IT SECURITY INVESTMENTS THROUGH THE LENS OF THE RESOURCE-BASED VIEW: A NEW THEORETICAL MODEL AND LITERATURE REVIEW

Complete Research

Weishäupl, Eva, University of Regensburg, Regensburg, Germany, eva.weishaeupl@wiwi.uni-regensburg.de

Yasasin, Emrah, University of Regensburg, Regensburg, Germany, emrah.yasasin@wiwi.uni-regensburg.de

Schryen, Guido, University of Regensburg, Regensburg, Germany, guido.schryen@wiwi.uni-regensburg.de

Abstract

IT security has become a major issue for organizations as they need to protect their assets, including IT resources, intellectual property and business processes, against security attacks. Disruptions of IT-based business activities can easily lead to economic damage, such as loss of productivity, revenue and reputation.

Organizations need to decide (1) which assets need which level of protection, (2) which technical, managerial and organizational security countermeasures lead to this protection and (3) how much should be spent on which countermeasure in the presence of budget constraints. Answering these questions requires both making IT security investment decisions and evaluating the effectiveness and efficiency of these decisions.

The literature has contributed to this field adopting approaches from micro-economics, finance and management, among others. However, the literature is rather fragmented and lacks a shared theoretical basis. As a consequence, it remains partly open what we can learn from past research and how we can direct and stimulate still missing research activities.

In order to address these deficiencies, we draw on the resource-based view (RBV) and provide a theoretical model for IT security investments. We use this RBV model to review the IT security investment literature and to identify research gaps.

Keywords: IT Security, Investment, Resource-Based View, Literature Review.

1 Introduction

The use of information technology (IT) is increasing steadily (Anderson, 2008; Anderson and Moore, 2006) so IT security has become a major issue for organizations aiming to protect their systems, data, hardware, intellectual property, and business processes against attacks, misuse or technical failures (Anderson, 2001; Frost & Sullivan, 2011; Gartner, 2011, 2012; Whitman, 2003). Organizations rely on stable IT to perform their business activities (Jakoubi et al., 2009) and disruptions through cyber attacks, for example, can easily lead to economic damages and strategic disadvantages like losses of productivity, revenue and reputation (Bandyopadhyay et al., 2009). According to McAfee (2014) "cybercrime is a growth industry" and most companies underestimate the risk they are opposed to. Challenging questions for these 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, security

policies) lead to this protection and how much should be spent on which countermeasure in the presence of budget constraints (Anderson and Schneier, 2005; Gordon and Loeb, 2007). The examples of security countermeasures demonstrate that not only technical but also managerial and organizational questions need to be addressed.

Answering these questions requires IT security investment decisions. Beyond this "ex ante" perspective, the "ex post" perspective must not be neglected (Cezar et al., 2013): Firms need to review their decisions and decision processes to evaluate their effectiveness and to prevent repetition of decision (process) errors (Böhme and Moore, 2013). Thus, companies need to conduct ex post evaluation to optimize future (ex ante) decisions. Unfortunately, the evaluation of IT security investment has proved problematical because, in contrast to investments in other areas, security investment has no obvious return but prevented economic losses and opportunity costs (Böhme and Nowey, 2008).

The academic literature provides many articles for both perspectives on IT security investments and we found more than 200 research papers. Key research streams are based on micro-economics, finance and management. Examples of micro-economic works are approaches based on game theory (e.g., Grossklags et al., 2008a; Sun et al., 2008). Financial analyzes are mainly based on return on investment, net present value and internal rate of return (Bojanc and Jerman-Blažič, 2008b; Buck et al., 2008). Management approaches are widely based on decision theory (e.g., Huang and Goo, 2009), risk management (e.g., Bojanc and Jerman-Blažič, 2008a; Hoo, 2000) and organization theory (e.g., Cohen, 2006; Hagen et al., 2008).

However, the literature is rather fragmented, lacks a theoretical basis and is incoherent based on the adoption of the above described concepts from different disciplines. As a consequence, it remains partly open what we can learn from past research and how we can direct and stimulate still missing research activities. In order to address these deficiencies, we provide two contributions: (1) We draw on the resource-based view (RBV) (Wernerfelt, 1984, Melville et al., 2004), an established theory in IS literature (Wade and Hulland, 2004), to provide a theoretical basis for IT security investments. We thereby adopt a new theory-based perspective, which is a contribution of literature reviews (Boote and Beile, 2005; Hart, 1998). The RBV is appropriate because (a) assets (IT systems, data, processes, etc.) which need protection can be straightforward modeled as resources, and (b) both tangible and intangible resources, such as firewalls, and security knowledge and data, respectively, can be covered. IT security resources can be seen as assets with no obvious return but prevented loss. In our case, an investment into IT security resources does not result in higher profits but has positive impact on the organizational performance as loss has been prevented. To our best knowledge, no comprehensive theoretical model of IT security investments has been suggested in the literature. (2) We use the RBV model on IT security investments to provide a structured concept-centric synthesis of the IT security investment literature and to reveal research gaps.

The remainder of this paper unfolds as follows: Section 2 frames the RBV model as it is understood in this work and Section 3 explains the methodology to find relevant academic literature. Subsequently in Section 4, we synthesize key research findings and identify research gaps. We conclude by outlining the contributions and limitations of this work.

2 A Resource-based View on IT Security Investment

In Section 2.1 we introduce the RBV before we derive our model in Section 2.2.

2.1 Theoretical foundations: The Resource-Based View

Although the influential role of the RBV model in the field of strategic management (Barney et al., 2001) came up with Wernerfelt's article "A Resource-Based View of the Firm", the origins can be traced back to earlier research: the key factors that led to Wernerfelt's article can be found in works by Coase (1937), Penrose (1959), Stigler (1961), Chandler (1977) and Williamson (1975). In Penrose (1959), for example, a firm is a "collection of productive resources" which includes physical and human resources

as the main productive resources. The RBV was established as one of the preeminent approaches to the analysis of enduring competitive advantage by Wernerfelt. His fundamental work was followed by Rumelt (1984), Barney (1986) and Mata et al. (1995). When RBV is applied to analyze the effect of information technology, IT is considered an organizational resource that can enhance a firm's capabilities and eventually lead to higher performance (Liang and You, 2009; Liang et al., 2010). Considering the literature on RBV for IT investments, there are various approaches, for instance, the concept of IT as an organizational capability, which is associated with IT capability and firm performance, was examined by Bharadwaj (2000). Vinekar and Teng (2012) also tested empirically how RBV postulates on IT business value and reasoned that IT is not an occasional and imitable resource that enables business value but must be regarded in combination with additional resources that give IT value. Mata et al. (1995) develop a model founded on the RBV of a firm and state that some firms may gain competitive advantages over other firms through their IT investment. A more theoretical approach is made by Nevo and Wade (2010) who synthesize systems theory with the RBV to argue that the business value of IT assets is linked with the aspiring capabilities exhibited by IT-enabled resources produced as a result of interactions between IT assets and organizational resources. A seminal study was conducted by Melville et al. (2004): the authors developed a model of IT business value based on the RBV of the firm that incorporates the various aspects of research into a single framework.

IT security investments can be regarded as a subset of (general) IT investments. The obvious reason for this is the fact that a firm usually would invest in security related IT assets and / or in human development (e.g., security awareness employee training). In Penrose's view both of these investments are made in physical and human resources which are the main productive resources of a firm (Penrose, 1959). In other words, we can state that if a firm invests in IT security, it invests in one of its core resources and thus the RBV lens can be applied. With the use of RBV, one can therefore identify the affected resources and protect them by investing into security measures. There is a strong link between IT security investments and RBV but it has not yet been made explicit in the literature. We could only identify two approaches that remotely relate RBV to IT security investments: Cavusoglu et al. (2002) briefly explain the RBV to underpin their hypotheses related to firm size and security breach without going into details about the RBV and its link to security investment. In the work of Demirhan (2005) core elements of the RBV can be found, however she does not name and link these factors to RBV. We conclude that a resource-based view of IT security investment is useful for two reasons: first, it provides a macro framework which allows us to integrate heretofore unconnected research streams; second, it is compatible with the original RBV because only minor modifications are necessary to adapt it to the context of IT security investment. In our work, we will therefore structure the IT security investment literature through the RBV. In particular, we draw on the model provided by Melville et al. (2004) because it operationalizes and covers major aspects of influences which need to be considered in investment decisions: among others the three environments (see Figure 1).

2.2 A RBV model for IT Security Investments

We adapt the RBV to the context of IT security investment by developing a modified RBV model (see Figure 1) and defining its constructs (see Table 1). The concept of a firm resource includes "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" (Barney, 1991). In conformance with the original RBV model, relationships, symbolized with arrows (e.g., between a resource and a business process) are defined as "may improve" (cf. Melville et al. (2004)). Consistent with our focus, we exclusively consider relationships between constructs which are related to security. For example, we do not conceptualize a relationship between human non-security IT resources and technological non-security IT resources. We adapt the "IT Business Value Model" (Melville et al., 2004) which contains three environments (1) the macro environment which comprises country specific factors, (2) the competitive environment which is separated into industry characteristics and trading

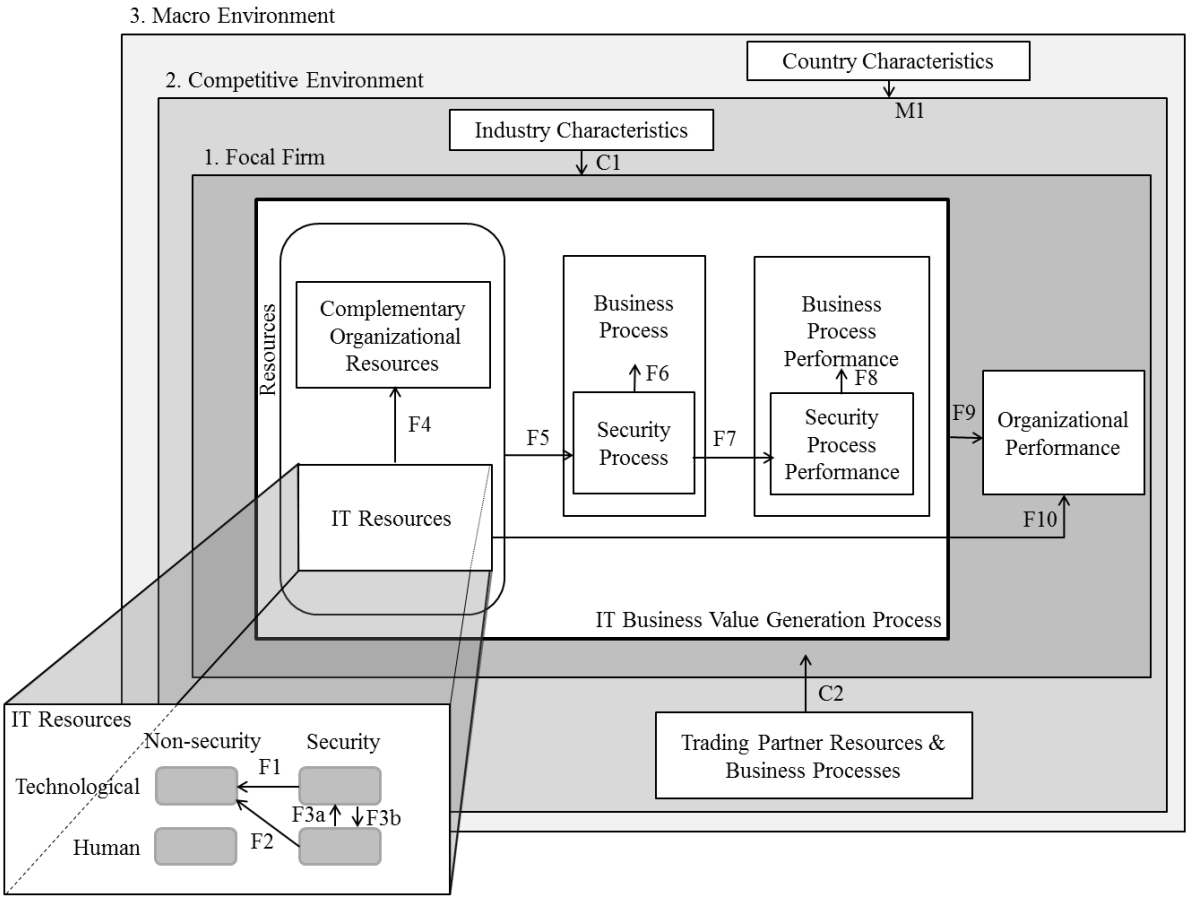

Figure 1. The Resource-Based View on IT security investment based on Melville et al. (2004).

partners, and (3) the focal firm which acquires and deploys the IT security resources (Melville et al., 2004). The focal firm comprises the IT resources, complementary organizational resources, processes, process performances and organizational performance.

In the context of IT security investment we modify the model of Melville et al. (2004) as follows: First, we added the security and non-security dimension within the IT resources and the corresponding relationships F1, F2, F3a and F3b in Figure 1. This allows us to account for security resources which are central constructs in the security literature (e.g., Gordon and Loeb, 2002b; Kanungo, 2006). In addition to the security/non-security dimension, we distinguish technological and human IT resources just as it was done by Melville et al. (2004). Technological IT security resources (e.g., firewalls or intrusion detection systems) affect technological non-security IT resources as data or systems (relationship F1). Furthermore human IT security resources, for instance Chief Information Security Officers (CISOs) or workshops on security awareness, influence technological non-security resources (relationship F2). Human IT security resources protect technological security resources, for example workshops on usage of IDSs and correct behavior in the case of breakdowns or attacks (relationship F3a). An example for path F3b is a Data Loss Prevention (DLP) system which controls outgoing file transfer and warns employees and thereby contributes to security awareness, i.e. the relationship between technical and human IT security resources. Second, we added an arrow from IT resources to complementary organizational resources (relationship F4) because IT security resources - technological or human - aim to protect complementary organizational resources. An example is the prevention of unauthorized access to buildings or files through passwords, PINs, card keys or fingerprints (Liu and Silverman, 2001). Third, we added an arrow from IT resources to organizational performance (relationship F10) because according to Dehning and Richardson (2002) there

is a "direct link between IT and overall firm performance, bypassing the effect of IT on business processes" (Dehning and Richardson, 2002). Fourth, we added security processes which affect business processes (relationship F6) since the unimpeded execution of business process is crucial for a company's success and business processes are permanently exposed to threats (Neubauer and Heurix, 2008; Wang et al., 2008). Therefore the connection between business processes and security should not be neglected. According to Wattel (2002) "the process of security is destined to fail if it does not protect the process of business". Therefore we added security processes, which protect the business processes, as a subtype of business processes to the model of Melville et al. (2004). An example for a security process could be the biometric authentication system which directly influences the business process in the sense that, if the authentication system breaks down, workflows are disrupted. Fifth, we added the security process performance which affects the business process performance (relationship F8) because a natural consequence of the relation business process - security process is the connection between business process performance and security process performance. An example for a security process performance could be metrics for the effectivity of authentication systems, for example the number of true/false or positive/negative authentication attempts.

Construct	**Description**
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 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 CIA of a firm's operations (Khansa and Liginlal, 2009b)
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 Enrol (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)

Table 1. Model Constructs.

3 Research Methodology

Our literature review can be classified as follows: Based on Rowe (2014), the scope is IT security investment and we focus (Cooper, 1988) on research outcomes. We conducted an exhaustive search with selective citation (due to lack of space) as suggested by Cooper (1988) and implemented by Dahlberg et al. (2008) for example. The technique (King and He, 2005) is narrative. In addition the organization (Cooper, 1988) is conceptual (because of the RBV perspective) and the goal is a synthesis and the identification of research gaps. In order to provide a systematic review, we followed the steps suggested by Bandara et al. (2011):

1. Identification of Articles (Phase 1): Following the recommendations of Webster and Watson (2002) we covered databases including ACM Digital Library, IEEE Xplore Digital Library, Ebsco Host Business Source Premier and AIS Electronic Library. Without limitating the period of time we scanned the databases for keywords[1] which result from the model and its boundaries. We complemented our search by scanning the Workshop on the Economics of Information Security (WEIS), Google Scholar and Science Direct. To identify all relevant papers, we conducted a backward search. We excluded papers that could not be classified according to our model (Section 2.2) for instance the paper Baker et al. (2007), Bitter et al. (2010) or Mercuri (2003). Furthermore we excluded papers that deal with economics of IT security in general and do not address specific constructs (e.g., Anderson, 2001, 2008; Anderson and Moore, 2006; Camp and Wolfram, 2000; Chew, 2008). To evaluate the fit of the works, we studied the abstracts.
2. Preparing for Analysis (Phase 2): We used the RBV (Section 2.2) to synthesize the literature conceptually.
3. Coding (Phase 3): All papers were analyzed and classified into the paths shown in Figure 1.

Further we identify research gaps as suggested by Webster and Watson (2002). Based on these gaps, we formulate research questions in order to stimulate further research.

4 Synthesis and Identification of Research Gaps

In this section we synthesize literature findings on IT security investments. Our presentation is structured along the relationships in the suggested RBV model (cf. Figure 1) and thus concept-centric as suggested by Webster and Watson (2002). Based on the synthesis we identify research gaps for each of the relationships.

4.1 Effects of Country Characteristics (M1)

Macro environmental factors, such as culture or law affect the company's possibilities and choices in the domain of information technology in many ways, especially with regard to investment. The development of the country influences the need to invest in security. For instance, culture and education of the workers determine the need for investment in security workshops. In addition, regulations such as tax subsidies and financial safeguards promote efficiency and competitive advantage (Melville et al., 2004). In the IT security domain firms need to conform to certain country-specific regulations which force them to spend

[1] (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.

on safeguards to ensure the confidentiality, integrity and availability of critical information; otherwise the firm will be facing monetary penalties and loss of customer base and goodwill (Khansa and Liginlal, 2009a). The level of security investment depends on how government authorities regulate. For example, if the law is more favorable to a bank when fraudulent transactions are disputed, the bank has less incentive to invest in security (Chun, 2011). Firms belonging to different business sectors have different regulatory frameworks, for instance, the New Capital Accord (Basel II) or the Gramm-Leach-Bliley Act (GLBA) apply to financial firms, the SOX (Sarbanes-Oxley) to accounting firms and the HIPAA (Khansa and Liginlal, 2009b) to healthcare firms.

However, few studies have investigated strategic investment decisions in security with respect to the legislation of countries. According to Weber et al. (2009) the goal of IT governance is to ensure that IT is a valued and embedded element of business and is not constraining a company's strategy. Yet, many works found negative effects of regulations, for example, Ghose and Rajan (2006) discuss how three US laws (SOX, Gramm-Leach-Bliley and HIPAA) exert pressure on firms: The SOX forces organizations to invest in IT security, so companies have to undertake a series of dramatic changes in the way they appropriate resources to IT security (Ghose and Rajan, 2006). This directly affects the overall firm performance by decreasing market competition or social welfare, particularly for small sized firms. However, the SOX contributes to increasing awareness about the necessity and the importance of IT security and draws attention to IT security investment announcements (Chai et al., 2011). Kwon and Johnson (2014) focus on regulations to protect the privacy of personal health information (HIPAA) and conclude that external pressure decreases the effect of proactive investments on security performance.

Furthermore, standards like ISO/IEC 27002: 2013 and best practice models such as ITIL and COBIT influence investment decisions: According to Lee (2010) COBIT helps firms to manage the risks associated with IT in general and to evaluate IT investments in particular (Fedorowicz and Gelinas, 1999). In summary, federal government needs to enforce changes in regulation. In other areas, like for mobile security breaches, there exist no governing rules so far (Chun, 2013). Anderson et al. (2008) provide fifteen key policy proposals which could be a sound basis for future action. According to Siponen (2006) IT security management standards focus on the existence of security processes but not their content and quality. This may provide a false sense of security. Siponen (2006) also gives advice for future research: case studies on how IT security management standards are met in organizations would be helpful to firms. For future academic research we therefore suggest the following question:

Research Question 1 ***(a)*** *How do culture and education influence investments in IT security?* ***(b)*** *How do laws and regulations impact security investment decisions?*

4.2 Effects of Industry Characteristics (C1)

According to Melville et al. (2004) industry characteristics shape the extent to which a firm can acquire and operate IT successfully. Empirical studies of IT business value typically include variables to control for industry effects, whether an industry dummy variable (Lichtenberg, 1995) or measures of industry structure such as competitiveness and regulation (Bharadwaj, 2000; Melville et al., 2004). Applying this in the context of IT security, an important task is embedding of IT security resources into business operations and the business sphere of a company. In other words, a firm should strive to invest in IT security resources that are 1) applicable in their IT and 2) generate value for the company. Thus, an organization must additionally increase the value-added balance for both the investment into IT security resources and their adoption into their infrastructure.

Regarding the literature on IT security investments with a specific focus to this area, research is almost absent. We could only identify two approaches that are remotely related to this topic. Hua and Bapna (2009) analyze risk in IT based information systems, predict the behavior of cyber terrorists, and find an optimal investment to ensure an optimum of business value for the focal firm. A comparable study is conducted by Liu and Bandyopadhyay (2010) who analyze the IT security investment decisions of two firms which find themselves in such a short list of hacking targets and must compete dynamically on their

IT security investments to reduce the risk of being breached. Whereas Hua and Bapna (2009) focus on a single firm, the approach of Liu and Bandyopadhyay (2010) is designed to discover the impact of security investment efficiency on security of two comparable firms. However, the following research question is not answered in detail yet:

Research Question 2 *Should a firm invest in IT security to achieve a competitive advantage compared to other firms in the industry sector and if so how much and in what security resource should be invested?*

4.3 Effects of Trading Partner Resources and Business Processes (C2)

This path covers the relationships between the focal firm and its trading partners, in particular with regard to information outsourcing and sharing. Naturally trust plays an important role when it comes to these inter-firm relationships and alliances.

First we attend to information outsourcing: Because of the growing complexity of IT security management (e.g., rising cost of security breaches; increasing scale, scope and sophistication of security attacks and regulatory obligations) many firms outsource IT security operations to Managed Security Service Providers (MSSPs), which offer prevention and detection services (Cezar et al., 2013). However, outsourcing holds challenges and risks for both user organizations and MSSPs, especially estimating the "true" costs and savings of outsourcing (Ang and Straub, 1998). That could be the reason why the survey of Gordon et al. (2005) discovered that IT security is rarely outsourced. The cost and benefits of outsourcing have been discussed extensively (Rowe, 2007) but relatively few studies have focused on the economic aspects of outsourcing IT security: in a recent study Gupta and Zhdanov (2012) discuss the network effects associated with outsourcing and analyze how MSSPs may develop. Ding et al. (2005) have conducted research on the decision of firms to outsource, specifically addressing the costs and benefits to MSSPs and firms. Thus the questions arise:

Research Question 3 ***(a)*** *Does security increase when a firm chooses different MSSPs for prevention and detection and if so, what might be the payoff?* ***(b)*** *What form of IT security outsourcing relationship (how intrusive) provides the highest cost-benefit ratio?*

Next we attend to information sharing: Many papers have investigated the costs and benefits of sharing data on cyber security breaches, threats and potential solutions (e.g., Anderson et al., 2008; Rowe, 2007) with information-sharing alliances (ISAs). There are incentives for not sharing data, like loss of reputation and trust, signal of weakness to adversaries and negative effects on the financial markets (Gal-Or and Ghose, 2005). Another problem concerning information sharing is related to trust: firms might free-ride off the security expenditures of other firms by only consuming shared security information but never providing any (Gordon et al., 2003). Also the ISA could report the incident of the breach-revealing firm to the public which would harm the reputation of the sharing company (Gal-Or and Ghose, 2005). The positive aspects of information sharing are that it is expected to lead to decreased spending and increased levels of security by minimizing the risk of security breaches (Gal-Or and Ghose, 2005; Gordon et al., 2003). Information sharing can also encourage additional investment in security (Gal-Or and Ghose, 2005) because firms learn from the mistakes of other firms. In particular, interorganizational information systems (IOSs) like electronic data interchange (EDI), collaborative design systems and extranets need to be considered as well (Melville et al., 2004): Banerjee and Golhar (1994) found out that users are not satisfied with security in EDIs and that this problem needs to be addressed. However, according to Gordon et al. (2003) other economic incentives to facilitate effective information sharing need to be created, for example government regulation. But the design and analysis of such incentive mechanisms awaits further research (Gordon et al., 2003) which leads us to:

Research Question 4 *What are the financial incentives to share information on security breaches and threats?*

4.4 Effects of technological IT security resources on technological non-security IT resources (F1)

The effect of technological IT security resources on technological non-security IT resources is analyzed in path F1 which is covered up by many approaches in literature for which we will give some examples. For instance, several studies (Grossklags et al., 2008b; Jiang et al., 2008; Torrellas and Vargas, 2003) focus on investments in network security in order to protect non-security IT resources. Jiang et al. (2008) study the equilibrium performance of the network security whereas Grossklags et al. (2008b) contribute to a network-side protection pool or invest in a private good to limit losses. The investigation of Torrellas and Vargas (2003) presents a distributed planning and control architecture for autonomous security assessment systems using a multi-agent paradigm. Apart from these aspects of investing in network security, there are other research streams as well. As an example, Levitin et al. (2012) consider a defender which seeks to store information securely by a multiple objective optimization model. This minimizes the probabilities of information destruction, data theft and cost. Rosenfeld et al. (2007) state that "all companies who use computer systems intensively must protect the security properties of their assets against malicious actions" and to achieve this "they must employ various countermeasures to mitigate the risk of attacks". In their approach, the authors focus on the usage of archetypes in computer security to aid understanding and diagnosis, and making decisions for risk mitigation. The study of investments in technological IT security resources is thoroughly and well-examined but specially designed. The current research provides an informative analysis on the complexities and problems surrounding of this topic. However, we could not identify a study which examines the impact of technological IT security resources on technological non-security IT resources in general. We thus propose the following research questions for future research:
Research Question 5 *How should a firm allocate its security budget to the different technological security resources to gain the highest return?*

4.5 Effects of human IT security resources on technological non-security IT resources (F2)

This section analyzes articles that deal with the effects that human IT security resources like workshops and training on IT security have on non-security IT resources such as data. A significant number of security incidents are caused by human, not by technical failures or intruders. Many security breaches result from employees' failure to comply with security policies (Beautement et al., 2009). According to Corriss (2010) awareness and compliance can be achieved through training, incentives, and commitment of employees. There are studies, like Stephanou (2009) which examine the impact of IT security awareness training on users' IT security behavior but do not consider cost factors. Blundell et al. (1999) regarded the returns from education and training to the individual, the firm and the economy but did not specialize in security. The crucial question is what percentage of the security budget should be allocated for workshops and training. When answering this question the company needs to consider that most security awareness trainings can be delivered at a relatively low cost but the time that employees spend away from productive work in order to take the training will cause financial loss as well (Richardson and Director, 2008). Another aspect is that these trainings need to be repeated at least annually due to staff turnover and fatigue (Böhme and Moore, 2013). So an important research question is:
Research Question 6 *What is the return on investment in workshops and trainings that aim at increasing the security of technological non-security IT resources?*

4.6 Effects of human IT security resources on technological IT security resources and vice versa (F3a/b)

We first attend to path F3a: Once a security measure is implemented the company needs to monitor their effectivity on a regular basis (Richardson and Director, 2008). Therefore many enterprises employ a Chief

Information Security Officer (CISO), who is confronted with two key questions (Bodin et al., 2005): how to allocate the IT security budget most effectively, and how to justify the budget (or possible increases) to the chief financial officer (CFO). CISOs have to make a couple of challenging decisions (Beresnevichiene et al., 2010) for which the literature provides guidelines: Bodin et al. (2005) uses the Analytic Hierarchy Process (AHP) to provide a mechanism to carefully compare criteria and alternatives. Bodin et al. (2008) build on this AHP analysis to assist a CISO in ranking proposals for enhancing a security system by developing a new metric, the Perceived Composite Risk. A systematic methodology to support multi-criteria security investment decision-making based on mathematical systems modeling was developed by Beresnevichiene et al. (2010). Although a corresponding case study showed that this methodology is feasible for CISOs, both theoretical work on the model (e.g., handling imprecisions) and further case studies (e.g., involving outside stakeholder) need to be conducted in the future (Beresnevichiene et al., 2010). Moreover, the benefits of workshops and trainings for employees on how to use IT security resources need to be taken into account. As already explained in Section 4.5 a lot of cost factors need to be considered but we found no paper that deals with this problem from a financial point of view. Therefore we formulate the research question:

Research Question 7 *What is the return on investment in workshops and trainings that aim at increasing the security of technological IT security resources?*

Next we attend to path F3b: Technical Data Loss Prevention systems filter the outgoing traffic for text sequences that might be credit card numbers, automatically block those massages and inform the user about the incident (Böhme and Moore, 2013). Thereby the user's security awareness is trained. As organizations primarily invest in such systems to protect their technical resources (path F1 in Figure 1) and not to train employees' security awareness, we list path F3b for the sake of completeness. This part therefore does not result in a research question.

4.7 Effects of IT resources on complementary organizational resources (F4)

Path F4 refers to the effect of IT security resources on complementary organizational resources. The most important example is the authentication and access control to physical resources (e.g., buildings). According to Liu and Silverman (2001) the security field uses three types of authentication: something you know (e.g., password, PIN, or piece of personal information, such as your mother's maiden name); something you have (a card key, smart card, or token and something you are (a biometric)). The third type, the biometric is the most secure and convenient authentication mechanism because it can not be borrowed, stolen, or forgotten and forging one is nearly impossible (Liu and Silverman, 2001). However, according to Babich et al. (2012) one of the greatest disadvantages of biometrics - besides privacy issues - is the cost of implementation. But on the other hand the problems and costs associated with lost, reissued or temporarily issued tokens/cards/passwords can be prevented and time can be saved (Matyáš and Říha, 2002). However, companies need to decide whether to purchase fingerprint, hand geometry, retina, iris, face, signature or voice - based biometric security system depending on their requirements (Liu and Silverman, 2001). Lease (2005) offered some areas of consideration to organizations considering the use of biometric security technology by investigating the manager's perception of the security effectiveness, need, reliability, and cost-effectiveness of biometrics. But the biometric authentication technologies are still evolving. Nowadays only few organizations and business applications employ biometric systems. But in the future biometrics are expected to play an important role and many business sectors will rely on biometrics. However the crucial cost-benefit question remains:

Research Question 8 *How does the value of complementary organizational resources impact the authentication budget?*

4.8 Effects of resources on security processes (F5)

Path F5 refers to the effect of IT security resources on security processes. Security processes are crucial because they safeguard the confidentiality, integrity and availability of a firm's operations (Khansa and Liginlal, 2009b) and therefore support the firm's business processes (see path F6 in Figure 1). According to Steinklauber (2003) a "good" security process is a cycle which constantly loops checking the security levels according to the security policies and shows control points to guarantee the compliance with the required security level. Steinklauber (2003) also provides a detailed example for the development of a security process in companies that need to communicate with a large number of stakeholders (e.g., customer, business partners, vendors) via extranet connections but financial aspects are not considered in his work. To guarantee stable security processes the firm needs to invest in security resources for example by purchasing a biometric authentication system or by developing security policies for the security process. Siponen (2006) states that not only the existence of a security process but the quality is essential. Also security processes need to be revised constantly (Kanungo, 2006) which is an additional cost factor. Considering the fragmented literature we formulate the following research questions:

Research Question 9 *What are the incentives to invest in IT security resources for a security process and how much and in what security resources does a firm need to invest to install a "good" security process?*

4.9 Effects of security processes on business processes (F6)

According to Jakoubi et al. (2009) the continuous, effective and efficient performance of business processes is the crucial element for success in an organization. Jakoubi et al. (2009) provide on overview of research approaches and open research challenges in the domain of business process security. Firms invest in security processes to guarantee the smooth operation or the improvement of business processes. For example, firms purchase biometric security systems to enhance their business process. The advantages of a biometric system like security, decrease of authentication time and convenience improve the business process but disadvantages like false matches downgrade the business process because workers have to wait to get to their office. Research on whether it does pay off to install a biometric security system is missing so far. As the technology behind biometrics is still evolving (Liu and Silverman, 2001), the False Match Rate, Failure to Enrole and False Non-Match Rate (OECD, 2004) will decrease and therefore the benefits of biometrics for the business process are expected to increase. Regarding the firm's investment in security processes in general, the following research question arises:

Research Question 10 *How is the correlation between the investment in an IT security resource for a security process and its benefits for the business process?*

4.10 Effects of security processes on security process performance (F7)

According to Kueng (2000) assessing process performance is crucial because it enables comparison with competitors and it provides the opportunity to recognize and correct problems before they escalate. So security processes should by measured with performance metrics but measuring security is difficult (Pfleeger and Cunningham, 2010). Technical performance metrics for security processes, such as biometric security authentication systems like FTE, FMR and FNMR (OECD, 2004), have already been developed but these metrics do not give the return on investment which leads to

Research Question 11 *How can the correlation between IT security investment and the quality of the security process be measured?*

4.11 Effects of security process performance on the business process performance (F8)

If a metric as suggested in research question 11 is found, the security process performance will influence the business process performance. We found no literature that covers the resulting research question:
Research Question 12 *How do security process performances affect the overall business process performance?*

4.12 Effects of the IT Business Value Generation Process on the organizational performance (F9)

Path F9 deals with the effect security process performances have on the overall firm performance. Indirectly the security process performance is integrated in the overall firm performance because it influences the business process performance (see path F8 in Figure 1). But the security process performance also has a direct impact on the overall firm performance: We assume that, compared to other organizations, firms with higher security process performance, have a substantial competitive advantage, a better reputation and market value and are more trustworthy. This aspect has not been considered in literature. That leads us to:
Research Question 13 *How does the firm's investment in security processes affect their overall performance?*

4.13 Effects of IT resources on the organizational performance (F10)

Path F10 refers to the effect of IT security resources on organizational performance. There are various studies in information systems research that examine the relationship between investments in IT and payoffs realized in terms of enhanced organizational performance (Bose et al., 2013). The investment in specific IT security resources has an impact on the organization expressed which can be quantified by several metrics. Commonly used metrics (Böhme and Nowey, 2008; Gordon et al., 2005) that measure the organizational performance with regard to investing into IT security resources are discussed in the following: A popular approach is the measurement of the *Return on Security Investment (ROSI)* which is adapted from the return on investment (ROI) and represents the financial gain of a project compared to its total cost (Böhme and Nowey, 2008). As Brocke et al. (2007) indicate, there is no standardized computation and definition of ROSI. 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 (Brocke et al., 2007). 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. For instance, Buck et al. (2008) discuss the value and practicality of applying a derivation of ROSI for the organizational performance of government IT security investment when information sharing is a key success driver. Mizzi (2010) determined the viability of an anti-spam solution with the organizational implications based on this return on IT security investment metric. Closely connected to the ROSI metric is the *Internal Rate of Return (IRR)* which describes particular discount rates at which current and future cash inflows equal cash outflows (Buck et al., 2008). *Net Present Value (NPV)* can also be used to determine whether to invest in IT security. NPV uses the expected discounted cash flows of the investments to quantify the current value of a company's investment project (Gordon and Loeb, 2002a). Eisenga et al. (2012) analyze financial objectives to determine if it is valuable to invest in certain security applications. They illustrate the organizational decision impact of NPV when investing in a technological IT security resource. In the study of Sheen (2010) a fuzzy cost-benefit evaluation model based on NPV is developed to assess the profitability of IT security system projects. Another approach for measuring the organizational performance is the *annual loss expectancy (ALE)* (Böhme and Nowey, 2008). The ALE is calculated by multiplying the estimated frequency of the occurrence of attacks by the potential amount of loss in each outcome (Tanaka et al.,

2005). Cremonini and Martini (2005) used the ALE for the evaluation of the organizational performance. Although they name their metric ROI, it is in fact a derivation of the ALE metric as they simply divided the ALE computation by the cost of security measures. The importance of the described metrics for the measurement of organizational performance when investing IT security resources is underpinned by Gordon et al. (2005). The study states "A significant number of organizations conduct some form of economic evaluation of their security expenditures, with 38 percent using ROI, 19 percent using IRR and 18 percent using NPV" (Su, 2004). Besides these commonly used and well-known metrics, there are other metrics, for example, the cumulated abnormal return (CAR): The studies of Campbell et al. (2003), Andoh-Baidoo and Osei-Bryson (2007) similarly examine the economic effect of IT security breaches on publicly traded corporations. We identified several metrics that are used to measure the organizational performance after having invested in IT security resources. To be precise, there are ample opportunity to assess the performance but we could not detect an extensive study which compares and analyzes the different techniques. An interesting study would be to examine the strengths and weaknesses of organizational performance measures. Although a first attempt is done by Gordon and Loeb (2002a), it is not exhaustive. We identified a lack of depth in comparisons between the organizational metrics; therefore, we propose the following research questions to address this issue:

Research Question 14 ***(a)*** *What are the strengths and limitations of the different organizational security measures?* ***(b)*** *Which metric describes the overall firm performance the best?*

5 Conclusion

We reviewed an extensive amount of IT security investment studies, used the established RBV for analyzing IT security investment research, and outlined research questions for future research. Our contribution is threefold: First, we suggested a new RBV model for IT security investments that unifies different perspectives of the literature. Second, we synthesize the literature based on the developed model. Third, we identified research gaps and formulated 14 research questions in order to stimulate future research on IT security investments.

However, our study has a few limitations. Although we followed a precise and structured process to identify important studies, we may have missed some relevant articles. Further, due to page limitations we had to cite selectively although our search and coverage is exhaustive. Moreover our model has boundaries (as in Webster and Watson (2002)) derived from our theoretical basis (RBV). We excluded papers which focus on the technical perspective of IT security (e.g., Lyu and Lau (2000)) and papers that do not focus on investment (e.g., Moore et al. (2001)).

Drawing a conclusion from our investigation, it should be stated that some aspects of investing in IT security resources are well researched. Especially the effects of IT resources on the organizational performance and the effects of technological IT security resources on technological non-security IT resources have been addressed in depth. Other aspects, such as the effects of resources on security processes or effects of security processes on business processes have received little attention. We hope that our literature review motivates researchers to contribute innovative and rigorous findings to the current body of knowledge.

6 Acknowledgments

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 "Bavarian State of Ministry, Education, Science and the Arts" as part of the FORSEC research association (`https://www.bayforsec.de`).

References

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

Anderson, R. (2001). "Why information security is hard-an economic perspective." In: *Computer Security Applications Conference, 2001 (ACSAC)*, pp. 358–365.

— (2008). "Information security economics - and beyond." In: *Deontic Logic in Computer Science*, pp. 49–49.

Anderson, R. and T. Moore (2006). "The economics of information security." *Science* 314 (5799), 610–613.

Anderson, R. et al. (2008). "Security economics and the internal market." *Study commissioned by ENISA*.

Andoh-Baidoo, F. K. and K.-M. Osei-Bryson (2007). "Exploring the characteristics of Internet security breaches that impact the market value of breached firms." *Expert Systems with Applications* 32 (3), 703–725.

Ang, S. and D. W. Straub (1998). "Production and transaction economies and IS outsourcing: a study of the US banking industry." *MIS Quarterly* 22 (4), 535–552.

Babich, A. et al. (2012). "Biometric Authentication. Types of biometric identifiers."

Baker, W. H. et al. (2007). "Necessary measures: metric-driven information security risk assessment and decision making." *Communications of the ACM* 50 (10), 101–106.

Bandara, W. et al. (2011). "A systematic, tool-supported method for conducting literature reviews in information systems." In: *Proceedings of the 19th European Conference on Information Systems (ECIS 2011)*.

Bandyopadhyay, T. et al. (2009). "Why IT managers don't go for cyber-insurance products." *Communications of the ACM* 52 (11), 68–73.

Banerjee, S. and D. Y. Golhar (1994). "Electronic data interchange: characteristics of users and non-users." *Information & Management* 26 (2), 65–74.

Barney, J. (1991). "Firm resources and sustained competitive advantage." *Journal of Management* 17 (1), 99–120.

Barney, J. et al. (2001). "The resource-based view of the firm: Ten years after 1991." *Journal of Management* 27 (6), 625–641.

Barney, J. B. (1986). "Strategic Factor Markets: Expectations, Luck, and Business Strategy." *Management Science* 32 (10), 1231–1241.

Barua, A. et al. (1995). "Information technologies and business value: An analytic and empirical investigation." *Information Systems Research* 6 (1), 3–23.

Beautement, A. et al. (2009). "The compliance budget: managing security behaviour in organisations." In: *Proceedings of the 2008 Workshop on New Security Paradigms*. ACM, pp. 47–58.

Beresnevichiene, Y. et al. (2010). "Decision support for systems security investment." In: *Network Operations and Management Symposium Workshops (NOMS)*. IEEE, pp. 118–125.

Berinato, S. (2002). "Finally, a real return on security spending." *CIO* 15 (9), 42–50.

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

Bitter, C. et al. (2010). "Application of artificial neural networks and related techniques to intrusion detection." In: *The 2010 International Joint Conference on Neural Networks (IJCNN)*. IEEE, pp. 1–8.

Blundell, R. et al. (1999). "Human capital investment: the returns from education and training to the individual, the firm and the economy." *Fiscal studies* 20 (1), 1–23.

Bodin, L. D. et al. (2005). "Evaluating information security investments using the analytic hierarchy process." *Communications of the ACM* 48 (2), 78–83.

Bodin, L. D. et al. (2008). "Information security and risk management." *Communications of the ACM* 51 (4), 64–68.

Böhme, R. and T. Moore (2013). *Security Metrics and Security Investment*. Tech. rep. SMU Lyle School of Engineering.

Böhme, R. and T. Nowey (2008). "Economic security metrics." In: *Dependability Metrics*. Springer, pp. 176–187.

Bojanc, R. and B. Jerman-Blažič (2008a). "An economic modelling approach to information security risk management." *International Journal of Information Management* 28 (5), 413–422.

— (2008b). "Towards a standard approach for quantifying an ICT security investment." *Computer Standards & Interfaces* 30 (4), 216–222.

Boote, D. N. and P. Beile (2005). "Scholars before researchers: On the centrality of the dissertation literature review in research preparation." *Educational researcher* 34 (6), 3–15.

Bose, R. et al. (2013). "The Relationship between Information Security Investment and Organizational Performance: A Critical Review." In: *Proceedings for the Northeast Region Decision Sciences Institute*, pp. 606–617.

Brocke, J. vom et al. (2007). "Return on security investments–towards a methodological foundation of measurement systems." In: *AMCIS 2007 Proceedings*.

Buck, K. et al. (2008). "Applying ROI analysis to support SOA information security investment decisions." In: *2008 IEEE Conference on Technologies for Homeland Security*. IEEE, pp. 359–366.

Camp, L. J. and C. Wolfram (2000). "Pricing security." In: *Proceedings of the CERT Information Survivability Workshop*. Citeseer, pp. 31–39.

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), 431–448.

Cavusoglu, H. et al. (2002). "The effect of internet security breach announcements on market value of breached firms and internet security developers." *International Journal of Electronic Commerce* 9 (1), 69–104.

Cezar, A. et al. (2013). "Outsourcing information security: Contracting issues and security implications." *Management Science* 60 (3), 638–657.

Chai, S. et al. (2011). "Firms' information security investment decisions: Stock market evidence of investors' behavior." *Decision Support Systems* 50 (4), 651–661.

Chandler, A. (1977). *The visible hand. the managerial revolution in American business*. Cambridge, Mass. [u.a.]: Belknap Press. XVI, 608.

Chew, E. (2008). *Performance measurement guide for information security*. National Institute of Standards and Technology, Technology Administration, US Department of Commerce.

Chun, S.-H. (2011). "Smart mobile banking and its security issues: from the perspectives of the legal liability and security investment." In: *Future Information Technology*. Springer, pp. 190–195.

— (2013). "The burden of proof and the optimal security investment of firms in ubiquitous computing." *Personal and Ubiquitous Computing* 17 (5), 965–969.

Coase, R. H. (1937). "The Nature of the Firm." *Economica* 4 (16), 386–405.

Cohen, F. (2006). *IT Security Governance Guidebook with Security Program Metrics on CD-ROM*. CRC Press.

Cooper, H. M. (1988). "Organizing knowledge syntheses: A taxonomy of literature reviews." *Knowledge in Society* 1 (1), 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*. ACM, pp. 35–41.

Cremonini, M. and P. Martini (2005). "Evaluating Information Security Investments from Attackers Perspective: the Return-On-Attack (ROA)." In: *Workshop on the Economics of Information Security 2005 (WEIS)*.

Dahlberg, T. et al. (2008). "Past, present and future of mobile payments research: A literature review." *Electronic Commerce Research and Applications* 7 (2), 165–181.

Davenport, T. (1993). *Process innovation: reengineering work through information technology*. Boston: Harvard Business School Press.

Dehning, B. and V. J. Richardson (2002). "Returns on investments in information technology: A research synthesis." *Journal of Information Systems* 16 (1), 7–30.

Demirhan, D. (2005). "Factors affecting investment in IT: a critical review." *Journal of Information Technology Theory and Application (JITTA)* 6 (4), 3.

Devaraj, S. and R. Kohli (2000). "Information technology payoff in the health-care industry: a longitudinal study." *Journal of Management Information Systems* 16 (4), 41–67.

Ding, W. et al. (2005). "Outsourcing internet security: Economic analysis of incentives for managed security service providers." In: *Internet and Network Economics*. Springer, pp. 947–958.

Eisenga, A. et al. (2012). "Investing in IT Security: How to Determine the Maximum Threshold." *International Journal of Information Security and Privacy (IJISP)* 6 (3), 75–87.

Fedorowicz, J. and U. Gelinas (1999). "Adoption and Usage Patterns of an IT Audit and Control Framework." In: *AMCIS 1999 Proceedings*.

Frost & Sullivan (2011). *The 2013 (ISC)2 Global Information Security Workforce Study*. Tech. rep. International Information Systems Security Certification Consortium ((ISC)2).

Gal-Or, E. and A. Ghose (2005). "The economic incentives for sharing security information." *Information Systems Research* 16 (2), 186–208.

Gartner (2011). *Magic Quadrant for Security Information and Event Management*. Tech. rep. Gartner RAS Core Research.

— (2012). *IT Key Metrics Data 2012: IT Enterprise Summary Report*. Tech. rep. Gartner RAS Core Research.

Ghose, A. and U. Rajan (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 M. P. Loeb (2002a). "Return on information security investments: Myths vs. realities." *Strategic Finance* 84, 26–31.

— (2002b). "The economics of information security investment." *ACM Transactions on Information and System Security (TISSEC)* 5 (4), 438–457.

Gordon, L. A. and M. P. Loeb (2007). "Economic aspects of information security: An emerging field of research." *Information Systems Frontiers* 8 (5), 335–337.

Gordon, L. A. et al. (2003). "Sharing information on computer systems security: An economic analysis." *Journal of Accounting and Public Policy* 22 (6), 461–485.

Gordon, L. A. et al. (2005). *CSI/FBI Computer Crime and Security Survey*. Computer Security Institute.

Grossklags, J. et al. (2008a). "Secure or insure?: a game-theoretic analysis of information security games." In: *Proceedings of the 17th International Conference on World Wide Web*. ACM, pp. 209–218.

— (2008b). "Security and insurance management in networks with heterogeneous agents." In: *Proceedings of the 9th ACM Conference on Electronic Commerce*. ACM, pp. 160–169.

Gupta, A. and D. Zhdanov (2012). "Growth and sustainability of managed security services networks: an economic perspective." *MIS Quarterly* 36 (4), 1109–1130.

Hagen, J. M. et al. (2008). "Implementation and effectiveness of organizational information security measures." *Information Management & Computer Security* 16 (4), 377–397.

Hart, C. (1998). *Doing a literature review: Releasing the social science research imagination*. Sage.

Hoo, K. J. S. (2000). *How much is enough? A risk management approach to computer security*. Stanford University.

Hua, J. and S. Bapna (2009). "Optimal Investment in Information System Security: A Game Theoretical Approach." In: *AMCIS 2009 Proceedings*.

Huang, C. D. and J. Goo (2009). "Investment decision on information system security: A scenario approach." In: *AMCIS 2009 Proceedings*.

Jakoubi, S. et al. (2009). "A roadmap to risk-aware business process management." In: *Services Computing Conference, 2009*. IEEE, pp. 23–27.

Jiang, L. et al. (2008). "Efficiency of selfish investments in network security." In: *Proceedings of the 3rd international workshop on Economics of networked systems*. ACM, pp. 31–36.

Kanungo, S. (2006). "Portfolio approach to information technology security resource allocation decisions." In: *PACIS 2006 Proceedings*.

Khansa, L. and D. Liginlal (2009a). "Quantifying the benefits of investing in information security." *Communications of the ACM* 52 (11), 113–117.

— (2009b). "Valuing the flexibility of investing in security process innovations." *European Journal of Operational Research* 192 (1), 216–235.

King, W. R. and J. He (2005). "Understanding the role and methods of meta-analysis in IS research." *Communications of the Association for Information Systems* 16 (1), 32.

Kueng, P. (2000). "Process performance measurement system: a tool to support process-based organizations." *Total Quality Management* 11 (1), 67–85.

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

Lease, D. R. (2005). "Factors influencing the adoption of biometric security technologies by decision making information technology and security managers." PhD thesis. Capella University.

Lee, S. (2010). "Using data envelopment analysis and decision trees for efficiency analysis and recommendation of B2C controls." *Decision Support Systems* 49 (4), 486–497.

Levitin, G. et al. (2012). "Data survivability vs. security in information systems." *Reliability Engineering & System Safety* 100, 19–27.

Liang, T. and J. You (2009). "Resource-based View in Information Systems Research: A Meta-Analysis." *PACIS 2009 Proceedings*.

Liang, T. et al. (2010). "A resource-based perspective on information technology and firm performance: a meta analysis." *Industrial Management & Data Systems* 110 (8), 1138–1158.

Lichtenberg, F. R. (1995). "The output contributions of computer equipment and personnel: A firm-level analysis." *Economics of Innovation and New Technology* 3 (3-4), 201–218.

Liu, D. P. and T. Bandyopadhyay (2010). "Modeling IT Security Investment in Target Group of Similar Firms: A Control Theoretic Approach." In: *SAIS 2010 Proceedings*.

Liu, S. and M. Silverman (2001). "A practical guide to biometric security technology." *IT Professional* 3 (1), 27–32.

Lyu, M. R. and L. K. Lau (2000). "Firewall security: Policies, testing and performance evaluation." In: *The 24th Annual International Computer Software and Applications Conference, 2000 (COMPSAC)*. IEEE, pp. 116–121.

Mata, F. J. et al. (1995). "Information technology and sustained competitive advantage: a resource-based analysis." *MIS Quarterly* 19 (4), 487–505.

Matyáš, V. and Z. Říha (2002). "Biometric authentication—security and usability." In: *Advanced Communications and Multimedia Security*. Springer, pp. 227–239.

McAfee (2014). *Net Losses: Estimating the Global Cost of Cybercrime*. Tech. rep. Center for Strategic and International Studies.

Melville, N. et al. (2004). "Review: Information technology and organizational performance: An integrative model of IT business value." *MIS Quarterly* 28 (2), 283–322.

Mercuri, R. T. (2003). "Analyzing security costs." *Communications of the ACM* 46 (6), 15–18.

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), 18–24.

Moore, A. P. et al. (2001). *Attack modeling for information security and survivability*. Tech. rep. DTIC Document.

Neubauer, T. and J. Heurix (2008). "Defining secure business processes with respect to multiple objectives." In: *Third International Conference on Availability, Reliability and Security (ARES)*. IEEE, pp. 187–194.

Nevo, S. and M. R. Wade (2010). "The formation and value of IT-enabled resources: antecedents and consequences of synergistic relationships." *MIS Quarterly* 34 (1), 163–183.

OECD (2004). *The Security Economy*. Tech. rep. Organisation for Economic Co-operation and Development.

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

Pfleeger, S. L. and R. K. Cunningham (2010). "Why measuring security is hard." *Security & Privacy* 8 (4), 46–54.

Richardson, R. and C. Director (2008). "CSI computer crime and security survey." *Computer Security Institute* 1, 1–30.

Rosenfeld, S. N. et al. (2007). "Archetypal behavior in computer security." *Journal of Systems and Software* 80 (10), 1594–1606.

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)*.

Rowe, F. (2014). "What literature review is not: diversity, boundaries and recommendations." *European Journal of Information Systems* 23 (3), 241–255.

Rumelt, R. P. (1984). "Towards a strategic theory of the firm." *Competitive strategic management* 26, 556–570.

Sheen, J. (2010). "Fuzzy economic decision-models for information security investment." *Proceedings of the 9th WSEAS International Conference on Instrumentation, Measurement, Circuits and Systems*, 141–147.

Siponen, M. (2006). "Information security standards focus on the existence of process, not its content." *Communications of the ACM* 49 (8), 97–100.

Sonnenreich, W. et al. (2005). "Return On Security Investment (ROSI): A practical quantitative model." *Journal of Research and Practice in Information Technology* 38 (1), 239–252.

Steinklauber, K. (2003). *Security Process for the Implementation of a company's extranet network connections*. Tech. rep. SANS Institute.

Stephanou, A. (2009). "The impact of information security awareness training on information security behaviour." PhD thesis. University of the Witwatersrand.

Stigler, G. J. (1961). "The economics of information." *The Journal of Political Economy* 69 (3), 213–225.

Su, X. (2004). *An overview of economic approaches to information security management*. Tech. rep. Centre for Telematics and Information Technology University of Twente.

Sun, W. et al. (2008). "Information security problem research based on game theory." In: *International Symposium on Electronic Commerce and Security*. IEEE, pp. 554–557.

Tanaka, H. et al. (2005). "Vulnerability and information security investment: An empirical analysis of e-local government in Japan." *Journal of Accounting and Public Policy* 24 (1), 37 –59.

Torrellas, G. A. S. and L. A. V. Vargas (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.

Vinekar, V. and J. T. C. Teng (2012). "The Resource-Based View of IT Business Value: Complementary Investments or Embedded Knowledge?" *Journal of Information and Knowledge Management* 11 (1), 1–20.

Wade, M. and J. Hulland (2004). "Review: the resource-based view and information systems research: review, extension, and suggestions for future research." *MIS Quarterly* 28 (1), 107–142.

Wang, X. et al. (2008). "Access Control for Human Tasks in Service Oriented Architecture." In: *International Conference on e-Business Engineering (ICEBE)*. IEEE, pp. 455–460.

Wattel, B. (2002). "Business process security." In: *Integrity, Internal Control and Security in Information Systems*. Springer, pp. 177–186.

Weber, K. et al. (2009). "One Size Does Not Fit All—A Contingency Approach to Data Governance." *Journal of Data and Information Quality (JDIQ)* 1 (1), 4.

Webster, J. and R. T. Watson (2002). "Analyzing the past to prepare for the future: Writing a literature review." *MIS Quarterly* 26 (2), 3.

Wernerfelt, B. (1984). "A resource-based view of the firm." *Strategic Management Journal* 5 (2), 171–180.

Whitman, M. E. (2003). "Enemy at the gate: threats to information security." *Communications of the ACM* 46 (8), 91–95.

Williamson, O. (1975). *Markets and hierarchies, analysis and antitrust implications: a study in the economics of internal organization*. Free Press.