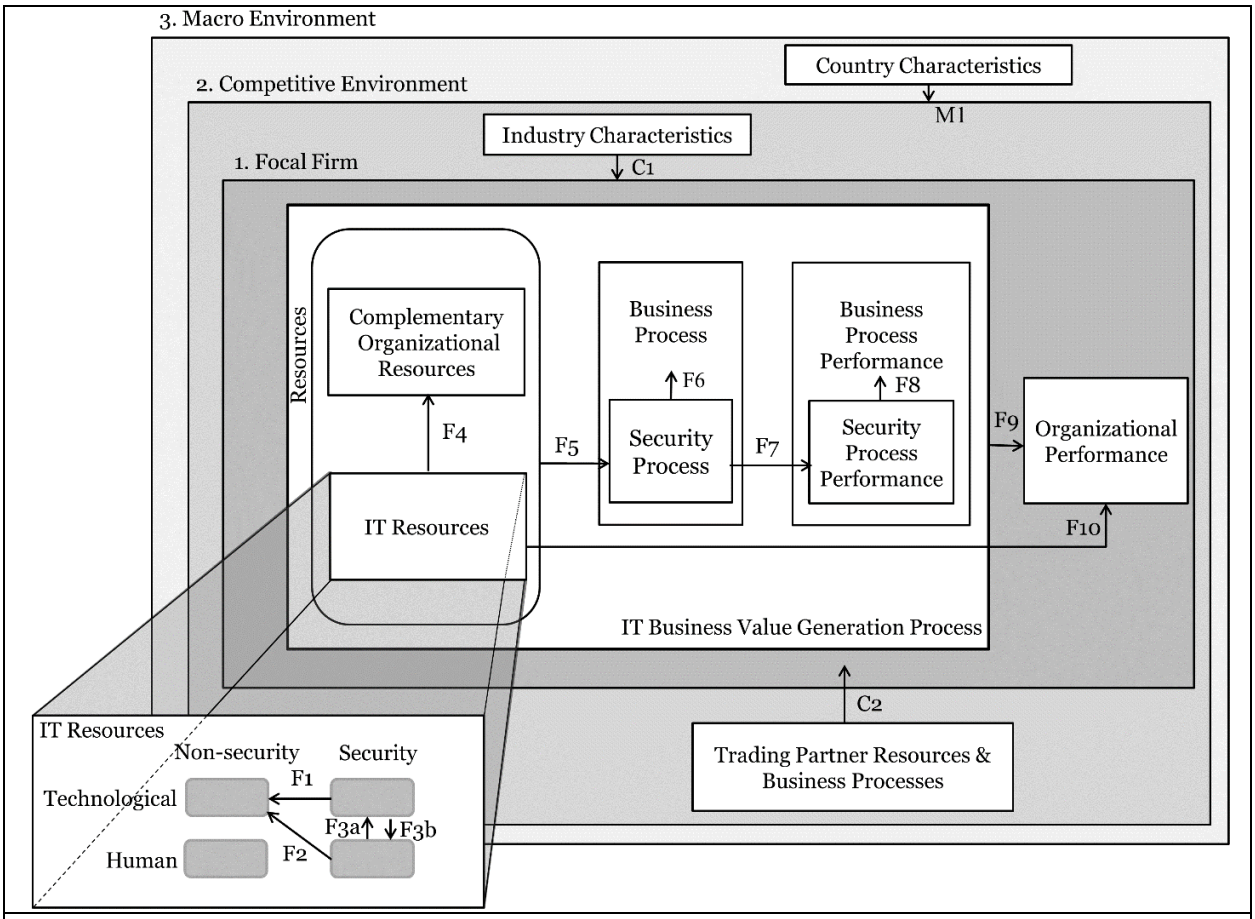

Figure 1. The Resource-based View on Information Security Investments based on (Melville et al. 2004; Weishäupl et al. 2015)

In Figure 1, the relationships between constructs mean "may improve". Impacts M1, C1 and C2 describe external factors which affect information security investment decisions of an organization. Country characteristics such as the level of development or governmental regulations influence a firm's information security investment decisions, which is depicted by the impact M1. Competitiveness, regulation, technological change, and other industry-characteristic factors (C1) and trading partners, such as buyers and suppliers (C2), have impact on a firm's decision to invest in information security.

The impacts F1 to F10 express the effects of investment in various IT security resources within the focal firm. F1 relates to the effect of technological IT security resources on technological non-security IT resources, such as investing into a firewall to protect non-security IT resources, e.g., data (e.g., Grossklags et al. (2008b), Jiang et al. (2008) and Torrellas and Vargas (2003)). As a significant number of security incidents are caused by human and not by technical failures or intruders (Beautement et al. 2008), F2 addresses the impacts of human IT security resources on technological non-security IT resources. An example is that security workshops and trainings aim at the protection of data. Impact F3a is related to effects of human IT security resources on technological IT security resources (e.g., workshops on usage of intrusion detection systems influence the IDS) with F3b vice versa (e.g., systems that control file transfer warn employees and therefore train their awareness).

Impact F4 relates to the effect of IT resources on complementary organizational resources, such as the building of a firm whose access may be protected by authentication systems (Liu and Silverman 2001). Investment in IT security resources and complementary organizational resources may improve business processes or enable new ones (impact F5). Impact F6 refers to the fact that information security processes are intended to protect business processes and their underlying resources (Neubauer and Heurix 2008; X.

Wang et al. 2008). The security processes are subtypes of business processes because "*the process of security is destined to fail if it does not protect the process of business*" (Wattel 2002, p. 177). The effectivity of a security process is measured by means of a security process performance (impact F7). The security process performance has impact on the business process performance, which is a result of the relation business process to security process and is conceptualized as impact F8. The IT business value generation process, including resources, processes, business and security performances, impacts directly the organizational performance (impact F9). Impact F10 refers to the "*direct link between IT and overall firm performance, bypassing the effect of IT on business processes*" (Dehning and Richardson 2002, p. 9).

Table 1. Definitions and Examples of Model Constructs of Figure 1 (Weishäupl et al. 2015)

Construct	Definition and Example
1. Focal Firm	
Resources: ▪ IT resources: - Technological	Hardware and software, e.g., shared technology and technology services across the enterprise, purchasing, sales, etc. (Melville et al. 2004)
- Human	Technical and managerial IT skills, e.g., training, experience, knowledge, judgment, intelligence and relationships (Barney 1991)
- Security	Resources protecting other resources, e.g., firewall, intrusion detection system, anti-virus software, authentication through biometric scan
▪ Complementary Organizational Resources	Organizational and physical resources which are complementary to IT, e.g., policies, rules, organizational structure and culture (Melville et al. 2004) as well as workers, offices and equipment
Processes: ▪ Business Process	Specific ordering of work activities and clearly identified inputs and outputs (Davenport 1993) , e.g., order taking, PC assembly, distribution (Melville et al. 2004)
▪ Security Process	Processes that help safeguard the confidentiality, integrity and availability of a firm's operations (Khansa and Liginlal 2009)
Performances: ▪ Business Process Performance	Operational efficiency of specific business processes (Melville et al. 2004), e.g., customer satisfaction (Devaraj and Kohli 2000), inventory turnover (Barua et al. 1995), gross margin and quality (Dehning and Richardson 2002)
▪ Security Process Performance	Operational efficiency of security processes, e.g., Failure to Enroll (FTE), False Match Rate (FMR) in a biometric authentication system (OECD 2004)
▪ Organizational Performance	Overall firm performance, including productivity, efficiency, profitability, market value, competitive advantage, etc. (Melville et al. 2004)
2. Competitive Environment	
Industry Characteristics	Factors which affect the application of IT within the focal firm to generate business value, e.g., competitiveness, regulation, technological change (Melville et al. 2004)
Trading Partner Resources and Business Processes	IT and non-IT resources and business processes of trading partners such as buyers and suppliers (Melville et al. 2004)
3. Macro Environment	
Country Characteristics	Macro factors shaping IT application and IT business value generation, e.g., level of development, basic infrastructure and culture (Melville et al. 2004)

Second Theoretical Lens: The Organizational Learning Theory

With the increasing globalization and the accelerating dynamics of the competitive environment, organizations need to constantly improve their products and processes in order to generate and maintain competitive advantage (Smith et al. 1996). The current interest in organizational learning among scholars and practitioners reflects this new competitive field (Hamdan 2013; Smith et al. 1996).

According to Argyris (1976, p. 365), learning is defined as "*the detection and correction of errors, and error as any feature of knowledge or of knowing that makes action ineffective*" and "*the detection and correction of error produces learning and the lack of either or both inhibits learning*". Furthermore, complex and ill-structured problems tend to be more ambiguous and are associated with a higher rate of errors, which makes it difficult to implement effective plans and actions (Argyris 1976). As information security investments are such complex problems, they would benefit from the perspective of Organizational Learning Theory specifically because it describes how the effectiveness of decisions can be improved over time by taking into account past experiences in feedback-loops. Furthermore, Organizational Learning Theory provides a dynamic view which can be used to continuously analyze the effects of investments on the security level (Culnan and Williams 2009; Culnan et al. 2008; Kwon and Johnson 2014). Conceptually, influences which affect information security investment decisions can be modeled as governing variables, investments in IT security resources can be modeled as action strategies which result in consequences such as higher security awareness.

We use the Organizational Learning Theory as suggested by Argyris et al. (1985) in the context of information security investments (cf. Figure 2 and Table 2). Organizational learning is defined as a change in the organization's knowledge because a firm gathers experience over time (cf. Argote (2011) and Fiol and Lyles (1985)). The model for Organizational Learning comprises three interconnected constructs: governing variables, action strategies and consequences. In conformance with the original model (Argyris et al. 1985), relationships are defined as "has impact on" (arrows in Figure 2):

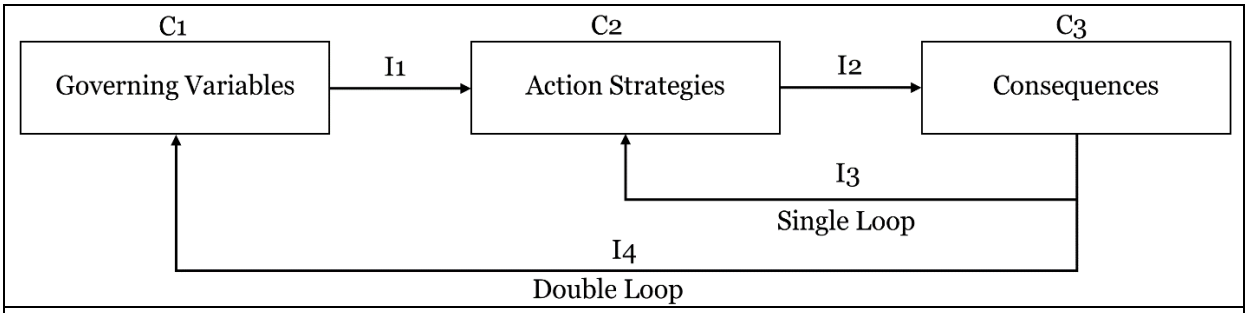

Figure 2. Organizational Learning Theory based on Argyris et al. (1985)

Governing variables (construct C1) are objectives a firm strives to achieve. As organizations align their actions with their objectives (Argyris et al. 1985), governing variables have an impact on information security investment decisions (impact I1). For instance, one objective might be the compliance with government and industry sector-specific regulations (Daneva 2006) such as the Clinger-Cohen-Act or the Federal Information Security Management Act (FISMA).

Action strategies (construct C2) are "sequences of moves" (Argyris et al. 1985) intended to fulfill certain objectives, as measured by the governing variables. In our case, action strategies are investments in IT security resources, such as the implementation of a firewall or an intrusion detection system.

Action strategies effect consequences (impact I2). An example would be investments in security workshops which are expected to reduce security incidents caused by employees (Stephanou 2009).

Consequences (construct C3) include all outcomes associated with information security investments whether they are intended or unintended, productive or counterproductive (Argyris et al. 1985). Consequences might match the governing variables if the firm has chosen an appropriate action strategy. Exemplary consequences are reduction of security incidents or increase in service availability.

Impacts 3 (I3) and 4 (I4) are complementary learning opportunities which reflect how well a firm tries to evaluate its information security investment decisions.

Impact I3 refers to single loop learning which comprises adjustments that are consistent with "*the existing set of rules and norms*" (Romme and Dillen 1997, p. 69), i.e., it does not involve changes to governing variables (Argyris 1983). For example, single loop learning occurs if the consequence of an action strategy is a decline of security incidents and the firm evaluates the positive outcome to ensure that the chosen action strategy is the best without changing the governing variables.

Impact I4 refers to the learning process which occurs in a double loop and involves modifications of "*the fundamental rules and norms underlying action and behavior*" (Argyris and Schön 1978; Romme and Dillen 1997, p. 69). Applied to the information security investment scenario, double loop learning occurs if the consequences of investment decisions do not satisfy the objectives and induce the firm to reevaluate the governing variables and invest differently. While single-loop learning is a general model of action, double loop learning provides "*feedback and more effective decision making*" (Argyris 1976, p. 363). However, "*the overwhelming amount of learning done in an organization is single loop because it is designed to identify and correct errors so that the job gets done and the action remains within the stated guidelines*" (Argyris 1977, p. 113).

Note that the constructs C1 to C3 with the impacts I1 and I2 imply a temporal sequence whereas impacts I3 and I4 describe two possibilities of evaluation and learning processes of a firm aiming to correct their potential mistakes and to make more effective and efficient decisions in the future.

Table 2. Model Constructs and Impacts in the Organizational Learning Theory (cf. Figure 2).

No.	Construct/Impact	Definition	Example
C1	Governing Variables	Objectives a firm seeks to achieve (Argyris et al. 1985).	Government and industry sector-specific regulations such as SOX or HIPAA (Daneva 2006), a firm's risk preference (Derrick Huang et al. 2008).
I1	Effect of Governing Variables on Action Strategies	To be successful in terms of the governing variables, an organization implements actions (Argyris et al. 1985).	The firm strives to maintain a certain quality of service and invests in intrusion detection systems to prevent denial of service attacks.
C2	Action Strategies	Sequences of moves used by actors in particular situations to keep the governing variables at a satisfactory level (Argyris et al. 1985).	Investments in workshops, firewalls, encryption or access control techniques.
I2	Effect of Action Strategies on Consequences	Actions have consequences for the organization's effectiveness (Argyris et al. 1985).	The investments in workshops on security results in fewer unintended security incidents caused by employees (Stephanou 2009).
C3	Consequences	Consequences of the strategies, intended or unintended, productive or counterproductive (Argyris et al. 1985).	Reduction of security incidents in the internal network or increase in service availability.
I3	Single Loop Learning	When new action strategies are used in the framework of the same governing variables. A change in action but not in the governing variables takes place (Argyris et al. 1985).	If investments in workshops effect a decline of unintended security incidents, the firm will learn from the effectiveness and consider future investments in such trainings.

I4	Double Loop Learning	Question and modify the governing variables according to the consequences (Shen and Jones 2005).	An organization adapts its investment strategy to changing environmental factors, such as investing into an improved encryption system to counteract an increased occurrence of hacker attacks.

An Integrative Model for Information Security Investments

We integrate the Resource-based View as depicted in Figure 1 and the Organizational Learning Theory as shown in Figure 2 into a multi-theoretical model (see Figure 3) which preserves the advantages of both of the original theories: the integrative 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 integrative model frames firm-characteristic components such as business process and security resources - making it compliant with the established body of research on the Resource-based View.

We merge the original theories in the following way: country characteristics, industry characteristics and trading partner resources and business processes influence firms in information security investment decision making; therefore, these factors are categorized as governing variables. Governing variables have an impact (impact 1 in Figure 3) on investment decisions in IT security resources which correspond to action strategies. For example, country-specific governmental regulations require certain investments to pass security audits (Ghose and Rajan 2006). Investments in technological or human IT security resources are associated with action strategies. This means, in particular, that investments in security training, education or awareness are part of the action strategies since they belong to human IT security resources. Note that only IT security resources are conceptualized as action strategies because we focus on investment in IT security in this article.

Investments in IT security resources have an impact on consequences which is depicted by impact 2. The consequences include the impact investments have on non-security resources, security processes, security process performance and the overall organizational performance. Impacts 3 to 6 within the consequences are adopted from the Resource-based View. Note that the construct "Business Process" within the "Consequences" refers to the business processes of the focal firm whereas the construct "Trading Partner Resources & Business Processes" in the "Governing Variables" refers to the business process of the trading partners, which influence the IT security investment decisions of the focal firm and therefore are part of the "Governing Variables".

The single and double learning loops (impacts 7 and 8) are adopted from the Organizational Learning Theory; they represent feedback loops from the consequences to the governing variables and to the action strategies.

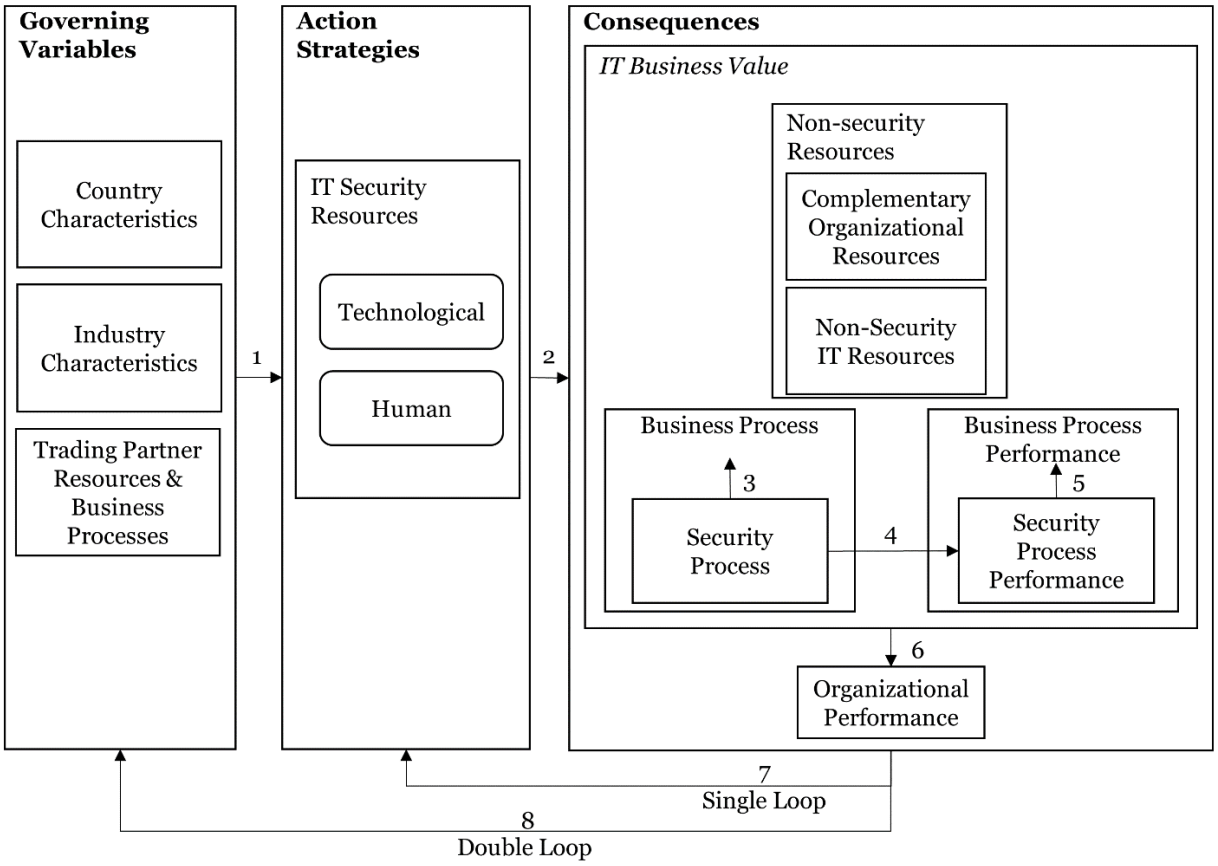

Figure 3. An Integrative Model for Information Security Investments

Definitions and examples of the impacts presented in Figure 3 are provided in Table 3.

Table 3. Impacts in the Integrative Model for Information Security Investments (cf. Figure 3)

No.	Impact	Definition	Example
1	Effects of Governing Variables on Action Strategies	Country Characteristics, Industry Characteristics, Trading Partner Resources and Business Processes influence a firm's information security investment decisions (Melville et al. 2004; Weishäupl et al. 2015).	SOX requires firms to invest in additional IT security resources in order to pass security audits (Ghose and Rajan 2006).
2	Effects of Action Strategies on Consequences	Investments in IT Security Resources (technological or human) have an impact on non-security IT resources, Complementary Organizational Resources, processes and performances (Melville et al. 2004; Weishäupl et al. 2015).	Investments in a technological IT security resource, such as biometrical authentication systems, affect non-security IT resources like data and hardware as it prevents unauthorized access to firm's premises.

3	Effects of Security Processes on Business Processes	Business Processes are constantly exposed to threats and need to run uninterruptedly to guarantee a company's success (Neubauer and Heurix 2008; X. Wang et al. 2008; Weishäupl et al. 2015).	Biometric authentication is a security process which directly influences the business process because, if the authentication system breaks down, workflows are disrupted (Weishäupl et al. 2015).
4	Effects of Security Process on Security Process Performance	The effectivity of a Security Process is expressed by a Security Process Performance.	The number of true/false or positive/negative authentication attempts measures the effectivity of an authentication system.
5	Effects of Security Process Performance on Business Process Performance	The Security Process Performance influences the Business Process Performance.	A low number of false rejection of an authentication system assures an uninterrupted workflow.
6	Effects of the IT Business Value on the Organizational Performance	All resources, processes and performances directly influence the overall firm's performance (Melville et al. 2004).	The efficiency and productivity of an organization increases when an organizational workflow is rarely interrupted and quickly recovered.
7	Single Loop Learning: Effects of Consequences on the Action Strategies	When new Action Strategies are used in the service of the same Governing Variables. A change in action but not in the Governing Variables takes place (Argyris et al. 1985). (cf. Table 2)	If investments in workshops effect a decline of unintended security incidents, the firm will learn from the effectiveness and consider future investments in such trainings. (cf. Table 2)
8	Double Loop Learning: Effects of Consequences on Governing Variables	Question and modify the Governing Variables according to the Consequences (Shen and Jones 2005). (cf. Table 2)	An organization adapts its investment strategy to changing environmental factors, such as investing into an improved encryption system to counteract an increased occurrence of hacker attacks. (cf. Table 2)

Literature Search and Selection

We followed the guidelines of Webster and Watson (2002) and implemented them by drawing on the steps suggested by Levy and Ellis (2006):

Step 1. (Inputs): We conducted a database search, as suggested by vom Brocke et al. (2009), which covered *ACM Digital Library, IEEE Xplore Digital Library, Ebsco Host Business Source Premier, Science Direct* and the *AIS Electronic Library*. Articles were identified through scanning the abstracts using the following two logical search strings:

- (invest* OR economic OR cost) AND (information OR "information technology" OR "information systems") AND ("security process" OR (secure* AND (decision OR "ex ante" OR "ex post" OR evaluat* OR audit OR monitor OR metric OR "business process")))
- (financ* OR invest* OR cost OR economic) AND "security breach" AND effect,

with "*" being the truncation symbol. We did not limit the period of time in our search. To complement our search, we queried the proceedings of the *Workshop on the Economics of Information Security (WEIS)* and *Google Scholar*. Finally, we conducted a backward search to identify further articles. We scanned the articles' abstracts and removed articles which do not focus on economics of information security. For example, we excluded articles which are purely technical (e.g., Bitter et al. (2010)) or which cover only management issues without considering investments in IT security (e.g., Chew (2008)).

Step 2. (Processing): After reading the remaining papers, we coded them according to the relationships of our integrative model of information security investments shown in Figure 3. Assigning articles to these

impacts – some articles address more than one impact – is useful in order to synthesize literature findings in a concept-centric way as suggested by Webster and Watson (2002). The concept used in this literature review is the aforementioned model.

Step 3. (Outputs): Due to page limitations, we cover the literature exhaustively but present only selected works, as described by Cooper (1988): for each of the relationships in our model of information security investments, we describe selected, exemplary works, which are representative for the findings related to the respective impact in the model.

Synthesis and Identification of Research Gaps

In this section, we synthesize the literature on information security investments according to our new model presented in Figure 3. Thus, our presentation is concept-centric as suggested by Webster and Watson (2002). From our synthesis we derive research questions for each of the impacts in Figure 3.

Effects of Governing Variables on Action Strategies

Governing variables such as country characteristics, industry characteristics, trading partner resources and business processes influence a firm's information security investment decisions, i.e., their decision on how much to invest in which IT security resources (Melville et al. 2004; Weishäupl et al. 2015). Examples for country characteristics are the New Capital Accord (Basel II) (Locher 2005) and the Gramm-Leach-Bliley Act (GLBA) for financial firms, the SOX (Sarbanes-Oxley) act for accounting firms and the HIPAA (Khansa and Liginlal 2009) for healthcare provider. Few studies focus on investment decisions in security in the light of specific national conditions and regulations and some of them conclude, interestingly, that these regulations have negative impact on investment decisions. Ghose and Rajan (2006) examine the effect of regulatory compliance and information assurance on the optimal level of investments in information security. For example, the authors find that the SOX act can have major consequences on market structure and on a firm's competitive position, although this was unintended by policy makers (Ghose and Rajan 2006). In a recent study which analyzed regulations of HIPAA in the healthcare sector, external influences have been found to reduce the impact of proactive investments on security performance (Kwon and Johnson 2014). However, a positive side-effect of these regulatory initiatives is that they increase security awareness and draw attention to information security investment announcements (Chai et al. 2011). Best practice standards, such as ITIL, COBIT, and international standards, such as ISO/IEC 27002: 2013, also affect information security investment decisions. Another factor which influences security investment decisions is the level of development of the country, in which the firm operates because culture and education of the workforce determine the need for security workshops or training (Bose and Luo 2014; Connolly and Lang 2013).

Industry characteristics influence how IT is employed within a focal firm to create business value, including competitiveness, regulation and clock speed (Melville et al. 2004). In the context of information security, a crucial factor is the integration of IT security resources of a firm's ongoing business operation and business environment which in fact means that a firm should aim at investing in IT security resources that are not only applicable in their enterprise IT architecture but also generate value (Weishäupl et al. 2015). The key challenge for a firm is thus a mixed balance between adoption of their IT security resources and the optimal investment into these which is, however, not covered by the academic literature.

Finally, the impact of a firm's trading partners with respect to information sharing and outsourcing needs to be considered. Sharing data on information security leads to decreased spending and increased levels of security since firms learn from the mistakes of other firms (Anderson et al. 2008; Gal-Or and Ghose 2005; Gordon et al. 2003; Landwehr 2004; Rowe 2007). There are good reasons for firms not to share their security-related data as these are often sensitive data, which include private data about the firm's personnel and which gives indication about corporate secrets. The transfer of such sensitive data might be misused and can cause loss of reputation and trust, negative effects on the market value of the firm and signal of weakness to adversaries (Gal-Or and Ghose 2005). To avoid such damages, Gordon et al. (2003) recommend to create financial incentives for information sharing which might be realized by legal regulation (Gal-Or and Ghose 2005).

Information outsourcing is becoming a more important subject due to the growing complexity of information security management (Lacity et al. 2009, 2010). When firms outsource their information security operations to Managed Security Service Providers (MSSPs), which offer prevention and detection services

(Cezar et al. 2013), in particular, the actual costs incurred and the savings of outsourcing have to be thoroughly considered (Ang and Straub 1998) which might be one reason why Gordon et al. (2005) noted that information security is rarely outsourced.

Overall, there are only few studies that deal with factors that influence information security investment decisions in general and their interdependencies. These studies view information security investment from a static point of view and do not consider learning strategies and their impact after several iterations. Therefore we propose the following research question:

Research Question 1: Which governing variables at the national, industry and firm level affect security investment strategies in terms of sequences of investment actions?

Effects of Action Strategies on Consequences

Investments in IT security resources, technological or human, have an impact on non-security IT resources, complementary organizational resources, processes and performances. Investments in technological IT security resources, such as biometrical authentication systems, have an impact on non-security IT resources, such as data and hardware, as it prevents unauthorized access to a firm's premises (Boukhonine et al. 2005; Liu and Silverman 2001). As a significant number of security incidents are caused by human, not by technical failures or intruders (Beautement et al. 2009), the impact of investments in human IT resources must not be neglected: Human IT security resources, such as workshops or training on information security, influence non-security resources through an increased security awareness of employees (Corriss 2010; Stephanou 2009).

Moreover, investing in IT security resources can affect security processes, for example, with the investment in a biometric authentication system, a process is installed which safeguards the confidentiality, integrity and availability (Khansa and Liginlal 2009).

A "good" security process (Weishäupl et al. 2015) must be reexamined continually (Kanungo 2006) and it can be regarded as a cycle that implements regular checks of the security levels with respect to the firm's guidelines and policies (Steinklauber 2003), i.e., a "good" security process needs to be adapted according to changing circumstances over time. The soundness of this adaption depends on the learning policy the firm chooses: single or double loop learning. From the indications of Steinklauber (2003), we can conclude that security processes should be evaluated through double loop learning but he does not give any concrete recommendations for implementation which leads us to the following research questions:

Research Question 2a: How does the investments in IT security resources influence non-security resources and security processes over time with changing environmental factors?

Research Question 2b: Depending on the learning technique, how does the relationship between action strategies and consequences evolve over time?

Effects of the Security Processes on the Business Processes

According to Jakoubi, Neubauer, et al. (2009, p. 26), the "*uninterrupted, efficient and effective running of business processes is one of the central components for successful business*". With the rising number of security threats, security processes, which guarantee the proper operation of business processes, are to be discussed by organizations. Jakoubi, Neubauer, et al. (2009) regard the security of business processes from a risk-management point of view and propose a roadmap for risk-aware business process management. Jakoubi, Tjoa, 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. Jakoubi, Tjoa, et al. (2009) conclude that the research on securing business processes is still a very young field but has a lot of potential. However, securing business processes through security processes has not been addressed in literature at all.

Overall, we can state that the impacts of security processes on business processes are not sufficiently covered by the literature, which gives rise to the following research question:

Research Question 3: How do security processes influence business processes and how is this influence mediated by the firm's learning strategy (single or double loop learning)?

Effects of Security Processes on Security Process Performance

The efficiency of security processes can be measured with a security process performance, for example the effectiveness of an authentication process can be quantified through the number of true/false or positive/negative authentication attempts (Weishäupl et al. 2015). Such a security process performance could be useful to compare alternative security processes to evaluate information security investments. Apart from the example provided above, we could not find any security process performance measures in the literature.

Since the literature does not discuss any security process performance measures, we formulate the following research question:

Research Question 4: How can the security process performance be measured and how can firms use this measurement for future information security investment decisions?

Effects of Security Process Performances on Business Process Performances

We hypothesize that, since security processes influence business processes, there is also an impact between security process performance and business process performance (Weishäupl et al. 2015). But we did not find any literature that deals with this impact.

Due to the scarcity of literature, we formulate the following research questions:

Research Question 5a: How do security process performances affect business process performances?

Research Question 5b: What and how (single or double loop learning) can firms learn from past process performance to achieve a higher security level?

Effects of IT Business Value on Organizational Performance

The organizational performance, including productivity, market value, competitive advantage and efficiency (Melville et al. 2004), is substantially influenced by security and business process performance. Since security processes protect business processes, the security and business process performance and the organizational performance are directly interrelated in the sense that the better the security process, the higher the organizational performance.

It is not yet analyzed in the literature how the security process performance affects the overall firm performance. Furthermore, it remains unclear how the organizational performance is influenced by the firm's learning strategy (single or double loop learning) over time. Therefore, we propose the following research questions:

Research Question 6a: What impact does security process performance have on the organizational performance?

Research Question 6b: How is this relationship impacted by the firm's learning strategy (single or double loop learning)?

Single Loop Learning

The evaluation of information security investments through single loop learning is the "more routine" way (Easterby-Smith et al. 2000, p. 786). Single loop learning occurs, for instance, when a firm reacts to mistakes by correcting them without questioning current governing variables, such as policies and objectives. In the literature on information security investments, the concept of learning is present: There are studies dealing with single loop learning of attackers: for example, Gupta et al. (2011) state that attackers learn from their past errors and find new ways to exploit vulnerabilities. As attackers learn, firms need to adapt to circumstances. However, single loop learning of organizations which learn from past investment decisions or mistakes has not been covered exhaustively. We identified only a few approaches that focus on this issue: Franqueira et al. (2010) propose a method for investment decision making with a learning cycle that stepwise raises the understanding of the investment alternatives from past actions. The study of Khansa and Liginlal (2009) concludes that learning from past actions through flexible security process innovation investment permits an organization to switch to more cost-effective technologies and achieve better future protection from attackers at lower cost.

Single loop learning from past actions is crucial for a firm and its development to adapt and apply new action strategies which may lead to improved consequences. However, the academic literature does not

provide guidelines on when and how single loop learning should take place and how it may improve the consequences. We thus propose the following research question for future research:

Research Question 7: How should single loop learning from past actions be designed and what is its impact on future security investment decisions after several iterations of learning loops?

Double Loop Learning

According to Easterby-Smith et al. (2000), double loop learning is the more radical way of learning compared to single loop learning because it questions not only the action strategy but also the governing variables. This perspective is rarely addressed in the literature and, if at all, remarked in a few studies indirectly. For instance, Hamdan (2013) mentions double loop learning as part of five major capabilities for future readiness. In the study of Shi and Wen (2012), double loop learning is indirectly addressed in their proposed value based risk assessment framework. J. Wang et al. (2008) propose a Value-at-Risk (VaR) approach which helps to quantify the risk of information security and can determine proper security solutions based on its risk preference and thus gives insights to learn from the past: The authors state that with the proposed VaR approach, the firm can find out whether extreme daily losses are influenced by environmental factors and therefore make strategic investment in information security more effective.

Although double loop learning is framed as the more effective learning technique compared to single loop learning in academic literature, there might be cases in which single loop learning can be preferred. For instance, since governing variables are considered, using double loop learning might be more time consuming than single loop learning. Furthermore, establishing double loop learning might lead to higher costs. Therefore, it is essential that future research's attention is drawn on double loop learning which is why we propose the following research questions:

Research Question 8a: What are the financial and security-related incentives to establish double loop learning instead of single loop learning?

Research Question 8b: How do security-related consequences improve over time when firms continue using double loop learning?

Discussion

Our synthesis of the body of knowledge on information security investments and the identification of research gaps was driven by and organized along a new theoretical model for information security investments (cf. Figure 3). This model is based on the integrative application of the Resource-based View and the Organizational Learning Theory. While it is the combination of both perspectives that allowed us to derive the research questions, each of the questions has one or, in some cases, even two prevalent theories on which it relies and which we recommend as a basis for future research. For example, financial and security-related incentives for double loop learning are largely based on concepts of the Organizational Learning Theory, the measurement of security process performance to drive firms' information security investment decisions is mainly based on the Resource-based View, and the influence of security processes on business processes mediated by a firm's learning strategy requires both the Resource-based View and the Organizational Learning Theory (cf. Table 4).

Answering the identified research questions and addressing related gaps has not only academic relevance but also managerial implications. Table 4 provides examples of how managers would benefit from answering the research questions, hereby the Resource-based View is referred to as RBV and Organizational Learning Theory as OLT respectively.

Table 4: Research Guidelines and Managerial Implications

Research Gap	Recommended Theories in Future Research	Managerial Implications
1. Effects of Governing Variables on security investment strategies	OLT+RBV	Banks need to comply with regulatory constraints, such as Basel III and PCIDSS, which require them to invest in security countermeasures. Understanding the security-related effects of regulatory constraints helps banks to identify and to focus

		on those investments in IT security resources which support compliance with all regulations.
2a. Influence of investment in IT Security Resources on Security Processes and Non-Security Resources over time in a changing environment	OLT+RBV	For instance, a chemistry laboratory needs to protect sensitive research data and knowledge by, for instance, investing into biometric authentication systems which protect non-security resources such as the laboratory's premises. The laboratory should adapt this biometric authentication system to changing environmental factors, such as growing risks of attacks, to be optimally protected from future physical break-ins (e.g. to prevent from robbery or terroristic attack).
2b. Evolution of the relationship between Action Strategies and Consequences	OLT	Consider an automobile manufacturer which applies a biometric authentication system in a security process. If there is a change in one of the governing variables (environment), as, for instance, a law is adopted that requires strict conditions for biometric systems due to privacy issues (e.g., fingerprints are not allowed for further processing), a single loop learning strategy of the firm might lead to financial penalties and reputational harm because the firm could be sued by employees. Adopting a double loop learning strategy would have prevented this because a firm could have changed its authentication system.
3. Influence of Security Processes on Business Processes mediated by firm's learning strategy	OLT+RBV	The introduced biometric authentication system directly influences the business process by preventing unauthorized access to an organization's premises where sensitive data is stored. Thereby the system may assure an uninterrupted business process. The firm's reaction to a considerably high false rejection rate of the biometric authentication system, when pursuing a single loop learning strategy, is to invest into an authentication system which is functionally different from the existing one (e.g., change from fingerprint to iris scanner).
4. Measurement of Security Process Performance to drive firms' information security investment decisions	RBV	The rate of false acceptances in an authentication system can be used to evaluate the accuracy of the system. If the accuracy is rather poor, the firm might consider additional investments in its authentication system.
5a. Effect of Security Process Performance on Business Process Performance	RBV	If the authentication system is set too restrictive, many employees will be mistakenly blocked when trying to get access to the premises of the firm. As a consequence, workflows become interrupted, which directly relates to a decline of the business process performance.
5b. Learning effects from past process performance	OLT+RBV	Consider a healthcare provider whose patient data (e.g., personal information of patients) have been exploited by an attacker. This incident leads to a decrease of patients' trust in the healthcare industry. When adopting a double learning strategy, the healthcare provider considers the decrease of trust by investing in a (more) secure authentication system which provides a better security process performance.
6a. Relationship between Security Process Performance and Organizational Performance	RBV	The authentication system's false rejection of an employee of a research institute due to non-acceptance of his fingerprint denies the employee access to the building hindering him from work and from being productive. The firm's efficiency and progress is impacted negatively in the sense that deadlines may be missed or daily workload may not be achieved.
6b. Influence of a firm's learning	OLT+RBV	When considering the double loop learning strategy, the authentication system has to be interoperable with the current

strategy on this relationship		authentication system of its trading partners so that the trading partners also have access to systems of the focal firm. This may lead to a more secure transaction of sensitive data and a continuous cooperative workflow that leads into a higher overall company revenue.
7. Impact on future security investment decisions after several iterations when using Single Loop Learning	OLT+RBV	Since employees unintendedly cause many security incidents, organizations invest in security trainings. If the security training results in fewer security incidents or break downs, the firm would learn to establish workshops for employees on a regular basis.
8a. Financial and security-related incentives for Double Loop Learning	OLT	Questioning the governing variables, e.g., education of the country's population and firm's employees can help firms to invest more efficiently in security workshops or trainings to prevent security incidents caused by employees' improper behavior.
8b. Improvement of security-related consequences over time when using Double Loop Learning	OLT	When adopting the frequency and content of security workshops to current governing variables, such as education or culture of the employees, unintended security incidents and breaches caused by employees should decrease over time since, for instance, dealing with firewalls is intelligibly presented to employees.

Conclusion

We developed a new theoretical model on information security investments by drawing on two established IS theories: the Resource-based View and the Organizational Learning Theory. Based on this integrative model, we synthesized the information security investment literature adopting a multi-theoretical perspective. It also allowed us to identify research gaps and to derive research questions which would otherwise have remained unidentified. We discussed implications for practice that follow from answering the identified research questions.

However, our analysis is not without limitations: Although we followed a structured and accurate search process to identify articles, we may have missed some relevant paper. Further, we could only conduct a representative citation due to space limitation, even though our search for articles was exhaustive.

In summary, a firm's ability to learn from past actions or mistakes is not covered sufficiently in the academic information security literature. Answering the derived research questions from the integrative model of information security investments might not only guide future research but also has managerial implications which help firms to make information security investment decisions. We therefore hope that our literature review inspires researchers to contribute innovative and rigorous findings to the existing body of knowledge.

Acknowledgement

The research leading to these results was supported by "Regionale Wettbewerbsfähigkeit und Beschäftigung", Bayern, 2007-2013 (EFRE) as part of the SECBIT project (http://www.secbit.de) and by the "Bavarian State of Ministry, Education, Science and the Arts" as part of the FORSEC research association (https://www.bayforsec.de).

References

Anderson, R. 2001. "Why Information Security is Hard - An Economic Perspective," in *Annual Computer Security Applications Conference (ACSAC 2001)*, pp. 358–365.

Anderson, R., Böhme, R., Clayton, R., and Moore, T. 2008. "Security Economics and the Internal Market," *Study commissioned by ENISA*.

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

Ang, S., and Straub, D. W. 1998. "Production and Transaction Economies and IS Outsourcing: A Study of the US Banking Industry," *MIS Quarterly* (22:4), pp. 535–552.

Argote, L. 2011. "Organizational Learning Research: Past, Present and Future," *Management Learning* (42:4), pp. 439–446.

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

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

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

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

Argyris, C., and Schön, D. A. 1978. *Organizational Learning: A Theory of Action Perspective*, Addison-Wesley Reading, MA, pp. 345–348.

Bandyopadhyay, T., Mookerjee, V. S., and Rao, R. C. 2009. "Why IT Managers Don't Go for Cyber-Insurance Products," *Communications of the ACM* (52:11), pp. 68–73.

Barney, J. 1991. "Firm Resources and Sustained Competitive Advantage," *Journal of Management* (17:1), pp. 99–120.

Barney, J. B. 1994. "Bringing Managers Back in: A Resource-Based Analysis of the Role of Managers in Creating and Sustaining Competitive Advantages for Firms," *Does Management Matter*, pp. 1–36.

Barney, J. B. 1997. *Gaining and Sustaining Competitive Advantage*, Addison-Wesley Reading, MA.

Barua, A., Kriebel, C. H., and Mukhopadhyay, T. 1995. "Information Technologies and Business Value: An Analytic and Empirical Investigation," *Information Systems Research* (6:1), pp. 3–23.

Beautement, A., Sasse, M. A., and Wonham, M. 2008. "The Compliance Budget: Managing Security Behaviour in Organisations," in *Proceedings of the 2008 Workshop on New Security Paradigms*, pp. 47–58.

Bitter, C., Elizondo, D. A., and Watson, T. 2010. "Application of Artificial Neural Networks and Related Techniques to Intrusion Detection," in *The 2010 International Joint Conference on Neural Networks (IJCNN)*, pp. 1–8.

Böhme, R., and Nowey, T. 2008. "Economic Security Metrics," in *Dependability Metrics*, pp. 176–187.

Bojanc, R., and Jerman-Blažic, B. 2008a. "Towards a Standard Approach for Quantifying an ICT Security Investment," *Computer Standards & Interfaces* (30:4), pp. 216–222.

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

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

Boukhonine, S., Krotov, V., and Rupert, B. 2005. "Future Security Approaches and Biometrics," *Communications of the Association for Information Systems* (16:1), p. 48.

Buck, K., Das, P., and Hanf, D. 2008. "Applying ROI Analysis to Support SOA Information Security Investment Decisions," in *IEEE Conference on Technologies for Homeland Security*, pp. 359–366.

Cavusoglu, H., Mishra, B., and Raghunathan, S. 2004. "The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers," *International Journal of Electronic Commerce* (9:1), pp. 70–104.

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

Chai, S., Kim, M., and Rao, H. R. 2011. "Firms' Information Security Investment Decisions: Stock Market Evidence of Investors' Behavior," *Decision Support Systems* (50:4), pp. 651–661.

Chandler, A. D. 1977. *The Visible Hand*, Cambridge, MA: Belknap Press.

Chew, E. 2008. *Performance measurement guide for information security*, National Institute of Standards and Technology, Technology Administration, US Department of Commerce.
Coase, R. H. 1937. "The Nature of the Firm," *Economica* (4:16), Blackwell Publishing Ltd, pp. 386–405.
Cohen, F. 2006. *IT Security Governance Guidebook with Security Program Metrics on CD-ROM*, CRC Press.
Connolly, L., and Lang, M. 2013. "Information Systems Security: The Role of Cultural Aspects in Organizational Settings," in *WISP 2012 Proceedings*.
Cooper, H. M. 1988. "Organizing Knowledge Syntheses: A Taxonomy of Literature Reviews," *Knowledge in Society* (1:1), pp. 104–126.
Corriss, L. 2010. "Information Security Governance: Integrating Security into the Organizational Culture," in *Proceedings of the 2010 Workshop on Governance of Technology, Information and Policies*, pp. 35–41.
Culnan, M. J., Foxman, E. R., and Ray, A. W. 2008. "Why IT Executives should help Employees Secure their Home Computers," *MIS Quarterly Executive* (7:1), pp. 49–56.
Culnan, M. J., and Williams, C. C. 2009. "How Ethics Can Enhance Organizational Privacy: Lessons from the ChoicePoint and TJX Data Breaches," *MIS Quarterly*, pp. 673–687.
Daneva, M. 2006. "Applying Real Options Thinking to Information Security in Networked Organizations,", Centre for Telematics and Information Technology, University of Twente.
Davenport, T. 1993. *Process Innovation: Reengineering Work Through Information Technology*, Boston: Harvard Business School Press.
Dehning, B., and Richardson, V. J. 2002. "Returns on Investments in Information Technology: A Research Synthesis," *Journal of Information Systems* (16:1), pp. 7–30.
Demirhan, D. 2005. "Factors Affecting Investment in IT: A Critical Review," *Journal of Information Technology Theory and Application (JITTA)* (6:4), pp. 1–13.
Derrick Huang, C., Hu, Q., and Behara, R. S. 2008. "An Economic Analysis of the Optimal Information Security Investment in the Case of a Risk-averse Firm," *International Journal of Production Economics* (114:2), pp. 793–804.
Devaraj, S., and Kohli, R. 2000. "Information Technology Payoff in the Health-care Industry: A Longitudinal Study," *Journal of Management Information Systems* (16:4), pp. 41–67.
Easterby-Smith, M., Crossan, M., and Nicolini, D. 2000. "Organizational Learning: Debates Past, Present and Future," *Journal of Management Studies* (37:6), pp. 783–796.
Elsenhardt, K. M., and Martin, J. A. 2000. "Dynamic Capabilities: What are they?," *Strategic Management Journal* (21:1), pp. 1105–1121.
eWEEK. 2014. "IT Security Spending to Rise, With Focus on Mobile,", August (available at http://www.eweek.com/small-business/it-security-spending-to-rise-with-focus-on-mobile.html).
Fiol, C. M., and Lyles, M. A. 1985. "Organizational Learning," *Academy of Management Review* (10:4), pp. 803–813.
Franqueira, V. L., Houmb, S., and Daneva, M. 2010. "Using Real Option Thinking to Improve Decision Making in Security Investment," in *On the Move to Meaningful Internet Systems: OTM 2010*, pp. 619–638.
Frost & Sullivan. 2013. "The 2013 (ISC)2 Global Information Security Workforce Study," (available at https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/2013-ISC2-Global-Information-Security-Workforce-Study.pdf).
Gal-Or, E., and Ghose, A. 2005. "The Economic Incentives for Sharing Security Information," *Information Systems Research* (16:2), pp. 186–208.
Gartner. 2011. "Magic Quadrant for Security Information and Event Management,", Gartner RAS Core Research.
Gartner. 2012. "IT Key Metrics Data 2012: IT Enterprise Summary Report,", Gartner RAS Core Research.
Gartner. 2014. "Gartner Says Worldwide Information Security Spending Will Grow Almost 8 Percent in 2014 as Organizations Become More Threat-Aware,", August (available at http://www.gartner.com/newsroom/id/2828722).
Ghose, A., and Rajan, U. 2006. "The Economic Impact of Regulatory Information Disclosure on Information Security Investments, Competition, and Social Welfare.," in *Workshop on the Economics of Information Security 2006 (WEIS)*.
Gordon, L. A., and Loeb, M. P. 2006. "Economic Aspects of Information Security: An Emerging Field of Research," *Information Systems Frontiers* (8:5), pp. 335–337.

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

Gordon, L. A., Loeb, M. P., Lucyshyn, W., and Richardson, R. 2005. *CSI/FBI Computer Crime and Security Survey*, Computer Security Institute.

Grossklags, J., Christin, N., and Chuang, J. 2008a. "Secure or Insure?: A Game-theoretic Analysis of Information Security Games," in *Proceedings of the 17th International Conference on World Wide Web*, pp. 209–218.

Grossklags, J., Christin, N., and Chuang, J. 2008b. "Security and Insurance Management in Networks with Heterogeneous Agents," in *Proceedings of the 9th ACM Conference on Electronic Commerce*, pp. 160–169.

Gupta, M., Chaturvedi, A., and Mehta, S. 2011. "Economic Analysis of Tradeoffs between Security and Disaster Recovery," *Communications of the Association for Information Systems* (28:1), pp. 1–17.

Hagen, J. M., Albrechtsen, E., and Hovden, J. 2008. "Implementation and Effectiveness of Organizational Information Security Measures," *Information Management & Computer Security* (16:4), pp. 377–397.

Hamdan, B. J. 2013. "Evaluating the Performance of Information Security: A Balanced Scorecard Approach," in *SAIS 2013 Proceedings*.

Hoo, K. J. S. 2000. *How much is enough? A Risk Management Approach to Computer Security*, Stanford University.

Huang, C. D., and Goo, J. 2009. "Investment Decision on Information System Security: A Scenario Approach," in *AMCIS 2009 Proceedings*.

Jakoubi, S., Neubauer, T., and Tjoa, S. 2009. "A Roadmap to Risk-aware Business Process Management," in *Services Computing Conference*, pp. 23–27.

Jakoubi, S., Tjoa, S., Goluch, G., and Quirchmayr, G. 2009. "A Survey of Scientific Approaches Considering the Integration of Security and Risk Aspects into Business Process Management," in *20th International Workshop on Database and Expert Systems Application (DEXA'09)*, pp. 127–132.

Jasperson, J. S., Carte, T. A., Saunders, C. S., Butler, B. S., Croes, H. J., and Zheng, W. 2002. "Review: Power and Information Technology Research: A Metatriangulation Review," *MIS Quarterly* (26:4), pp. 397–459.

Jiang, L., Anantharam, V., and Walrand, J. 2008. "Efficiency of Selfish Investments in Network Security," in *Proceedings of the 3rd International Workshop on Economics of Networked Systems*, pp. 31–36.

Kanungo, S. 2006. "Portfolio Approach to Information Technology Security Resource Allocation Decisions," in *PACIS 2006 Proceedings*.

Khansa, L., and Liginlal, D. 2009. "Valuing the Flexibility of Investing in Security Process Innovations," *European Journal of Operational Research* (192:1), pp. 216–235.

Kraaijenbrink, J., Spender, J.-C., and Groen, A. J. 2010. "The Resource-Based View: A Review and Assessment of its Critiques," *Journal of Management* (36:1), pp. 349–372.

Kwon, J., and 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., and 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.

Lacity, M. C., Khan, S., Yan, A., and Willcocks, L. P. 2010. "A Review of the IT Outsourcing Empirical Literature and Future Research Directions," *Journal of Information Technology* (25:4), pp. 395–433.

Landwehr, C. E. 2004. "Improving Information Flow in the Information Security Market," in *Workshop on the Economics of Information Security*, pp. 155–163.

Levy, Y., and Ellis, T. J. 2006. "A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research," *Informing Science: International Journal of an Emerging Transdiscipline* (9:1), pp. 181–212.

Liu, S., and Silverman, M. 2001. "A Practical Guide to Biometric Security Technology," *IT Professional* (3:1), pp. 27–32.

Locher, C. 2005. "Methodologies for Evaluating Information Security Investments - What Basel II can change in the Financial Industry," *ECIS 2005 Proceedings*.

McAfee. 2014. "Net Losses: Estimating the Global Cost of Cybercrime,", June (available at http://www.mcafee.com/uk/resources/reports/rp-economic-impact-cybercrime2.pdf).

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

Neubauer, T., and Heurix, J. 2008. "Defining Secure Business Processes with Respect to Multiple Objectives," in *3rd International Conference on Availability, Reliability and Security (ARES 2008)*, pp. 187–194.

OECD. 2004. "The Security Economy,", Organisation for Economic Co-operation and Development.

Paré, G., Trudel, M.-C., Jaana, M., and Kitsiou, S. 2015. "Synthesizing Information Systems Knowledge: A Typology of Literature Reviews," *Information & Management* (52:2), pp. 183–199.

Penrose, E. T. 1959. *The Theory of the Growth of the Firm*, New York: John Wiley & Sons.

Romme, G., and Dillen, R. 1997. "Mapping the Landscape of Organizational Learning," *European Management Journal* (15:1), pp. 68–78.

Rowe, B. R. 2007. "Will Outsourcing IT Security Lead to a Higher Social Level of Security?," in *Workshop on the Economics of Information Security 2007 (WEIS)*.

Schryen, G. 2015. "Writing Qualitative IS Literature Reviews–Guidelines for Synthesis, Interpretation and Guidance of Research," *Communications of the Association for Information Systems* (37:12).

Schwandt, D., and Marquardt, M. J. 1999. *Organizational learning*, CRC Press.

Shen, D., and Jones, B. L. 2005. "A New Implication for China's Rural Education Reform: Organizational Learning Theory," *Journal of International Agricultural and Extension Education* (12:1), pp. 27–36.

Shi, Y., and Wen, Q. 2012. "A Value Based Security Risk Assessment Method," in *2012 Fourth International Conference on Multimedia Information Networking and Security (MINES)*, pp. 49–51.

Siponen, M., Mahmood, M. A., and Pahnila, S. 2014. "Employees' Adherence to Information Security Policies: An Exploratory Field Study," *Information & Management* (51:2), pp. 217–224.

Smith, K. A., Vasudevan, S. P., and Tanniru, M. R. 1996. "Organizational Learning and Resource-Based Theory: An Integrative Model," *Journal of Organizational Change Management* (9:6), pp. 41–53.

Steinklauber, K. 2003. "Security Process for the Implementation of a Company's Extranet Network Connections,", SANS Institute.

Stephanou, A. 2009. "The Impact of Information Security Awareness Training on Information Security Behaviour,".

Stigler, G. J. 1961. "The Economics of Information," *The Journal of Political Economy* (69:3), pp. 213–225.

Sun, W., Kong, X., He, D., and You, X. 2008. "Information Security Problem Research Based on Game Theory," in *International Symposium on Electronic Commerce and Security*, pp. 554–557.

The Guardian. 2010. "WikiLeaks supporters disrupt Visa and MasterCard sites in 'Operation Payback,", December (available at http://www.theguardian.com/world/2010/dec/08/wikileaks-visa-mastercard-operation-payback).

The Washington Post. 2014. "The Sony Pictures hack, explained,", December (available at http://www.washingtonpost.com/blogs/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/).

Thomson Reuters. 2015. "Obama seeks $14 billion to boost U.S. cybersecurity defenses," (available at http://www.reuters.com/article/2015/02/02/us-usa-budget-cybersecurity-idUSKBN0L61WQ20150202).

Torrellas, G. A. S., and Vargas, L. A. V. 2003. "Modelling a Flexible Network Security Systems Using Multi-agents Systems: Security Assessment Considerations," in *Proceedings of the 1st International Symposium on Information and Communication Technologies*, pp. 365–371.

vom Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R., and Cleven, A. 2009. "Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process.," in *ECIS 2009 Proceedings*.

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

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

Wang, X., Zhang, Y., and Shi, H. 2008. "Access Control for Human Tasks in Service Oriented Architecture," in *International Conference on e-Business Engineering (ICEBE)*, pp. 455–460.

Wattel, B. 2002. "Business Process Security," in *Integrity, Internal Control and Security in Information Systems*, pp. 177–186.

Webster, J., and Watson, R. T. 2002. "Analyzing the Past to Prepare for the Future: Writing a Literature Review," *MIS Quarterly* (26:2), p. 3.

Weishäupl, E., Yasasin, E., and Schryen, G. 2015. "IT Security Investments through the Lens of the Resource-based View: A new theoretical Model and Literature Review," in *ECIS 2015 Completed Research Papers*.

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

Whitman, M. E. 2003. "Enemy at the Gate: Threats to Information Security," *Communications of the ACM* (46:8), pp. 91–95.