Hanna Toivanen

CASE STUDY OF WHY INFORMATION SECURITY INVESTMENT DECISION FAIL?

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2015

TIIVISTELMÄ

Toivanen, Hanna
Case tutkimus - Miksi informaatioturvallisuuden investointihanke hylätään?
Jyväskylä: Jyväskylän yliopisto, 2015, 76s.
Tietojärjestelmätiede, pro gradu-tutkielma
Ohjaaja(t): Siponen, Mikko ja Tuunanen, Tuure

Tämä tutkielma keskittyy tietoturvainvestointien päätöksentekoprosessiin. Tavoitteena on tutkia miksi tietoturvainvestointipäätös hylätään. Tutkimuksen teoreettinen tausta perustuu aiemmin suoritettuun tutkimukseen, mikä on pääosin käsitellyt tietoturvainvestointeja joko optimaalisen investointitason näkökulmasta, tai tehokkaan investointitason näkökulmasta. Aiempi tutkimus ei ole käsitellyt tietoturvainvestointeja epäonnistuneen päätöksenteon näkökulmasta, eikä siten voi esittää perusteluita päätöksenteolle. Tämän tutkielman tuloksena esitetään teoreettisia väittämiä, jotka tarjoavat mahdollisia vastauksia tutkimuskysymykseen. Tämä tutkimus täydentää osaltaan akateemista kirjallisuutta, ja tarjoaa käytännön tietoa organisaatioille tietoturvainvestointien päätöksentekoprosessiin vaikuttavista tekijöistä.

Tutkimuksessa käytettiin tutkimusstrategiaa, missä uutta teoriaa luodaan case-tutkimuksen pohjalta. Tutkimus toteutettiin kvalitatiivisena case-tutkimuksena, jossa oli mukana neljä eri case-yritystä. Empiirinen osuus toteutettiin avoimina haastatteluina, joiden tulokset analysoitiin hyödyntäen induktiivista sisällönanalyysia. Tutkimustuloksia analysoitiin edelleen taso-teoria mallin avulla.

Tämän tutkimuksen löydökset osoittavat, että haasteet tietoturvainvestointien suhteen ovat moninaiset. Tämä tutkielma määritteli kolme teoreettisista väittämää ja niihin liittyvät ala-väittämät. Määriteltyjen teoreettisten väittämien mukaan tietoturvainvestointihankkeen hylkääminen liittyy organisaation metodeihin ja kyvykkyyksiin määritellä ja perustella investointihankkeita, sekä johdon tietotaidon tasoon tietoturvaan liittyen. Myös organisaation tapa toimia, organisaation kulttuuri sekä asenne tietoturvaan liittyen vaikuttavat päätöksentekoprosessiin, kuten myös johdon sitoutuminen ja tuki, sekä poliittiset tekijät.

Avainsanat: Tietoturva, tietoturvainvestointi, päätöksenteko, tietotaito, kyvykkyys, metodit.

ABSTRACT

Toivanen, Hanna
Case study of why information security investment fail?
Jyväskylä: University of Jyväskylä, 2015, 76p.
Information Systems, Master's Thesis
Supervisor(s): Siponen, Mikko and Tuunanen, Tuure

This thesis focuses on information security investment decision making process, and the object is to investigate why decisions fail. The theoretical background of the research consist of previous research, which are mainly conducted from the optimal information security investment, and the efficiency of information security investment perspectives. Previous research have not addressed the problem why information security investment decisions fail, and thus cannot explain the reasoning. A key outcome of the thesis is to provide theory propositions which offers a feasible answer to the research question. This research fills the research gap in the academic literature, and provides guidance to organizations about affecting drivers in the field of information security investment management.

This research utilized a research strategy where theory is built from case studies, including four case companies. The study material was gathered with open interviews, and material was analyzed with the inductive content analysis method. Analyzed material was further processed with stage model.

This study findings indicated, that the challenge of information security investment management is multilateral. This thesis defined theory propositions and related sub-propositions. According to the defined theory propositions the likelihood of getting the information security investment proposal rejected relates to organizations' methods and capabilities to define and argue an investment proposal, and to sufficient level of knowledge about information security in management level. The organizational way of working and organizational culture and attitude affect to decision making, as well as the management commitment and support, and political aspects.

Keywords: Information security, information security investment, decision making, knowledge, capability, method.

FIGURES

TABLES

TABLE OF CONTENTS

1 INTRODUCTION

Security can only be achieved through constant change, through discarding old ideas that have outlived their usefulness and adapting other to current facts.

(William O. Douglas, U.S. Supreme Court Justice (1898 – 1980)

This study offers a detailed case study of why information security investment decision making process fail. In particular, it is examined which are the key drivers behind the information security investment decision. By examining *why* information security investment decision fail, it is attempted to extrapolate certain series of theory propositions, which are justified with empirical data.

In today's business setting, business operations are enabled by technology. Information technology enables the storage and transportation of the information – which is most probably the company's most valuable asset. The ultimate purpose of the information security is to secure the continuous operation of information systems and data networks which are crucial for business, to protect the unauthorized usage of the data and information systems, unintended and intended data destruction or distortion, and to minimize the derived damages. The management of the organization is in key role in organizing, planning, maintaining and developing the information security. Information security and its successful management requires managerial commitment to be developed further (Andreasson and Koivisto, 2013). The key factor in getting value from information security is to insure that technology investment protects the right things. The financial returns from a successful implementation of a security-enabled business process should justify the expenses of security in terms of enabling business (Tsiakis and Stephanides, 2005). From information technology point of view it is essential that in a competitive environment the right information systems/technology investments are selected in order to sustain corporate viability and prosperity (Bacon, 1994). According to Siponen et al (2014), the information security investments are not keeping the pace with information technology investments. This has caused a problem of underinvestment. One concrete level example of this could be that an organization has

made information technology investments to establish email communication, but has not invested in email encryption. According to Siponen et al (2014), the underinvestment of information security is a highly ranked problem in practitioners' surveys.

The main objective of this thesis is to gather empirical data about the information security investment decision making process and understand the reasons behind failed investment decisions. A key outcome of the thesis is to provide theory propositions as there are no existing theory that offers a feasible answer to the research question. Previous research have approached the information security investment problems theoretically examining the optimal information security investment (for example Gordon and Loeb, 2002; Huang et al., 2008; Kort et al., 1999) and the efficiency of information security investment (for example Gordon and Loeb, 2006; Purser, 2004) (Karjalainen et al., 2014). Previous research does not address the research question at all, or it is done in inadequate way.

This study's main research question is:

- Why information security investment decision fail?

This study utilized a research strategy where theory is built from case studies. It involves using one or more cases to create theoretical constructs, propositions and/or midrange theory from case-based, empirical evidence (Eisenhardt, 1989). A data collection method used was an open interview. Case study can be seen justifiable for this research, because it serves for both causes: the main research objective and the research approach. Case study is an empirical inquiry, where specific cases are examined for example by observing or interviewing in their natural condition. The research material of the empirical part of the study were gathered by interviewing pre-selected people having a key role in making information security investment management decisions. Interviewed people represented four different case companies, which are not detail level identified within this study, as information security is case sensitive. The status of each case company's information security management is described with the stage models by describing the process for managing information security investments from initializing the investment proposal until its decision making.

This study results indicated that the challenge of information security is multilateral. There are several variables that determines how information security is structured in an organization. This study results indicated, that the most influential variables are both the organizational culture and attitude toward, and management commitment and support to information security management. This study also indicated, that appropriate level of reasoning of investment proposals, definition the value of security investments and finding an appropriate criteria to argue the value of investment are challenges in the information security investment decision making process. There are also challenges that relates to decision makers' different interests, and to political aspects.

1.1 Thesis outline

In the introduction the study background and the basis for this research are presented. This does include the research question and the motivations for conducting the study. The purpose of the chapter two is to familiarize the reader to the study subject and to the field of the information security management in business operational setting. The second chapter gives a definition to information security specific terminology, containing also information about the information technology and information security investment. The second chapter also discusses what kind of challenges information security investment decision makers are facing in managing information technology and information security investments, which familiarize the reader in a concrete level. Third chapter of this study walks through the previous research conducted within information security investments. Chapter three defines also the stage theory model and how it is utilized within this study. Chapter four defines the research methods and the research progress. The fifth chapter provides the stage models for each case company, provides the analysis of the interview findings with empirical evidence and lastly defines the theory propositions and related sub-propositions. The sixth chapter discusses the study findings, implications both to the research and practice, and finally the chapter seven concludes the study summarizing the study as a whole.

2 OVERVIEW TO INFORMATION TECHNOLOGY AND INFORMATION SECURITY INVESTMENT MANAGEMENT

This chapter gives background to information security as a definition with also presenting an overview to information security management, information technology, and information security investments. This chapter also discusses about the key challenges of the information technology and information security investment management, which purpose is to provide concrete level information to the reader about the key challenges that the information security investment decision makers are facing within this study subject. This chapter also attempts to describe the difference between information technology and information security investment.

2.1 Information security

Being secure is to be protected from the risk of loss, damage, unwanted modifications or other hazards. In an organization, security is normally achieved by combining and implementing several strategies, where each strategy is concentrating on a specific area of security. Management of the organization should take care that each strategy is properly planned, organized, staffed, directed, and controlled. Information security includes several broad areas of information security management, computer and data security, and network security, which are illustrated in the Figure1 (Whitman and Mattord, 2013). Whitman and Mattord (2013, p. 4) defined information security as follows:

"Information security is the protection of information and its critical characteristics (confidentiality, integrity, and availability), including the system and hardware that use, store, and transmit that information, through the application of policy, training and awareness programs, and technology."

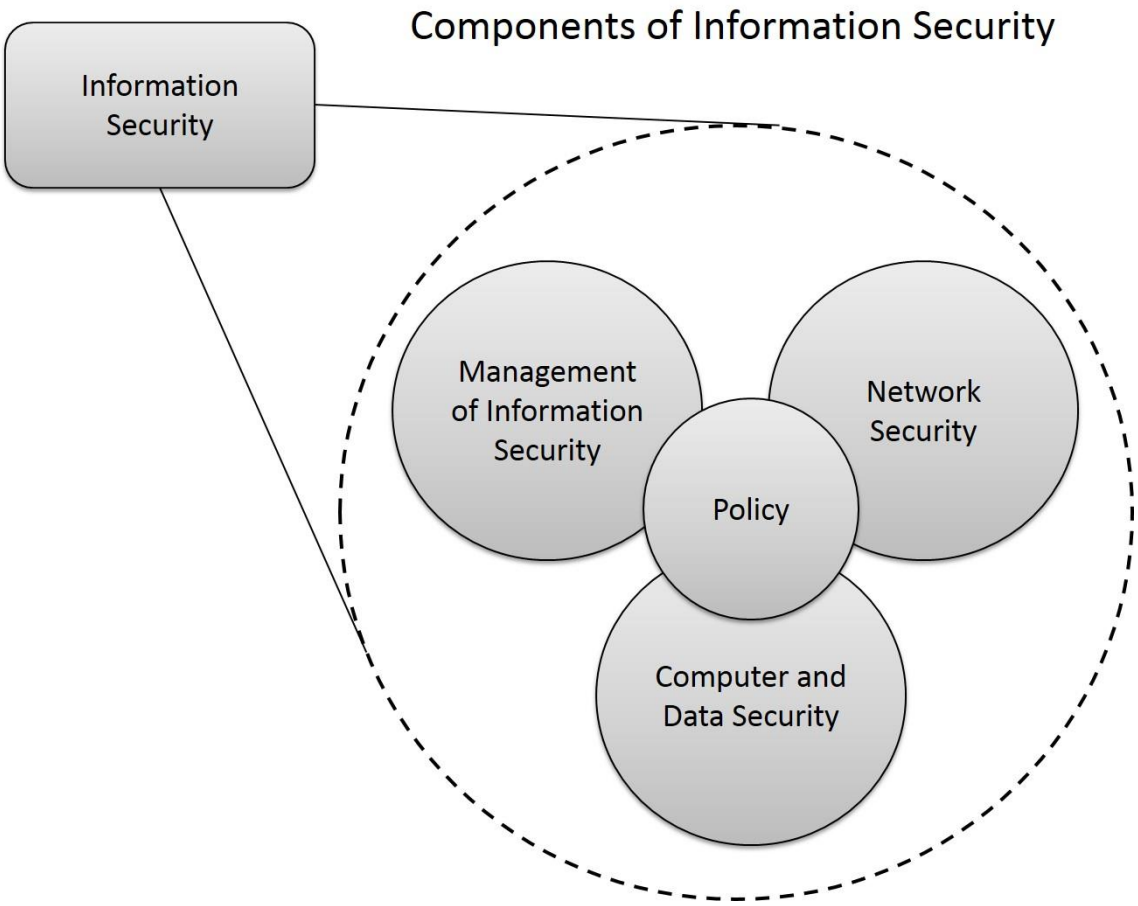

FIGURE 1 Components of information security by Whitman and Mattord (2013)

Whitman and Mattord (2013) further defined security as a continuous series or chain of projects, which comprise a process. They defined an information security program chain, where each link could be a specific project. Still some aspects of information security are not project based, they are managed processes and called as operations. Such operations are for example the monitoring of the external and internal environments during incident response, ongoing risk assessments of routine operations, and continuous vulnerability assessment and vulnerability repair. Projects are defined as discrete sequences of activities both with defined starting and ending points. Although, each individual information security project has an ending point, especially in larger organizations information security improvement process never completely finish. In such cases process is periodically reviewed and planning is realigned to meet business and information technology objectives. This realignment can lead to new goals and projects, but as well to modification, cancellation or reprioritization of existing projects (Whitman and Mattord, 2013). Also Andreasson and Koivisto (2013), defined that information security is a process, which is constantly followed and modernized. They defined, that the purpose of the information secu-

rity is to secure the continuous operation of information systems and data networks which are crucial for business, to protect the unauthorized usage of the data and information systems, unintended and intended data destruction or distortion, and to minimize the derived damages. Andreasson and Koivisto (2013), stressed that information security should be carefully considered especially in situations when information management and/or information technology maintenance is outsourced, company takes new operating models into use or is investing in information technology and defining requirements related to it.

2.2 Information security management

Information security management is a management process, which defines how information security specific issues should be managed in the company or/and organization. Information security management should be organized and implemented to support organization's business operations and achieving its strategical goals. Information security management is partly execution of the law requirements and good regime. Implementation of the information security management should also be cost effective. Andreasson and Koivisto (2013) further defined, that information security management should be natural part of the organization's daily operation and especially part of the risk management. It should form a basis for continuous planning and operational reliability. With a proper information confidentiality organization can protect its operational environment and its customers' trade secrets – and also provide privacy for citizens (Andreasson and Koivisto, 2013).

The management of the organization is in key role in organizing, planning, maintaining and developing the information security. Information security and its successful management requires managerial commitment to develop it further. There should be named a responsible person for information security management, and he should be supported by sufficient resources to manage and implement the organizational information security obligations. The responsible person should report about the development and implementation status of the information security to the management, whose responsibility is to ensure that responsible person has access to all relevant information related to information security. The responsible person should be informed for example about the all relevant investment and development projects and he should also be involved in decision making. Management team should take care that information security is implemented in every level in the organization. Management should ensure, that information security is taken into consideration and it is implemented in essential administrative operations, for example in information-, human resources-, financial- and in material management as well as in procurement (Andreasson and Koivisto, 2013).

Organization's information security policy defines the targeted level of information security. Information security policy defines in detail the company's

information security targets and the instructional factors, for example law based requirements and industry specific requirements. It also defines the obligations, commands and instructions for the company. Information security policy also specifies the risk management procedure for information security specific issues and guides the prioritization of them. It also states the information security related responsibilities and roles, and specifies how both the training and communication about information security should be managed in the company.

2.3 Information technology investment

Tsiakis and Stephanides (2005) defined, that the concept of investment has one purpose – to generate a return. This return can be seen in the form of capital, time and benefits, which could be both tangible and intangible. The calculation of intangible assets is more difficult and it is proper to be transformed into a monetary equivalent. According to Bacon (1994), there is no uniform definition of what constitutes an information technology investment, and not all investment in information technology is of a capital nature. There are current cost of processing and operations, which are clearly not – as neither is "routine" systems maintenance. Bacon (1994) stated, that the outlays for hardware, network facilities and externally developed software products are clearly capital expenditures. In addition to that, also in-house development projects involving new systems and significant enhancements activities would also be seen as capital expenditures. An investment in the form of salaries to pay for in-house information systems development may not appear to fit in the capital definition, as it may not involve the implicit external expenditure. Still, making the decision to go forward with such a project generally commits the organizations to remarkable internal expense, and the decision is based on a stream of expected benefits. According to Bacon (1994), by giving a go-ahead decision for an in-house information system development project, nevertheless the absence of external expenditure, it seems to have the economic nature of a capital investment decision. Bacon (1994), stated that definition of capital investment for information technology purposes include any investment that looks beyond the short term, which he saw to be anything beyond one year (Bacon, 1994). In a competitive environment, selecting and effectively pursuing the right information systems/technology investments can be a key factor in sustaining corporate viability and success (Bacon, 1994). Kambil et al. (1991) saw information systems investments enabler for companies to exercise their business strategies for future growth and cost savings. They argued that strategic information system investments provide firms with managerial flexibility and real options to effectively respond to changing business environments. Also Mithas et al. (2011) studied how the information technology capabilities contribute to firm performance. Mithas et al. (2011) derived the information management capability definition from Marchand et al. (2000) research work, who defined information

management capabilities to three sets of factors, which they saw to explain firm success. These three factors are as follows:

1. The quality of Information Technology management practices (e.g. integrating Information Technology into key operational and managerial processes),
2. The ability to develop appropriate information management processes to sense, gather, organize, and disseminate information; and
3. The ability to instill desired information behaviors and values (e.g. proactiveness, sharing, integrity) (Marchand et al., 2000).

Mithas et al. (2011) study results indicated that information management capability plays an important role in developing other firm capabilities for customer management, process management and performance management. They pointed that these capabilities favorably influence customer, financial, human resources, and organizational effectiveness measures of firm performance. Among other key managerial responsibilities senior leaders must focus on creating necessary conditions for developing information technology infrastructure and information management capability because they play a foundational role in building other capabilities and enablers for improved company performance (Mithas et al., 2011).

2.4 Information security investment

The incidence of security breaches and cyber-attacks has become a major concern in recent times. There has been attacks, which have been directed at a wide variety of organizations, ranging from high-profile companies to prestigious universities. According to Stamp et al. (2005), present-day hackers seem to appear more motivated by financial gains than by personal curiosity or thrill seeking behavior. Liu et al. (2011) saw information security investment as a direct way to increase company's security, which should be made after carefully trading-off investment costs with the increase in information security that is brought by the investment.

Tsiakis and Stephanides (2005) defined that the key factor in getting value from information security is to insure that technology investment protects the right things. They saw as critical that the business organizations evaluate the security procedures for network infrastructure and information assets. The financial returns from a successful implementation of a security-enabled business process should justify the expenses of security in terms of enabling business. Brink (2001), defined that financial returns are typically application-specific, meaning that a security in the absence of a specific business process returns nothing. For that reason, business organization has the responsibility to assess the security investments versus the chance that an incident or security breach

will happen, that could produce losses multiplied by the impact of the problem will create.

Magnusson et al. (2007) evaluated information security investments from business value point of view. They found at least two ways how information security investment could create business value. As a first, they identified that it can enhance company's efficiency, by decreasing operational expenses due to investments in information security. A security service will for example execute controls which were previously carried out by back office personnel, thus increasing back office productivity. Information security investments can also increase efficiency by decreasing costs for business interruption, fraud and embezzlement. Secondly, Magnusson et al. (2007) defined that information security investment can increase company's effectiveness by enabling new, superior processes and products, and thus providing competitive advantage in the market (Magnusson et al., 2007).

CISCO instead, has analyzed the concept of security from economic impact point of view. In their estimation, organizations could have three different impacts in case of security breach:

- Immediate economic impact – the cost of repairing or replacing systems and the disruption of business operations and cash flow.
- Short-term economic impact – the loss of contractual relationship or existing customers because of the inability to deliver products or services and a negative impact on the reputation of the organization.
- Long-term economic impact – the decline in an organization's market valuation and stock prices (CISCO).

Wisely investments in information security can enhance and improve organizational performance. Making a good investment that will best satisfy all the necessary decision criteria requires a careful and inclusive analysis. Usually the expenses for any investment made are compared to the cost saved. The economic justification of investments in information security is a basic issue for information technology management. In a management level, strategic security investments are to support business strategy. Information security should not be seen as technological problem resolved only with technical means. Information security should be part of the business approach and in risk management that needs to identify significant costs (time, expense, reduced functionality, unavailability, etc. if a security incident take place) meaning economic reasoning that explains the investment in security (Tsiakis and Pekos, 2008). When the investment decision relates to information security, it is essential to know what areas of improvement are prioritized in the organization. There are multiple stakeholders in a company, whose needs and demands should be taken into account and who need to take appropriate actions. Like defined already earlier, many information security initiatives provide value to the company by managing identified risks through decreased incident costs. Other security investments aim at improving governance effectiveness or meeting compliance requirements. Despite what is the targeted outcome of the investments, they need

to be clearly aligned to one or several business objectives in order to guide the leadership team making the investment decisions (Tsiakis and Theodiosos, 2014).

Fenz et al., (2011) analyzed that information security investment decision maker's encounter with following questions:

1. What are potential threats for my organization,
2. What is the likelihood of these threats,
3. What is the potential impact of a particular treat,
4. Which vulnerabilities could be exploited by such treats,
5. Which controls are required to mitigate these vulnerabilities, and
6. What are the investments in security worth?

According to Whitman and Mattord (2013), information security exists in an organization primarily to manage information technology risks. They defined risk management as a process of discovering and assessing the risks to an organization's operations and determining how those risks can be controlled and mitigated. They further stated, that in well-organized business operational setting both the risk identification and assessment, and the risk control are implemented. In order to manage risk properly, organization need to have understanding how information is processed, stored and transmitted. In this context it requires knowledge about which information assets are valuable to the organization, identifying, categorizing and classifying those assets, and understanding how those assets are currently protected (Whitman and Mattord, 2013). According to Tsiakis and Pekos (2008), risk analysis is useful method for providing appropriate data input to the financial analysis and effectiveness measurement of information security management. Tsiakis and Pekos (2008) stated, that risk analysis is best performed as top-down scenario oriented, where for example business units quantify costs of unavailability based on the duration and costs due to loss of confidentiality while the information technology department quantify costs due to loss of integrity and the probability of these security issues. He saw this resulting in the business impact of security risks and allowing determination of influence of security on necessary capital charge and the expected losses (Tsiakis and Pekos, 2008).

When top level management makes investment decisions, it strives to find a balance between risk and reward for the company to meet its overall goals and ambitions. Decision making process contains many challenges, though those differentiate between information technology and information security investment. Following chapter will discuss in more detail the challenges in information technology and information security investment management.

2.5 Challenge of information technology and information security investment

Companies are facing increasing economic and competitive pressures. The importance of aligning information technology strategy with business strategy is essential (Ariyachandra and Frolick, 2008). In order to promote shareholder value, every measure taken by the company management should maximize the value creation, from strategic investments to procedures for managing the daily operations (Magnusson et al., 2007). From information technology point of view it is essential that in a competitive environment the right information systems/technology investments are selected in order to sustain corporate viability and prosperity (Bacon, 1994). The challenge of information security is different. There are several variables that determines how information security is structured in an organization. According to Whitman and Mattord (2013), the first and most influential variable is the organizational culture. They saw it challenging, if upper management and staff does believe that information security is a waste of time and resources, as then information security will remain small and poorly supported. If information security is seen important and there exists a strong, positive view of it – information security is likely to be larger and well supported, both financially and otherwise. Whitman and Mattord (2013), saw it critical, that information security and the culture of an organization is aligned.

Investments in information technology constitute a large part of firms' discretionary expenditures, and managers need to understand the likely impacts and mechanism to justify and realize value from their information technology and related resources allocation processes (Mithas et al., 2012). Bardhan et al. (2004) discussed the challenge of information technology investment, and they pointed that the valuation of information technology investment is challenging as it is characterized by long payback periods, uncertainty and constantly changing business conditions. Traditional finance theories suggests that firms should use a discounted cash flow approach to analyze capital allocation requests. According to Bardhan et al. (2004) this approach does not properly account for the flexibility inherent in most information technology investment decisions. As an example, an information technology project may have a negative net present value when evaluated on a stand-alone basis, but still it will provide an option to launch future value-added services e.g. for application development or customer interaction. Without taking the option value of flexibility into consideration, firms will not be able to justify strategic investments in information technology that provide an accurate representation of strategic business value (Bardhan et al., 2004).

Goodhue and Thompson (1995) task-technology-fit theory was expanded by Karim et al. (2007) to organizational level, meaning that information technology will only have a positive impact on organizational performance if it matches the business processes. Karim et al. (2007) study also pointed, that despite significant investments in information technology a considerable number

of firms have not been able to derive full benefits due to their own inability to effectively deploy information technology in their business strategies. By ensuring that information technology is aligned with organization and that provides support for organization's business strategy is critical to business success (Bleistein, Cox, Verner, and Phalp, 2006). Duh et al. (2006) defined that the proper level of information technology investment is contingent on company's strategy and to other organizational resources which further interact with information technology and with the external environment. In addition to that, it is crucial to understand that the information technology itself does not bring any competitive advantage by itself; managers need to reengineer their core business processes from a customer perspective. Trkman (2010), made a research study about the critical success factors of business process management, and one part of the study considered the fit between business processes and technology. Trkman emphasized, that environment of an organization is an important contingent variable in the determination of the level of information technology investment (Trkman, 2010).

Information security investment are seen more challenging than information technology investments – both from the decision making point of view and for measuring the efficiency of them. According to Whitman and Mattord (2013), organizations of every size and purpose should prepare themselves for the unexpected. Every organization's ability to weather losses caused by an unexpected event depends on proper planning and execution of such a plan. Without proper plan, an unexpected event can cause severe damage to an organization's information resources and assets which may not be able to recover ever. Defining the value of security investments and efforts to find appropriate criteria, which are used to evaluate information security investments, is challenging. If investments in information security are evaluated alongside other investment projects, it may help to consider them on an equal footing, implying the use of similar methods of calculating the financial costs and benefits. Benefits that cannot be measured with quantitative values may mean less for company decision makers. This may lead to situation, that company's management see information security as an inhibitor to daily business operations if the investment is not well aligned with current business activities or is presented in financial terms not relevant to their agenda (Tsiakis and Pekos, 2008).

Because information security field is so young, there is not much empirical probabilistic data available. There are no information about who and when and by what means is going to attack. And even this information would be available, it would not apply to a specific organization and its unique security setting. There are many different known and unknown factors, which influence the prevailing level of information security in a specific setting. Wood and Parker (2004) listed these unknown factors as following:

- budget for information security,
- attitude and attentiveness of technical staff,
- time staff devote to information security,
- management's attitude about security and risk and,

- security policies and safeguards currently deployed

One challenging aspect is that information loss experiences are often kept as secret, as companies are not willing to cause risk for company's reputation by informing about a damage that a single information security incident has caused. Information security projects are challenging also due to the fact that they are not fitting into a traditional information-systems-related financial evaluation process. This is because they do not produce measurable loss reduction benefits, for example what losses the increased security may have stopped from happening.

Also Magnusson et al. (2007), discussed about the challenge of information security investment. They also saw it difficult to identify and quantify the benefit of information security investment, especially in translating it into economic terms and via that show its potential profitability. They indicated, that the problem to motivate information security investments economically is partly a consequence of the difficulties to generally produce correct calculations for information technology investments while comparing to traditional investments. Main reasons for this are:

- The lack of uniform working method to establish profitability.
- Information technology investments will often carry their expenses, but not their benefits.
- The general difficulty to identify and quantify the yield of information technology investments (Magnusson et al., 2007).

Information security investment distinguish from information technology investment by having specific challenges. Magnusson et al. (2007), listed following challenging questions what comes to the problemacy of information security investments:

- How can the argument be overcome that security investments do not generate any revenue?
- How can an information security investment be established as cost-effective, when the best that could happen is that "nothing" happens?
- How the optimal level of the total information security investments be can determined (Magnusson et al., 2007)?

Fenz et al. (2011) found that the lack of information security knowledge at the management level is one major reason for inadequate or nonexistent information security risk management strategies. Smith and Spafford (2004), came to a conclusion that information security risk management is one of the top ten challenges in information technology security. Vitale 1986; Bandyopadhyay and Mykytyn, 1999; Jung et al., 1999; Baker and Wallace, 2007 discussed about the domain expert dependence in their studies, meaning that best practice guidelines provides excellent knowledge about potential threats, vulnerabilities, and

controls, but without an information security domain expert, the company is not always capable of considering complex relationships between all the relevant information security concepts. This results to non-holistic information security approach, which endangers the company's operations. Baker et al., (2007) pointed the challenge of implementing abstract implementation suggestions related to risk mitigation. They came to a conclusion, that information security standards frequently only includes very abstract implementation suggestions for risk mitigations, which lead to inefficient risk mitigation strategies (Baker et al., 2007). Lander and Pinches, (1998) indicated the challenge of decision making related to information security investments. They pointed, that management decision makers, for example Chief Information Officer, has to cope with the task of selecting the most appropriate set of information security investment from a huge spectrum of potential information security investments. The results of existing decision making methods provide decision makers with inadequate or little intuitive and/or interactive decision support, which is not supporting them in identifying an appropriate risk versus cost trade-off when investing in information security solutions (Lander and Pinches, 1998).

To sum up the challenge of information security investment management, there are several uncertainties. There is no information against what the company should be secured to, no information what is the expected loss from unknown attackers against unknown vulnerabilities is after implementation of the security project – nor information about the expected losses, which could have been caused if the security project have not been implemented. There are also many intangible factors related to security projects (for example the risk of possible reputation loss), which make the financial analysis even more problematic (Wood and Parker, 2004). The measurement of information security investments is a business/organizational problem that must be formed and resolved in the context of organizations strategic drivers. Protecting information assets is technological and human management (management of security policy, users' compliance, proper hardware and software solutions and qualified stuff) (Tsiakis and Pekos, 2008).

3 PREVIOUS RESEARCH ABOUT INFORMATION SECURITY INVESTMENT

This chapter reviews the previous research on the information security investment and describes how the existing researches have approached it. This chapter also introduces the stage theory, which was utilized in this study as an approach to fulfill the identified research gap.

The importance of information security had been identified already a decade ago (Niederman et al., 1991). Small and large companies are investing heavily in information and network security technologies to minimize the potential dam-ages caused by security problem. Previous researches conducted by practitioners and academics have concentrated to different aspects. The researches have mainly approached the information security investment problems theoretically examining the optimal information security investment (for example Gordon and Loeb, 2002; Huang et al., 2008; Kort et al., 1999) and the efficiency of information security investment (for example Gordon and Loeb, 2006; Purser, 2004) (Karjalainen et al., 2014). Also other aspects of information security have been researched. Liu et al. (2011) studied the relationship between decisions made to knowledge sharing and investment, Ioannidis et al. (2011) had a utility-theoretic approach in their research related to information security investments, and Karjalainen et al. (2014) have studied the information security investments from the stakeholder theory perspective. Following chapters will introduce these different research approaches by describing the key findings of these researches.

3.1 The optimal information security investment approach

The researches with the optimal information security investment approach have determined different methods to evaluate and or to determine the optimal amount to invest on information security.

In 1999, Kort et al. developed two models to evaluate optimal company investment in information security. In the first model, the company has the possibility to invest in information security and decrease the possibility of losses from criminal activities and hence capable of building up a security capital stock. It means, that by these information security investments the discounted stream of reductions of criminal losses is equal to marginal security investment expenses. The second model considers the company's reputation. According to Kort et al (1999), the company that has been successful but not invested in information security is in a great danger of security breach, and at the same time increase the future criminal losses (Kort et al, 1999). Both these two models have an approach that decision-maker's goal is to maximize the net cash flow stream and that company can protect itself by investing in security equipment (Karjalainen et al., 2014).

Gordon and Loeb (2002) proposed an economic model that determines the optimal amount to invest to protect a given set of information. They based their study approach with the assumption that the decision maker of a company is risk-neutral. The key assumption of their study is that risk-neutral company will maximize its expected profit from security investments (Karjalainen et al., 2014). Gordon and Loeb (2002) model considers how the vulnerability of information and the potential loss from such vulnerability affect to the optimal amount of resources that should be dedicated to securing that specific information (Gordon and Loeb, 2002). The mathematical model demonstrates that the optimal amount to spend on information security never exceeds 37% of the expected loss resulting from a security attack, and it would typically be far less than even the expected loss from a security attack. Because extremely vulnerable information may be too expensive to protect, Gordon and Loeb (2002) suggest that a company may be better to off concentrating its efforts on information with midrange vulnerabilities. They further suggest that in order to maximize the expected benefit from investment to secure information, a company should spend only a small fraction of the expected loss due to security attack (Gordon and Loeb, 2002).

Huang et al. (2008) theory determines the security investment level that maximizes the utility of the investment. Their approach determines optimal level of investment while addressing multiple security threats and counteracting technologies (Huang et al., 2008). They offer several findings into information security practices, which are walked through in following. Huang et al. approach the optimal security investment with the assumption that the decision maker of a company is risk-averse (proposition 1.). This is the most significant difference to Gordon and Loeb (2002) approach, as they adopted a risk-neutral assumption. Huang et al. based their assumption to studies which have shown that companies which performance is above the industry average are usually risk-averse. Risk-averse decision makers are more willing to invest in-formation security to reduce company risks, but at the same time they do not see every security risks are worthwhile to protect from. Fiegenbaum and Thomas (1988) and Jegers (1991) also presented that risk-averse decision makers tend to have less capital constraints in decision making. Huang et al. (2008) saw a great po-

tential in a risk-aversion model of security investment, which could offer valuable managerial insight into process of how companies should make decision while investing in information and system security (Huang et al., 2008).

Huang et al. (2008) proposed the expected utility theory, which defines the optimum level of security investments (proposition 3). This specifically intends that until the potential loss from a security breach obtain certain level, the company is not worthwhile to invest any money in protecting against such a risk. They evaluated that optimal investment in information security does not always go up with the effectiveness of such investment. With these two proposition (1 & 3), Huang et al. (2008) suggest that:

"Managers should conduct careful evaluations of the vulnerabilities of their information systems and the potential losses in case of a breach before deciding whether specific investment to address these vulnerabilities is called for."

They proposed also the finding that the optimal level of security investment does not necessarily increase with one's aversion to risk (proposition 2). This proposition suggest that company decision makers should carefully consider the security risks against to other business risks in decision making process related to level of investment in information security. Huang et al. (2008) continued with the suggestion that for a firm trying to defend against targeted attacks, optimal security investment would increase with system vulnerability. Before determining the investments based on system vulnerability, a company should carefully identify its main information security threat (Huang et al., 2008).

Hausken (2006), used economic model under different scenarios to evaluate the relation between the optimal level of information security investment and the vulnerability of information. Hausken (2006) studied the effect of return assumptions on the optimal information security investment level, which concludes that the nature of returns is a critical factor in providing guidance in investment decision making process (Gordon and Loeb, 2006). Hausken (2006) proposed a four classes of security investment breach functions that have different characteristics from Gordon and Loeb (2002). Hausken (2006) introduced four types of marginal returns to information security investment, while Gordon and Loeb model defines only one. Wang et al. (2008) also extended Gordon and Loeb (2002) model. They work propose probability-based model to calculate the probability of insecurity of each protected resource and the optimal investment level with the help of two algorithms. The proposed API algorithm is based on a threat flow model that models the probabilistic flow of possible security breach on information systems. The proposed OSI algorithm is based on risk-neutral assumption that the optimal information security investment should maximize the total expected net benefit (Wang et al., 2008).

Matsuura (2003) argues Gordon and Loeb (2002) model to fail as it is based on a single decision variable. Matsuura (2003) proposed an extension for integrating the investment optimization with the insurance decision making Matsuura (2003). Also Tatsumi and Goto (2009) extended Gordon and Loeb

(2002) model. They argue Gordon and Loeb (2002) model not considering any aspect of dynamic theory (for example time value of money, or first mover advantage) and introduced a real options theory to achieve the optimal timing of the information security investment level. Key findings of their research indicates that positive drift of threat causes larger and later expenditure, but negative drift of threat causes lower and immediate investment expenditure. They also found out that the efficiency of vulnerability reduction technology encourages companies to invest earlier, which induces cost reduction. Tatsumi and Goto (2009) also mentioned the importance of knowing the form of vulnerability, as the effect of high vulnerability on timing and amount of the investment expenditure is mixed (Tatsumi and Goto, 2009).

Cavusoglu et al., (2008), analyzed the problem of determining information security investment level from decision theory and game theory perspective. They argued that traditional decision-theoretic risk management techniques are in-complete because of the problem's strategic nature and proposed game-theoretic approaches for the information security investment problem. They considered both sequential and simultaneous games between company and hackers and compared results along several dimensions such as the investment level, vulnerability and payoff from investment. Their study showed that the company realizes the maximum payoff when the company and the hacker play a sequential game with the company and the hacker acts as a follower. In sequential setting company must communicate and commits its strategy to the hacker. If there is no commitment and communication, the company still gets higher payoff when the company and the hacker play a simultaneous game compared to when the company assumes that the hacker is nonstrategic and utilizes decision theory approach to determine investment level. Their study also indicated that if company learns from prior observations of hacker effort and utilizes these to estimate the future hacker effort, then the gap between results when decision theory is used and those when they play a simultaneous game approach diminished over time. Cavusoglu et al., (2008) theory approach assumes that vulnerability function is known both to the company and to hackers. They argued model to be more realistic, when security investment problem incorporate both targeted attacks as well as random attacks – i.e. the impact of uncertainty about the vulnerability function is taken into account (Cavusoglu et. al, 2008).

According Bandyopadhyay et al. (2012), hackers evaluate potential targets to identify poorly defended companies to attack by creating competition in information security between companies that possess similar information assets. Bandyopadhyay et al. (2012) utilized a differential game framework to analyze the information security investment decisions in this targeted group of companies. Their study analysis showed that information security planning should not be kept an internal company-level decision, but also incorporate the actions of those firms that hackers considers as potential alternative targets. They also showed, that in order to achieve cooperation between companies, the company with highest asset value must take the lead and provide appropriate incentives to elicit participation of the other company (Bandyopadhyay et al., 2012).

3.2 The efficient information security investment approach

The researches with the efficient information security investment approach have determined different measurements to evaluate and or to determine the effectiveness of information security investment. Traditionally, the effectiveness of a security investment is presented with return of investment (ROI) calculation (Gordon and Loeb, 2006; Purser, 2004; Davis, 2005; Hausken, 2006). This chapter will walk through the key finding of these approaches.

When evaluating the efficiency of information security investment, Gordon and Loeb (2006) focused on three different aspects in their ROI model: (1) How much should an organization spend on information security, (2) How should an organization allocate their information security budget to specific security activities, and (3) what is the economic cost of information security breaches? According to Karjalainen et al. (2014) the ROI-type metrics have the same underlying assumption as studies in optimal information security investment approach (Gordon and Loeb, 2006; Huang et al. 2008), because the higher the expected benefit / the less the expected costs, the higher the ROI (Karjalainen et al., 2014).

There are several different studies done related to return on investment in information security investment. Purser (2004), Davis (2005), Mizzi (2004) and Sonnenreich et al. (2006) have presented an extended ROI models. Purser (2004), discussed the challenge of ROI with information security investments. From information security perspective, ROI definition is challenging, as ROI kind of definitions do not take account the risk mitigation – whereas mitigated risk is in many senses the primary deliverable of the information security process. Purser (2004) has argued, that ROI provides only a partial image of the true return of investment. Purser (2004) discussed that, ROI does not consider the effect of the change in risk associated with business initiatives. Also Karjalainen et al. (2014) argue that ROSI model provides only partial image of the true return on investment. Purser (2004) states;

"The information security process add value to the enterprise by reducing the level of risk that is associated with its information and information systems."

Reduced risks profile is valuable to the company and thus should be seen as a return on the investment that made it possible. Purser (2004), defined a new term, the Total Return on Investment (TROI) in order to improve ROI of security management process. TROI includes the financial impact of the change in risk. According to Purser (2004), using TROI instead traditional ROI calculation enables to put information security management initiatives on the same level as other business initiatives as security management initiatives can be required to produce positive TROI. Still, there is one exception; initiatives which must comply with legal or other regulatory requirements must go ahead despite the TROI status. Purser (2004) defined TROI as is presented in Figure2.

$$\text{Total Return on Investment} = \frac{\text{Generated revenue} + \text{Generated cost savings} - \text{Value of change in risk}}{\text{Investment}}$$

FIGURE 2 Purser (2004) Total Return on Investment

Purser (2004) states that the TROI provides more accurate understanding of the overall business benefit of security investment as it contains a component that reflects the associated risk. This means, that if risk is increased as a results of the investment, this will result in a decrease of the TROI, whereas initiatives that mitigate risk will be associated with the negative value for the change in risk and thus add to the TROI. Purser (2004) differentiated the information security related initiatives to tactical and strategical initiatives. Tactical ones are usually driven by short-term business opportunities and enable company to quickly realize the associated business benefit. Strategical security initiatives are driven by the requirements which are targeting to achieve a certain risk pro-file for the company. The aim of those initiatives is to achieve a positive TROI and mitigated risks. Purser also discussed about the importance of strategic approach and careful planning of information security management process. The security management process should be business-driven and integrated to existing business framework as smoothly as possible (Purser, 2004).

Davis (2005) developed a ROSI, which is defined as the calculation of the financial return from an investment in security. Sonnenreich et al. (2006) extended ROI model to consider risk exposure and risk mitigation. Sonnenreich et al. (2006) ROSI model is illustrated in Figure 3. Mizzi (2010), extended ROI model to analyze the mechanics of an information security program. Mizzi's (2010) return on information security investment (ROISI) model attempts to set up a threshold value for the information security expenditure. ROISI model considers different concepts ("Viability of Expenditure", "Motivation to Attack" and "Successfulness of an Attack") and their relationship. According to Mizzi (2010), organizations should adopt the model and adapt it to their circumstances by defining relationship among these variables according to the nature of their organization (Mizzi, 2010). Mizzi indicates that an organization should not invest more to information security than the total cost of the information assets that may be lost by a security breach (Karjalainen et al., 2014).

$$\text{ROSI} = \frac{(\text{Risk Exposure} * \% \text{ Risk Mitigated}) - \text{Solution Cost}}{\text{Solution Cost}}$$

FIGURE 3 Sonnenreich et al. (2006) Return on Investment for Security Investment (ROSI)

Also Magnusson et al. (2007) challenged the ROI model(s) suitability for information security investments. Their study objective was to investigate the theoretical conditions for information security to become a part of value creation. As a result of their study, they argued economical models to be with limited value in calculating value creation or effectiveness. They saw that the fundamental reason is that the economic models are not stated explicitly, which decreases their practical usefulness. They also argued that one further difficulty to apply ROI models is that they all value advantage in terms of net benefit, which cannot easily be transformed into cash flow (Magnusson et al., 2007).

3.3 The other approaches to information security investment

This chapter will walk through different than optimal or efficient research approaches to information security investment. Liu et al. (2011) studied the relationship between decisions made to knowledge sharing and investment in information security. Liu et al. (2011) indicated that the nature of information assets possessed in the company – either complementary or substitutable – plays a crucial role in influencing to investment decisions. In case of complementary assets, the firms tend to have a natural incentive to share security knowledge and due to that no external influence to induce sharing is needed. In case of substitutable assets the firms tend not to share security knowledge in equilibrium, despite the fact that it is beneficial. Liu et al. (2011), recommends firms to consider whether the information they are trying to protect is of value to a hacker itself, or whether its value is realized only if the firm's information is combined with the information stored at another firm. The complementary cases, where the information provides value to hackers only if it is combined with other company's information, provides a natural incentive to the company to collaborate with each other on security intelligence, as sharing the security knowledge makes both firms more secure. In substitutable cases, it is socially optimal for two firms to share security knowledge, but in equilibrium the firms engage in a sharing outcome to dilemma where each firm would like to its partner to share, but the dominant strategy is not to share. This is both individually and socially harmful for the firms (Liu et al., 2011).

Ioannidis et al. (2011) had a utility-theoretic approach in their research related to information security investments. Their key target was to determine the optimal timing of interventions in information security management. By utilizing utility theory, Ioannidis et al. (2011) derived the limiting condition under which, given a potential or realized risk, a decision to invest, delay or even abandon can be justified. Their focus was on decision making in deferring costly deterministic investments, when the costs associated with future security vulnerabilities are uncertain. Ioannidis et al. (2011) outlined an investment func-

tion with irreversible fixed costs which adduce a rigidity into the investment decision making. Further, the rigidity causes delays in the implementation of security measures, which results in cyclical information security investments, while the decision maker(s) determines the optimal investment horizon.

Karjalainen et al. (2014) have studied the information security investments from the stakeholder theory perspective, where they evaluated through in-depth case studies the key participants' information security investment decision making and how that was affected by their values. They found out that information security investment decision making process involves more than identifying the optimal investment level or justifiable return of investment. Based on their empirical findings Karjalainen et al. (2014) formulated a preliminary stakeholder values theory of information security investment. Their theory is both descriptive and instrumental. Theory is descriptive, as it identifies the key stakeholders, describes their key values and identifies stakeholders' value orientations towards information security investment decision making. According to theory information security investment decisions are mainly driven by three different stakeholders (end users, information security specialists, and organizational decision makers). All these different stakeholders have different values, and if those are satisfied, they support information security investment. End users are willing to support information security investments, if it does not re-quire additional effort or new technical skills. Investment must also be clearly connected to their work-related activities. Information security specialists value the technical quality, but at the same time they prefer tradeoffs between the users' values and technical quality. Organizational decision makers value the compatibility of information security investment to organizational environment and its usability for the organization.

Karjalainen et al. (2014) theory is instrumental as it provides guidelines for improving the success of information security investment. The key implication of the theory is to recognize the key stakeholders and understand that they have different values and expectations for information security investments. The study identified that all stakeholders have one common expectation for information security investments, which is the efficiency. For that reason, it is critical to communicate to stakeholders, that information security investment does not require the users learn new technical skills and its implementation is as harmless as possible for users. Still due to different core values of different stakeholders the usability of information security investment must be presented differently depending on the target audience. Karjalainen et al. (2014) found out that the stakeholders have different information technology security risk opinions. These differences are critical to evaluate and understand, when promoting information security investment, Karjalainen et al. (2014) stated:

"Information Technology security risks related to the information security investment should be communicated to the different stakeholders in the manner that suits their information technology security risk mitigation values, such as risk minimization, risk taking, personal accountability, and worst-case scenario thinking."

The study also identified, that in-formation security specialist should recognize that users and high-level decision makers have different drivers for their decision making as security managers, and that users do not evaluate the information security investment technical implementation with knowledge of expertise. Finally, the study defines the best way to influence to decision making by recommending showing to the decision makers the importance of information security investment, users' need for the information technology for work activities, and information about how much extra effort is needed due to solution implementation (Karjalainen et al., 2014).

To summarize the previous research about the information security investments, it can be stated that previous research have not addressed why information security investment decisions fail in decision making process, and thus cannot explain the reasoning behind the decision making. The previous researches with the optimal information security investment approach have determined different methods to evaluate and or to determine the optimal amount to invest on information security, and the researches with the efficient information security investment approach have determined different measurements to evaluate and or to determine the effectiveness of information security investment. Liu et al. (2011) studied the relationship between decisions made to knowledge sharing and investment in information security, whereas Ioannidis et al. (2011) utilized an utility theory, from where they derived the limiting condition under which, given a potential or realized risk, a decision to invest, delay or even abandon can be justified. Karjalainen et al. (2014) studied the information security investments from the stakeholder theory perspective, where they evaluated through in-depth case studies the key participants' information security investment decision making and how that was affected by their values. This study address the research problem why information security investment decision fail by understanding the information security investment decision making process and by understanding the decision makers' experience of decision making in terms of stages. The stages have stage-specific factors, which address the research problem. Following chapter describes the stage theory model utilized in this research.

3.4 Stage theory

Van De Ven and Poole (1995) stated, that process is used as a sequence of events describing how things change over time and why they change in this way. According to Schwarzer (2008), stage theorists' have made an attempt to consider process characteristics by proposing a number of qualitative stages. The stage is a theoretical construct, which is useful in understanding the development path for how behavior evolves over time. Stage theories have been used to investigate human behavior, for example health behavior (Weinstein et al 1998). According to Weinstein et al (1998), every stage theory needs a set of rules that

assign each individual to one of the limited categories. By defining the stages and specifying their sequence are initial steps towards demonstrating the stage process.

Chowdhury (2002) defined, that there are three critical requirements of a stage theory, which are incident, event and concept. Incident is a recurring activity, which can be empirically observed in one or more stages of the process model. Incident can be comprised using terms such as actions, indicators and occurrences. An incident change in terms of form, direction, quantity, quality or state must be compliant to direct observation (Van de Ven, 1995). Event can be seen as an abstract conceptual entity, which explain the pattern of critical incidents and their temporal order. An event is a construct, which are not compliant to direct observation and thus events cannot be seen, heard or felt; they are inferred. Concept describe the progression of the whole phenomenon. In order to be able to identify events to be observed and incidents to be recorded, it is important to identify a core concept that represents each stage of the process model (Chowdhury, 2002).

Stage theory seem appropriate for this study as information security investment decision making process involves dynamic change, and any dynamic phenomenon can be seen as a combination of sequential events over period of time and can therefore be fruitfully viewed as a process (Chowdhury, 2002). Stage theory perspective gives an approach, which can explain how and why a chronology of occurrences play out over time and finally lead to rejected decision in information security investment decision making process. The status of each case company's information security management is described with the stage model in chapter 5 by describing the process for managing information security investments from initializing the investment proposal until its decision making.

4 RESEARCH METHODOLOGY

This qualitative research utilized a research strategy where theory is built from case studies. It involves using one or more cases to create theoretical constructs, propositions and/or midrange theory from case-based, empirical evidence (Eisenhardt, 1989). Case studies are rich, empirical descriptions of particular instances of a phenomenon that are typically based on a variety of data sources (Yin, 1994). This qualitative research utilized a data collection method named an open interview. The research data was analyzed utilizing the method called inductive content analysis. An inductive approach was chosen due to fact that there is not enough former knowledge about the phenomenon. This chapter defines in more detail both the concept of the qualitative research, theory building from cases, open interview, content analysis, and also how the empirical research within the study was performed and analyzed.

4.1 Qualitative research and theory building from cases

The main principle of the qualitative research approach is to be as descriptive as possible (Hirsijärvi et. al., 2009). Qualitative research methods are both descriptive and inferential in character. According to Gillham (2010), description and inference are necessary in scientific research. One may have significant statistical results, but those have to be described and interpreted: "Tact's do not speak for themselves – someone has to speak for them" (Gillham, 2010). Qualitative research methods focus primarily on the kind of evidence (what people tell you, what they do), that will enable one to understand the meaning what is going on. One great strength of qualitative research methods is that they can illuminate issues and turn up possible explanations (Gillham, 2010).

Qualitative research is always related to certain time and place. The purpose of the qualitative research is to find new, realistic and fact based information about the research object. It is a diverse and comprehensive method for gathering information in natural conditions. In interview the information is

gathered from interviewee(s), and for that reason it is typical that interviewees' personal aspects affect to the study results. Qualitative research aims to gather information about specific occasion (single case) or from small group of cases (multiple cases) which are related to each other (Hirsijärvi et al., 2009). Gillham, (2010) specifies that qualitative research methods enable:

- To carry out an investigation where other methods – such as experiments – are either not practicable or not ethically justifiable.
- To investigate situation where little is known about what is there or what is going on. More formal research may come later.
- To explore complexities those are beyond the scope of more "controlled" approaches.
- To get under the skin of a group or organization to find out what really happens – the informal reality which can only be perceived from the inside.
- To view the case from the inside out: to see it from the perspective of those involved.
- To carry out research into the processes leading to results (for example how reading standards were improved in a school) rather than into the "significance" of the results themselves (Gillham, 2010).

According to Eisenhardt (1989), building theory from case studies is a research strategy that involves using one or more cases to create theoretical constructs, propositions and/or midrange theory from case-based, empirical evidence. Case studies are seen as rich, empirical descriptions of particular instances of a phenomenon that are typically based on a variety of data sources (Yin, 1994). The central notion of this research strategy is to use cases as a basis from which to develop theory inductively. Theory can be seen as emergent as it is situated in and developed by recognizing patterns of relationships among constructs within and across cases and their underlying logical arguments (Eisenhardt & Graebner, 2007). Eisenhardt (1989), defined that the central to building theory from case studies is a replication logic. It means, that each case serves as a separate experiment that stands on its own as an analytic unit. Multiple cases as discrete experiments serves as replications, contrasts, and extensions to the emerging theory (Yin, 1994). Instead of using only single-case within the study, multiple-case studies typically provides a stronger base for theory building – meaning, that theory is better grounded, more accurate, and more generalizable. Multiple-cases also enable comparisons in order to clarify whether an emergent finding is characteristic to a single case or consistently replicated by several cases (Eisenhardt, 1991).

Yin (1989), emphazised that in order to gain good case study results, research design need to be well planned. Yin (1989), stressed following five steps in research design phase :

1. Research questions

2. Research propositions (if any)
3. Analysis unit for research propositions
4. Logic how the research results are connected to research proposition
5. Criteria for analyzing the research results

4.2 Open interviews as a data collection method

Case studies can accommodate a rich variety of data sources, including interviews, archival data, survey data and observations. But because research incorporates more cases and moves away from everyday phenomena such as work practices to intermittent and strategic phenomena such as acquisitions and strategic decision making, interviews are easily selected as the primary data source. Interviews are a very efficient way to gather rich and empirical data (Eisenhardt, 2007). According to Järvinen & Järvinen (2011), researcher need to be able to state good questions, and also has an ability to analyze the responses. Researcher should have proper understanding about the study subject, in order to make questions in changing environment. Researcher should also have a good ability to listen and also to read between the lines. Researcher should be flexible and able to change his study plan if needed – but still able to remain with the study subject. Researcher should also be able to receive and recognize contradictory information (Järvinen and Järvinen, 2011).

This qualitative study utilize an open interview as a data collection method. Interview is an interactive conversation between two or more people where questions are asked by the interviewer to elicit facts or statements from the interviewee. The interview can be divided to three different types. An open interview is the most informal type of the interview. The questions are open and the response choices are not specified beforehand. Open interview is a conversational kind of situation, where exist a certain topic. Open interview is guided through according to study themes. People selected to participate to an interview, are the ones who have the best knowledge about the study subject. The amount of interviewees can be increased by searching them during the study process, in order to gain best possible understanding about the subject. This phenomenon is called as a snow-ball effect. In a structured interview the exact questions and often also the answer choices are defined ready before the interview. A structured interview conducts according to the form and all the interviewed persons respond to same questions. In structured interview, the questions are related to research hypothesis. Third type of the interview is the theme interview. This interview method is also called as a semi-structured interview. Theme interview conducts according to predefined themes, but the interviewer has also some room to the changes. Theme interview is very close to the open interview, and the interview includes both open and closed questions. The themes are same to all interviewed persons (Järvinen and Järvinen, 2011).

4.2.1 Preparation of the open interviews, execution and analysis

The research material of the empirical part of the study were gathered by interviewing pre-selected people having a key role in making information security investment management decisions. The target of the interviews were to gather proper information to produce theory propositions which could answer to the research question. The people interviewed within case study represented four different cases. Cases or interviewed people are not detail level identified in this study due to the information sensitivity.

The Case A is a company providing frozen vegetables, frozen ready meals and fresh fish and its products are renowned for their taste and home-grown content. Largely based on Finnish raw materials, the frozen vegetables and frozen ready meals are produced at Western Finland, and frozen pizzas at Central Finland. Company's product range is constantly developed to suit Finnish tastes, meet nutritional recommendations and respond to changing trends in eating habits. The Case B represent a large-size Finnish municipality union, which consist of one large size town and seven smaller municipalities around of it. Case B is located in the western Finland. This specific municipality union has cooperative organization for the information management, and for example all the eight members of the municipality union have approved and implemented the one common information security policy. The Case C is a privately-owned medium-sized company, which key business is to provide customer services as outsourced service for small- and mid-size companies. The business processes of the case C are heavily tied to information technologies, and its services are provided via different channels, for example via phone, chat, internet and email. It provides its services to circa 200 different clients in Finland. The Case C is located in western Finland. The Case D is a privately-owned small-sized company, which key business is to provide information technology solutions both for the consumers and businesses. Company's product portfolio contains for example following products: web services (customer can set up its own website or online store), cloud services (virtual data centers, virtual servers, data back-up) and data center services (maintenance and supervision of customer virtual servers). Also the Case D is located in western Finland.

The case organizations were contacted in November 2014 via phone and email. Also other possible case organizations were contacted, but these defined case companies were selected on the basis of their own motivation to the research subject. The interviews were started in December 2014 with the plan, that from case organization A will be interviewed four persons, from case organization B three persons, from case organization C two persons and from case organization D one person. As targeted in the beginning of the study phase, the amount of the interviewees increased during the empirical part of the study, and the total amount of interviewees is presented in Table 1. The amount of interviewed persons per Case Company.

TABLE 1 The amount of interviewed persons per case companies

CASE COMPANY	AMOUNT OF INTERVIEWED PEOPLE
CASE A	5
CASE B	6
CASE C	2
CASE D	1

All the interviews were open interviews, supported by very flexible framework which is presented in Appendix 1.

All the interviews were recorded permitted by the interviewees. All the interviews were littered afterwards in order to proceed to the data analysis phase of the study. The purpose of the analysis was to analyze the gathered study data and produce theory propositions for research problem - why information security investment decisions fail? Theory was developed by distinct propositions in such a way, that each is supported by empirical evidence from at least some of the cases.

4.2.2 Progress of the study and background information about the interviewees

Like described earlier, the case organizations were contacted in November 2014 via phone and email. Also other companies were contacted, but due to lack of their own interest and motivation they were not selected to the study. With the selected case organizations, there were discussed who and which roles from the organization could be contacted and interviewed. Target was to find people with roles and responsibilities, in where they involve with information security investment management decision making. In the beginning of the study phase, there were contacted eight persons from the case organizations. With these selected persons, it was agreed an individual time for interview. Interviews were executed in interviewees' premises or via phone, and time reserved for one interview was approximately one hour. Interviewees were confirmed, that interview results will be treated sensitively and case organizations, nor interviewees will not be identified within the study. All the recorded interview material were promised to be destroyed after the analysis work. One additional target of the interviews was to get further contacts who could be interviewed within the study. Due to that, in total 14 people were interviewed along the study. Interviews were performed within the time scale January – February, 2015. Analysis of the interviews were started right after each interview. Following Table 2 Interviewees' roles in organization defines the interviewees' role in the case organizations.

TABLE 2 Interviewees' roles in organization

INTERVIEWEE	CASE	ROLE
1	Case A	Risk Manager
2	Case A	Chief Financial Officer
3	Case A	Chief Information Officer
4	Case A	Real Estate Manager
5	Case A	Controller
6	Case B	Chief Information Officer
7	Case B	Information Security Manager
8	Case B	Investment project manager
9	Case B	Chief Financial Officer, municipality
10	Case B	Project Manager
11	Case B	Manager, Internal audits
12	Case C	CEO
13	Case C	Chief Technical Officer
14	Case D	CEO

4.3 Content analysis as a data analysis method

Content analysis is a method of analyzing written, verbal or visual communication messages (Cole, 1988). Content analysis method can be used to analyze both qualitative and quantitative data, and it can be used both an inductive and deductive way. Lauri & Kyngäs (2005) recommended, that if there is not enough former knowledge about the phenomenon or if knowledge is fragmented, inductive approach should be chosen. This study analysis utilized an inductive approach.

Inductive content analysis process contains three different phases; open coding, creating categories and abstraction. In open coding, notes and headings are written in the text while reading it. The written material is read through several times, and as many headings as necessary are written down to describe all aspects of the content (Hsieh & Shannon, 2005). The headings are gathered and grouped expressions are freely generated at this stage (Burnard, 1991). After open coding, the lists of grouped expressions are created under higher order headings. The purpose of this is both to reduce the number of categories in abstraction phase by collapsing those that are similar to each other and to provide means of describing the phenomenon, to increase

understanding and to generate knowledge (Cavanagh, 1997). After creating categories phase, the abstraction starts. In abstraction each category is named using content-characteristic words. Categories with similar incidents and events are grouped together as main categories (Kyngäs & Vanhanen, 1999). The abstraction phase can continue as far as it is reasonable and possible. Table 3 Content analysis illustrates how the study data is processed thorough the content analysis phases.

According to GAO (1996), the analysis process and the results should be described in sufficient detail so that readers could get proper understanding how the analysis was carried out. Dey (1993), defined that creating categories is both empirical and a conceptual challenge, as categories must both be conceptually and empirically grounded. In order to succeed in content analysis, the researcher must be able to analyze and simplify the data and form categories that reflect the subject of the study in reliable manner (Kyngäs & Vanhanen, 1999). In order to increase the reliability of the study, it is necessary to demonstrate a link between the results and data. This study utilized an authentic citations to increase the trustworthiness of the research and by that points out to readers from where or from what kinds of original data categories are formulated. Authentic citations are presented in chapter 5. Study Findings and Theory Propositions.

Table 3 Content analysis

Original expression	**Headings**	**Grouped expression**	**Category**	**Main category**
...we cannot define the value of information security investment. It should be evaluated from risk management point of view. So far, there has not been any risk related to information security.	capability to define investment with business arguments	capability to define	Methods and capabilities to define and argue investment proposals	Information security competence to define and argue information security investment proposals.
…the arguments for IS investment are not enough – investment is not seen worthwhile – company prefers to take the risk.	capability to argue with sufficient reasoning	capability to argue		
Small investments are more easily put through	small investment are easy to get approval	capability to define		

…there are no substance level knowledge in decision making level. Decisions are not based on knowledge, and decision makers are no able to understand their decisions' consequences.	sufficient subtance knowledge	sufficient substance knowledge	Sufficient information security specific knowledge	
…decision is made on the basis of the maturity, common language and common knowledge about the investment. All these things affect together. Sometimes the criticality of the investment proposal remains unclear.	different level of knowledge used in analyzing the need for investment	different level of knowledge		
…substance knowledge about the Information Security is very low. That tied with low amount of resources put a lot of pressure to IT department.	no sufficient resources with substance knowledge	sufficient substance knowledge		
…information Security investment are not approved / implemented, because they cause usability issues among the employees; e.g. encryption of laptops, email encryption.	IS investment is seen to cause usability problems	sufficient substance knowledge		

5 STUDY FINDINGS AND THEORY PROPOSITIONS

This chapter presents the stage models, which are defined on the basis of the empirical findings of the study, and describes shortly how the information security investment management is organized in each case study company. This chapter also presents the study findings in detail, and theory propositions and related sub-propositions, which are supported by an authentic citations to increase the trustworthiness of the research. The theory propositions and study findings, are both categorized according to the stage model phases. The theory propositions comprise a theory framework which affect behind of the information security investments decision making process through the stages: initialization, definition and decision making.

5.1 Within case analysis of the information security investment process

The status of each case company's information security management is described with the stage models by describing the process for managing information security investments from initializing the investment proposal until its' decision making with stage model. In each case company, stage model contains following process stages:

1. Initializing of Information Security Investment Proposal,
2. Definition of Information Security Investment Proposal,
3. Information Security Investment Decision Making and,
4. Decision (Rejection).

Like defined, stage theory perspective gives an approach, which can explain how and why a chronology of occurrences play out over time and finally lead to either rejected decision in information security investment decision making process. Stage models contain different phases, which are illustrated with or-

dered stages. Each ordered stage has stage specific influential factors, which are defined in figures. Influential drivers explain things that are important in each stage, and which affect to managing the investment proposal. There are also defined, which sources could initiate the information security investment proposals (in stage Initializing of IS investment proposal), and who are the key stakeholders both in Defining the information security investment proposal and in IS Investment decision making phase. The arrows between stages illustrates changing from one stage to another. In the first stage, the information security investment proposal is initialized. It means, that an idea for investment proposal can be initialized by different stakeholders, as illustrated in following stage models. In initializing phase, the investment proposal is evaluated by information security responsible stakeholders, who considers is it further processed to second stage of the process or is it rejected. If the investment proposal is seen reasonable and valuable, it is moved to next phase where the definition of the information security investment proposal starts. In the second phase the investment proposal is detail level defined and evaluated by relevant stakeholders. They can both reject the proposal at this stage or prepare it for the management decision making. In the last stage of the process, the investment proposal is managed by the stakeholders who either reject or approve the investment. Investment proposal is presented to decision makers by relevant stakeholder, whose main target is to argue the value of the investment proposal to the business operation and organization.

The Figure 4 illustrates an information security investment decision making process of the case company A. The case A is a company providing frozen vegetables, frozen ready meals and fresh fish and its products are renowned for their taste and home-grown content. There are approximately 350 employees using information technology within the company. In general, the company A has a relatively slight information security policy. It defines the password policy, which seem to be well implemented in the company. Company A has also invested in employees' awareness program, which aims to increase the awareness about the information security. It is a web based learning, which does include also a test for each individual employee. Company A has taken also other actions which improve the level of information security. It has taken into use the Microsoft SharePoint application and discontinued to use old file system, which lacks of proper admin control. It is also in process of upgrading its cash management solution, which is outsourced from external service provider.

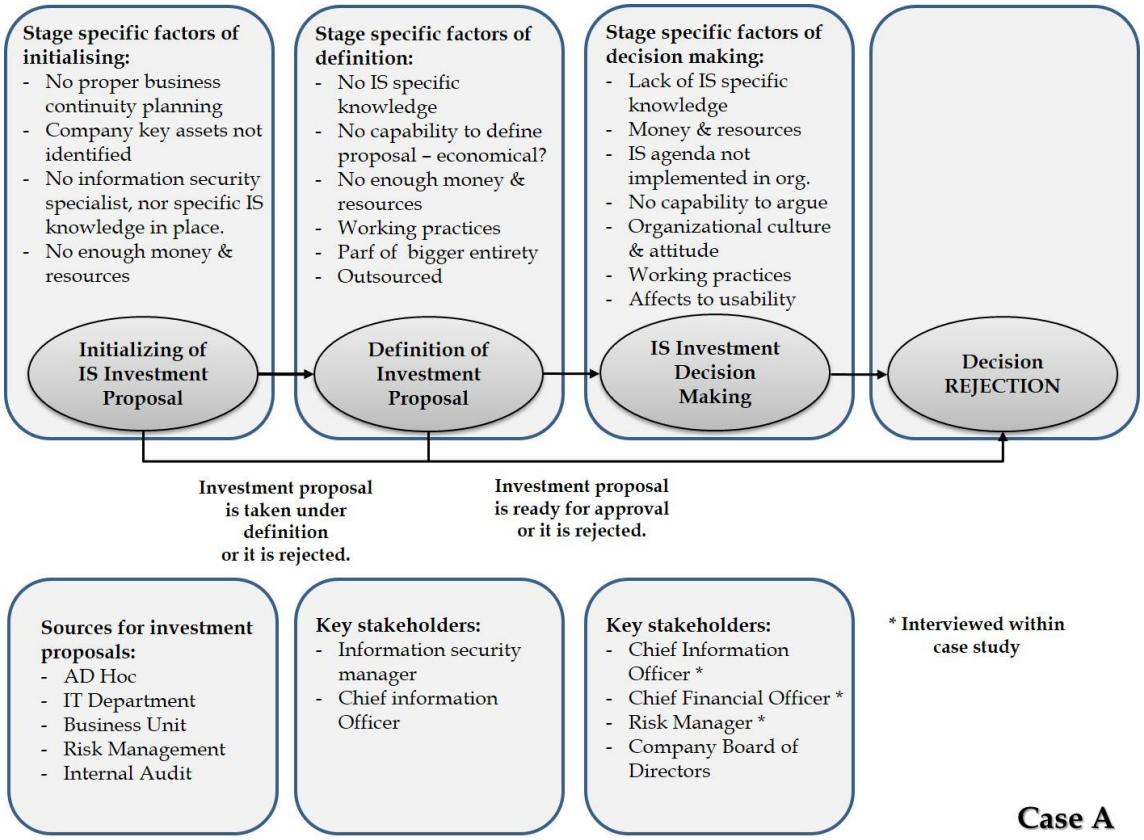

FIGURE 4 Case Company A, information security investment management process.

In a case company A information security investment decision making, following roles are involved: Chief Financial Officer and Chief Information Officer. In case of high expenditures, the board of directors process the decision making. Also other relevant roles can affect to the decision making, for example Risk Manager. Information security investment proposals can be initiated by information technology department, business units, risk management or internal audits. Also other individual sources exists. The foundation for proper information security investment management lacks non-existing business continuity planning, which in concrete level is visible in a fact that the company's key assets are not identified. Another challenge is that case company A does not have information security resources with specialist level skills. They also lack of time and resources to process further valuable information technology or information security investment proposals, and to follow up existing information security trends. They also find it challenging to define information security investment proposal in a way that they can argue the economic value of it. Information security investments are rarely initiated by risk management, meaning that scenario modeling is not utilized in the company, at least from information security management perspective. During the past eight years, there have been only few information security investment proposals, as most of the information security specific investments are part of bigger entirety, like upgrading the

computer operating system from Windows XP to Windows7. Also many information security specific services are outsourced, for example firewall and antivirus programs. When the information security investment proposals ends up to the stage of decision making, there are several drivers which affect to the decision making.

Most often the information security investment is rejected due to unavailable time and resources. This altogether indicates the level of implementation of the information security agenda in the company. It seems also that organizational culture is not information security oriented and attitude towards it is at least slightly immature. One concrete level example is that the value of encrypting the laptops is not seen critical for the business (because of the usability problems), though the Windows7 operating system is very easily hacked and severe damage could be caused to the business continuity. Organizational culture and attitude towards information security management is seen also in how well the company has considered its business continuity. So far, the company A has not identified what are the key assets of the company – or what kind of information could severely damage the company's brand and image, in the case of information leakage. According to the study results, there also exists challenge to argue the information security investments. As the information security investment cannot be economically presented, the proposal easily lacks proper arguments. Proper arguments are difficult to state, as there does not exists specialist level knowledge about the information security.

The Figure 5 illustrates an information security investment decision making process of the case B. The case B represent a large-size Finnish municipality union, which consist of one large size town and seven smaller municipalities around of it. Case B is located in the western Finland. This specific municipality union has a cooperative organization for the information management, and all the eight members of the municipality union have approved and implemented the one common information security policy. Each municipality have its own information security manager. They do have also one common policy for mobile phone security. In this municipality union, there are approximately 600 different information technology systems in use, and circa 35000 users. Information technology services are outsourced from approximately 70 different external service providers, from which the major ones also actively take part to the operational development actions. According to the study interviews, the most important information technology investment during the year 2015 is the competitive tendering of the existing service agreements. During the past years, there have been done several information security investments – either specific ones or investments which have partially improved the level of security. Upgrading the operating systems from Windows XP to Windows7, during which also the Windows XP support was separately continued are examples of these kinds of investments.

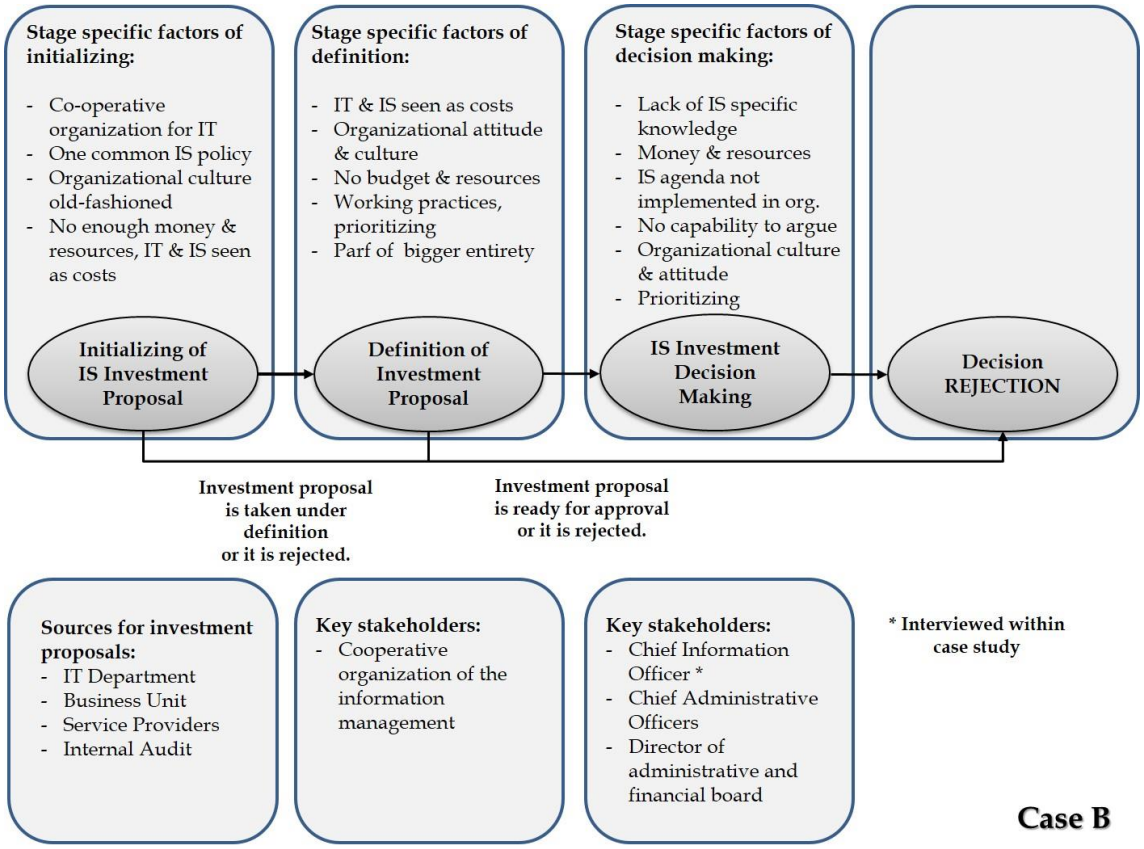

FIGURE 5 Case Company B, information security investment management process.

In the case B, the cooperative organization of the information management has a responsibility to define information security investment proposals to administrative and financial board of directors. There are several roles and organizational representatives, which are involved within the information security investment decision making process, for example; Chief Information Officers, Information Security Managers, Chief Financial Officers, Chief Administrative Officers, Director of administrative and financial board and Director of internal audits. Information security investment proposals are initiated by various different stakeholders. Different business units initialize ideas, internal audits propose development ideas and also deviations to existing policies and procedures, service providers come up with development ideas and of course information technology department follows-up existing trends and develops constantly the information infrastructure of the municipality union to meet laws and regulations, and among all - process the ideas further to actual investment proposals.

There are several challenges, which affect to initializing stage of the information security investments. In general, information technology is still seen mainly as costs and attitude towards information security is immature – at least by some members of the municipality union. According to the study interviews,

there are lot of room for cultural change and the maturity of information security is in a quite low level as a whole. This indicates, that organizational culture does not support information security. Information technology costs are circa 2% of municipality union operational costs, which are seen very low and which should be increased in order to enhance the operation of municipality union. It was also stated that in municipalities management level there exists no knowledge, nor clear statement who has the ultimate responsibility of the information security.

Most often information security specific requirements are bundled together with other information technology investments, and this is seen workable way to get investment proposals approved. There are also information security specific investments, which are evaluated towards the existing policies. In stage of decision making, several challenges exists. Organizational culture naturally affects also in decision making phase. Information security specific issues are seen differently in different municipalities and municipalities are concerning the investments proposals different way. This partially is due to unawareness about the information security specific issues meaning that there are not enough information security specific knowledge at decision making level. Also the attitude towards information security specific investment affects to decision making, especially in municipalities where information security is in contemptible agenda. There are also lack of capabilities to utilize economic arguments for information security investment proposals, and costs versus the achievable value is challenging to argue. One challenge seems to relate to the budgeting. If and when there are no separate "not ear-marked" money for information security specific investments, they are challenging to get approved as decisions are made under strict budget control. Some investments costs are divided according to municipalities' population, which causes also challenge as some municipalities are not willing or able to pay high costs. In decision making stage there exists also challenge related to prioritizing practices. Decision makers may have individual priorities, and investment proposals might be managed in some cases in non-relevant way. There exists no clear principles how the investment proposals should be evaluated and prioritized towards each other. This makes existing prioritizing practices questionable. In municipality level, also political aspects affect to decision making. Decisions might be evaluated for example from the perspective how much the implementation of the investment proposal affect to employment level. In stage of decision making, it is also seen critical that the investment proposals are presented with the same language as with the decision makers' use – meaning that investment proposals cannot contain too specific technological information. Related to that, it was also pointed that information security investment proposals are more easily approved if they are presented as a risk.

The Figure 6 illustrates an information security investment decision making process of the case company C. The case company C is a privately-owned medium-sized company, which key business is to provide customer services as outsourced service for small- and mid-size companies. The business processes of the case C are heavily tied to information technologies, and its services are

provided via different channels, for example via phone, chat, internet and email. It provides its services to circa 200 different clients in Finland. According to study interviews, there exists no definition of information security policy from management level, though some information security specific working practices are implemented, for example a password policy. Company has also implemented some other information security specific issues, like utilizing Secure Sockets Layer within their internet connections where they transfer people specific information. In general, the development actions are customer driven, otherwise company C is in reactive working mode, which means that they prefer to react in case of problems. Company C has neither not evaluated the company's key assets, nor implemented the continuity planning or risk management practicalities. In general, company management level commitment – or non-existence of it seem to affect heavily into information security management.

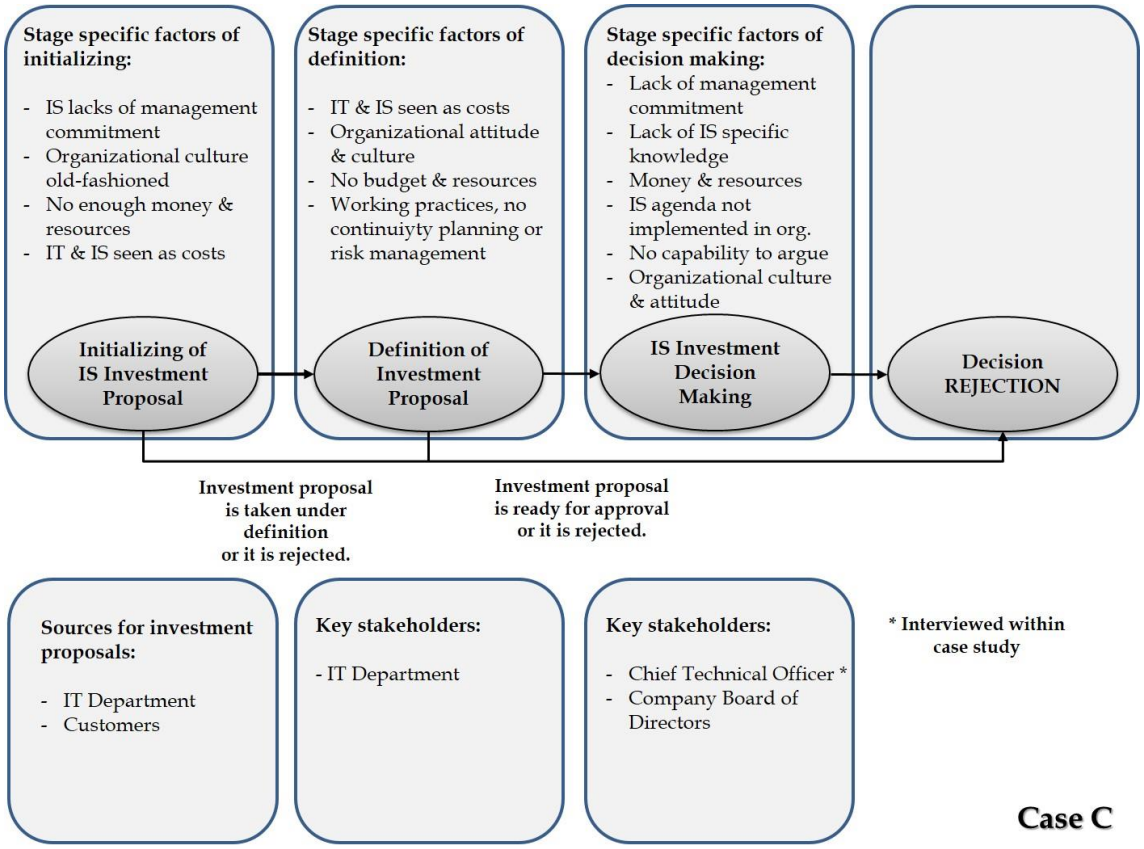

FIGURE 6 Case Company C, information security investment management process.

Both the stages of initializing and defining the information security investments are heavily on the responsibility of one person. There seems to be both lack of time and information security specific knowledge in identifying the investment proposals. Definition of information security investment proposal was found

challenging, as it is difficult to argue from economic point of view. Its value was seen difficult to state because of small company. In the stage of decision making, information security investment face several challenges. As there exists no implemented agenda for information security, investment proposals are challenging to argue to management team. As organizational culture and organization's working practices support reactive way of working, investment proposals which are seen kind of insurances are not seen appropriate proposals to approve.

The Figure 7 illustrates an information security investment decision making process of the case D. The Case D is a privately-owned small-sized company, which key business is to provide information technology solutions both for the consumers and businesses. Company's product portfolio contains for example following products: web services (customer can set up its own website or online store), cloud services (virtual data centers, virtual servers, data back-up) and data center services (maintenance and supervision of customer virtual servers).

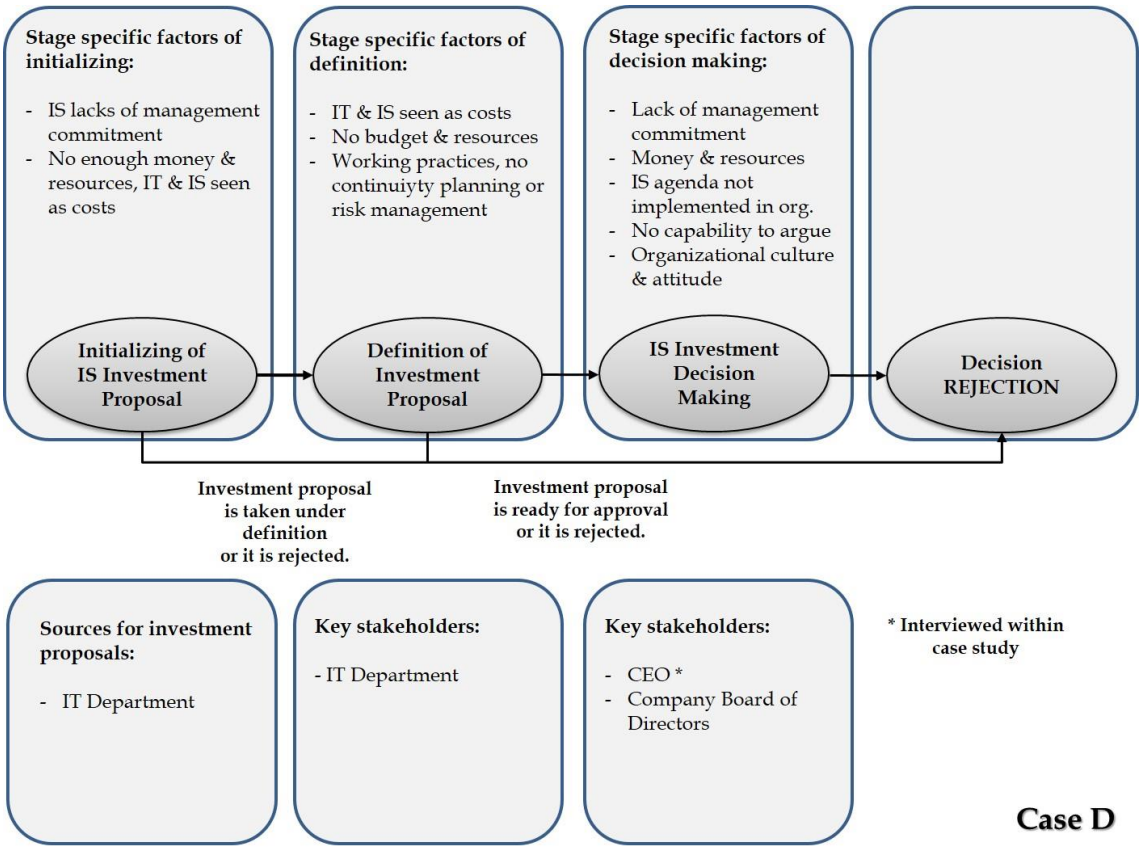

FIGURE 7 Case Company D, information security investment management process.

In general, the organizational culture and attitude supports information security management. There is no information security policy defined, nor continuity or risk management practicalities defined. Organizational working method is to

solve problems case by case when they occur. Still, CEO seems to be information security oriented, and willing to enhance the level of company information security. As the company's key business solutions are closely tied to information systems, company has considered also information security requirements. Challenge is that board of directors are not committed to information security, and investment proposals are approved mainly from total costs point of view. There have not been any specific information security investment proposals, and information security requirements are normally bundled together with other information technology solution requirements. When arguing information security investment proposals, the CEO find it difficult to state the value of investment towards the value achieved.

5.2 Cross-cases analysis of the information security investment process

As a result of the study material content analysis, there were composed two separate main categories from the study findings, which are the followings – and which are utilized as a basis for theory propositions.

1. Information security competence to define and argue information security investment proposals.
2. Organizational security culture.

In following text study findings are organized according to stage model and its phases: 1) Initializing an investment proposal, 2) Definition of investment proposal, and 3) Decision making. These defined categories are supported with empirical evidence gathered during the study phase of this thesis work.

5.2.1 Information security competence to define and argue information security investment proposals

Organizational capabilities to define and argue information security investment proposals was defined as a main category within content analysis phase, and it was onwards divided to following sub categories; Methods and capabilities to define and argue investment proposals, and Sufficient information security specific knowledge (Figure 8.).

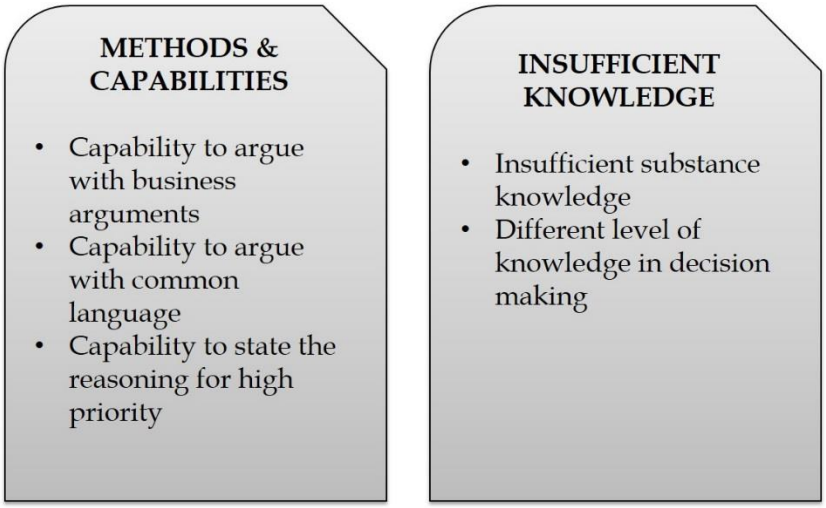

FIGURE 8 Sub-categories for Information security competence to define and argue information security investment proposals.

Methods and capabilities

There were lot of challenges in utilizing business arguments in both in defining and arguing the investment proposals.

In **defining the investment proposal phase**, the information security investment proposals were seen unmanageable via economical calculations, and stating the investment value against estimated costs was seen problematic.

> *...we cannot define the value of information security investment. It should be evaluated from risk management point of view. So far, there has not been any risk related to information security. (Case A)*

> *...investment proposal should be presented as a risk. Management team have different approach to risks than investment proposals. (Case B)*

> *…there is a high level criteria even to propose information security investment. There is always something more important. (Case A)*

> *...there are no economical methods to define the information security investments. (Case B)*

In **decision making phase**, it was seen that there are no proper way to prioritize the proposals, as each stakeholder is willing to support the one which is important to himself/herself. In some cases, decision making was unsuccessful due to lacking common language. Decision makers consist of people having no specialist level skills about information security and the investment proposals should be stated with common language. In some cases, information security

investment proposals were presented as a risk, which were seen appropriate way to get investment proposal approved.

> *...small company vs. costly investment for something that might not even happen - mission impossible. (Case D)*

> *…there were no proper arguments for the investment proposal. Investment proposal was seen too expensive, and there were no visibility what will be achieved with it. (Case B)*

> *…decision making is challenging, as decision makers have difficulties to understand what they are deciding. Investment proposals should be presented with common language. (Case B)*

> *...everyone is willing to drive their own interest. There are no clear principles, how prioritizing should be done among the investment proposals. (Case B)*

> *...there should be some kind of golden mean in doing decisions, but there is not. (Case B)*

Insufficient knowledge

There were lot of variation, how much – or how little there exists knowledge about the information security. It seems, that the knowledge is tight to certain roles and responsibilities.

In **initializing of investment proposal phase**, the insufficient knowledge about the information security affect to fact that investment proposals are not even initialized or processed further to definition phase.

> *…why bother to use email encryption, our email system is secure. We have never had any problems. (Case A)*

> *…there are no information security specialist in the company, who could advise which way to go. (Case A)*

> *…there are no risks from information security point of view. Who would harm us? (Case C)*

Some top level managers seem to lack even basic level knowledge about the information security. In **decision making phase** there exist different level of knowledge, which affects directly to decisions made.

…this certain investment (encryption of laptops) would most probably cause more burden to IT support, than enhance the security. And are there even somebody who is interested about our business? (Case A)

…there are no substance level knowledge in decision making level. Decisions are not based on knowledge, and decision makers are no able to understand their decisions' consequences. (Case B)

…even management level does not know who has the ultimate responsibility about the information security. They don't know it, and they seem not to be even interested about it. Until something happens. (Case B)

5.2.2 Organizational security culture

Organizational security culture was defined as a main category within content analysis phase, and it was onwards divided to following sub categories; Organizational way of working, Organizational attitude, Commitment & support for information security, and Politics (Figure 9).

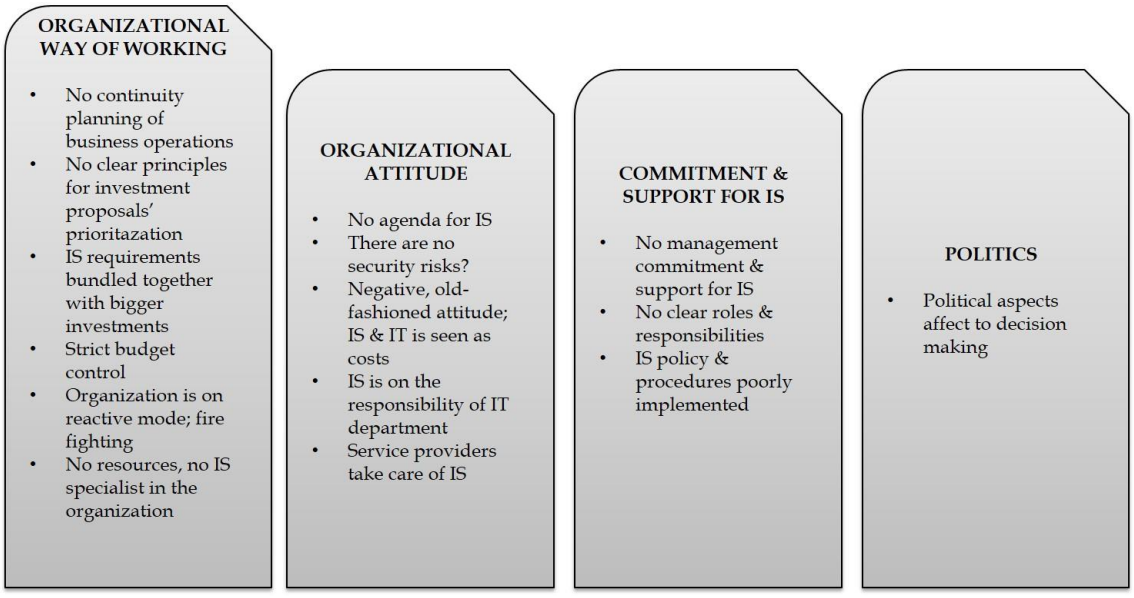

FIGURE 9 Sub-categories for Organizational security culture.

Organizational way of working

In several cases, there seem to exist drivers which directly affects to **initializing of the information security investment proposal**. There seem not to be constant continuity planning of business operations. Risk management practicalities were somehow implemented, though information security issues were not

considered. Some organizations work on reactive mode, and prefer to react only in case of problems. Greatest challenge seem to be non-existence of knowledgeable information security resources, who could follow up existing trends, define requirements and proposals – and convince the management team about the relevancy of information security investment proposal.

> *…our culture does not support proactive way of working. We react in case of problems. (Case C)*
>
> *…we have not yet considered continuity planning of our business operations. Target of this year is to identify the key assets of the company. (Case C)*
>
> *…we have enough challenges to cope with existing problems. No time or resources to consider what kind of problems we could have in future. (Case C & D)*
>
> *…we lack of information security specialist. (Case A)*
>
> *…there is no time and resources. (Case A & B)*

In decision making phase, organizations lack of proper principles for prioritizing investment proposals, which cause misunderstanding what really is important. Investment decisions are also done under strict budget control, and if there is not "ear-marked" money available, investment proposal gets easily rejected. Information security investment are most often bundled together with bigger information technology investments, and this is seen a proper way to get proposals approved. Greatest challenge seem to be non-existence of knowledgeable information security resources, who could follow up existing trends, define requirements and proposals – and convince the management team about the relevancy of information security investment proposal.

> *…there are no principles how the investment proposals should be prioritized. Everyone drive their own interest. (Case B)*
>
> *…we obviously lack of proper way of working! (Case A)*
>
> *…if there are no ear-marked budget for investment proposal, it is really difficult to get the proposal approved. Decisions are done under strict budget control. (Case B)*
>
> *…easiest way to get investment proposal approved is to tie information security requirements part to some other bigger investment proposal. (Case B)*

Organizational attitude

One of the most influential aspect to information security investments is the organizational attitude. Within study it came obvious that in organizations where information security agenda was not strong, the investment proposals are randomly **initiated**. In some cases, the attitude towards information security was very immature. There exists understanding, that there exists no security risks. Information security was also seen as a responsibility area of somebody else. In case of third party service providers, it was seen that service provider takes care of the information security. In case of own business operations, the IT department was seen as responsible stakeholder.

> *...there are no agenda for information security. (Case C & D)*
>
> *…there should happen some cultural change in this organization. Attitude towards information security is so old-fashioned. (Case A)*
>
> *…we still live in the 1990's century! (Case A)*
>
> *…maturity level of information security is very low. (Case D)*

Non-existence of strong information security agenda affect also to **decision making phase**. It came obvious, that the information security investment proposals lack of approval in decision making phase when organizational culture does not support information security. Attitude seem to be also immature and negative, as information security investment are mainly seen as costs.

> *…why somebody would harm us? (Case A)*
>
> *…information security – it always mean costs, and what we will get from those investments? (Case C)*

Commitment and support for information security

In commitment and support for information security category, there are several drivers which seem to affect directly to **initializing of investment proposal phase**. There seem to exist un-clarity of roles and responsibilities, even top management does not know who has the ultimate responsibility of information security. Information security policy and related procedures might exist, but

their implementation is not deployed nor followed up properly. In some cases, there exists no separate policy or procedures for information security.

> *…nobody is interested about the information security. It is always somebody else responsibility. (Case B)*

> *…information security, that's something IT department takes care of or…? (Case C)*

> *…there are some policy and procedures written, but the deployment lack of time and resources. They are not supported, there is always more important things to work with. (Case A)*

> *…I must say, that our information security policy is quite weak. It contains only password policy. (Case A)*

> *…I think we should have some kind of policy about information security. We do consider environmental affairs, maybe we should consider also information security? (Case A)*

Management level commitment and support for information security affects heavily also to investment proposals **decision making**. There are organizations who seem to lack totally the commitment and support for information security from management level.

> *…management is not interested about the information security. (Case D)*

> *…even top level management does not know who has the ultimate responsibility of information security. (Case B)*

> *…I feel like fighting against wind mills when discussing about information security with management team. (Case D)*

> *…decisions are cost-driven, despite the other facts. (Case D)*

> *…information security, my top favorite! (Case C)*

Politics

There are also political aspects, which affect to **decision making**. Decisions might be considered for example from employment point of view.

> *...some stakeholders are not willing to invest, as it might affect to the level of employment. (Case B)*

…investment is considered from our point of view, they should understand how that affect to our IT department and its employment. (Case B)

5.3 Theory propositions

This chapter describes the key outcome of the thesis, the theory propositions which aims to offer a feasible answer to the thesis research question:

- Why information security investment decision fail?

The theory propositions and related sub-propositions are categorized according to stage model and its phases 1) Initializing an investment proposal, 2) Definition of investment proposal and 3) Decision making of investment proposal.

5.3.1 Theory proposition related to initializing phase of the information security investment proposal

The first theory proposition relates to initializing phase of the decision making process of information security investment proposal. The theory proposition has four sub-propositions, which all are defined in following.

Theory proposition1: The likelihood of getting the information security investment proposal rejected in **initializing phase of the decision making process** will be higher when (1) organization lacks of information security competence, and (2) organizational security culture does not support information security.

The theory proposition1 is further divided to following sub-propositions:

Sub-proposition1: The likelihood of getting the information security investment proposal rejected in **initializing phase of the decision making process** will be higher when organization lacks of capabilities of business operations continuity planning.

Sub-proposition2: The likelihood of getting the information security investment proposal rejected in **initializing phase of the decision making process** will be higher when there exists (1) insufficient knowledge and (2) insufficient resources for the information security.

Sub-proposition3: The likelihood of getting the information security investment proposal rejected in **initializing phase of the decision making process**

will be higher when (1) information security agenda is not strong and (2) attitude towards information security is negative.

Sub-proposition4: The likelihood of getting the information security investment proposal rejected in **initializing phase of the decision making process** will be higher when (1) there exists un-clarity of roles and responsibilities and (2) management is not aware of their responsibility towards information security.

5.3.2 Theory proposition related to definition phase of the information security investment proposal

The second theory proposition relates to definition phase of the decision making process of information security investment proposal. The theory proposition has three sub-propositions, which all are defined in following.

Theory proposition2: The likelihood of getting the information security investment proposal rejected in **definition phase of the decision making process** will be higher when (1) organization lacks of information security competence to define investment proposal, and (2) organizational security culture does not support information security.

The theory proposition2 is further divided to following sub-propositions:

Sub-proposition1: The likelihood of getting the information security investment proposal rejected in **definition phase of the decision making process** will be higher when (1) organization lacks of capabilities to define the monetary value of investment proposal.

Sub-proposition2: The likelihood of getting the information security investment proposal rejected in **definition phase of the decision making process** will be higher when (1) organization lacks of information security specific resources, time and knowledge.

Sub-proposition3: The likelihood of getting the information security investment proposal rejected in **definition phase of the decision making process** will be higher when (1) information security lacks of management commitment and support in prioritization of tasks.

5.3.3 Theory proposition related to d phase of the information security investment proposal

The third theory proposition relates to decision phase of the decision making process of information security investment proposal. The theory proposition has five sub-propositions, which all are defined in following.

Theory proposition3: The likelihood of getting the information security investment proposal rejected in **decision phase of the decision making process** will be higher when (1) organization lacks of information security competence to argue an investment proposal, (2) organizational security culture does not support information security, and (3) political aspects affect to decision making.

The theory proposition3 is further divided to following sub-propositions:

Sub-proposition1: The likelihood of getting the information security investment proposal rejected in **decision phase of the decision making process** will be higher when (1) organization lacks of methods, (2) proper capabilities and (3) knowledge both to prioritize and argue the monetary value of investment proposal.

Sub-proposition2: The likelihood of getting the information security investment proposal rejected in **decision phase of the decision making process** will be higher when there exists (1) no common knowledge within decision makers about information security, and (2) no common understanding who has the ultimate responsibility of information security.

Sub-proposition3: The likelihood of getting the information security investment proposal rejected in **decision phase of the decision making process** will be higher when (1) organization lacks of business continuity management, (2) organization lacks of strong information security agenda, and (3) attitude towards information security is immature.

Sub-proposition4: The likelihood of getting the information security investment proposal rejected in **decision phase of the decision making process** will be higher when (1) information security lacks of management commitment and support, and (2) information security is not part of the organization's business approach.

Sub-proposition5: The likelihood of getting the information security investment proposal rejected in **decision phase of the decision making process** will be higher when (1) there does not exist deployed security policy and procedures within the organization, and (2) political aspects affect to decision making.

6 DISCUSSION

The purpose of this study was to understand why information security investment decision making process fail in its different stages. This study findings indicated, that the challenge of information security investment management is multilateral. The key factor in getting value from information security is to insure that technology investment protects the right things. The financial returns from a successful implementation of a security-enabled business process should justify the expenses of security in terms of enabling business (Tsiakis and Stephanides, 2005). From information technology point of view it is essential that in a competitive environment the right information systems/technology investments are selected in order to sustain corporate viability and prosperity (Bacon, 1994). According to Siponen et al (2014), the information security investments are not keeping the pace with information technology investments. This has caused a problem of underinvestment. In this study, it was examined which are the key drivers of the decision making, and why information security investment decision fail.

By examining why information security investment decision fail, it was extrapolated certain series of theory propositions, which were justified with empirical data. This chapter discuss and evaluate the findings of the case study, which are organized according to stage model and its phases. Also the implications for research and practice will be discussed in this chapter.

6.1 Research question and main findings

The main objective of this thesis was to gather empirical data about the information security investment decision making process and understand the reasons behind failed investment decisions. This study utilized an open interview as a data collection method. The research material of the empirical part of the study were gathered by interviewing pre-selected people having a key role in making information security investment management decisions. Interviewed people represented four different case companies.

This study's main research question was:

- Why information security investment decision fail?

To provide answer to this research question, this study utilized a research strategy where theory is built from case studies. This thesis defined three theory propositions and related sub-propositions according to the study findings. These study findings are summarized in table 4 and discussed further in the following text. Study findings are categorized according to stage model and its phases 1) Initializing an investment proposal, 2) Definition of investment proposal and 3) Decision making. Study findings are also categorized either to new findings, which are not identified by previous literature, or to existing findings, which are already identified by previous research and literature.

TABLE 4 Categorized findings affecting to failed investment decision

Category	**Main affecting findings to failed investment decision**	**New finding**	**Existing finding**	**Initializing phase**	**Definition phase**	**Decision phase**
Methods and	• Organization has no capability to define		X	X	X	X

capabilities	or/and argue with business arguments • Organization has no capability to define and argue with common language • Organization has no capability to state the reasoning for high priority	X X		X	X X	X X
Knowledge	• Organization lacks of sufficient level of knowledge about information security		X	X	X	X
Organizational way of working	• No continuity planning of business operations • No clear principles for investment proposals' prioritization • Strict budget control • Organization is on reactive mode; fire fighting • No resources, no IS specialist in the organization	X X X X	X	X X X	X	X X X
Organizational culture and attitude	• No agenda for information security • Negative, immature attitude; information security and information technology is seen as costs • Information security is on the responsibility of IT department • Service providers take care of information security	X X	X X	X X X		X X X X
Commitment and support for information security	• No management commitment & support for IS • No clear roles & responsibilities • Information security policy & procedures poorly implemented	X	X X	X X X		X X X
Politics	• Political aspects affect to decision making	X				X

According to the study findings the likelihood of getting the information security investment proposal rejected in initializing phase relates to organization's methods and capabilities of continuity planning of the business operations and to the level of knowledge about information security. Also the importance of information security might be unclear within the management team. The management of the organization is in key role in organizing, planning, maintaining and developing the information security. Information security investments should be supported by the management, and they should be aligned with business objectives. In a management level, strategic security investments are to support business strategy. Study findings also revealed, that organizational culture and attitude towards information security, and management commitment and support affect to initializing phase. The organizational culture and attitude seem actually to be one of the most influential aspect. If there are no information security agenda implemented in the organization, information security management targets are not existing or they are not aligned with business strategy, investment proposals are more likely not even to be initialized. This was one of the new findings within this study. This finding reflects directly to the management commitment, attitude and support towards the information security. If management does not see information security important or is having for example immature or negative attitude towards it, the implementation of it in organizational level is challenging. These findings can partly be supported by previous studies. Fenz et al. (2011), found that the lack of information security knowledge at the management level is one major reason for inadequate or nonexistent information security risk management strategies. According to Whitman and Mattord (2013), the first and most influential variable is the organizational culture. They saw it challenging, if upper management and staff does believe that information security is a waste of time and resources, as then information security will remain small and poorly supported. If information security is seen important and there exists a strong, positive view of it – information security is likely to be larger and well supported, both financially and otherwise.

Also understanding the responsibility of information security is one affecting aspect to initializing phase of the information security investment proposal, which was analyzed to be a new finding within this study results. There seems to be attitude that information security is only on the responsibility of information technology department, or in case of outsourced service, the service provider is the responsible one. This again reflects back to management commitment and support, as the management should understand that they have ultimate responsibility of business operations and its information security. This relates also directly to general awareness and knowledge about the information security, meaning that the information security is not something that can be managed only by means of the information technology department or third party service provider.

If organization lacks of constant continuity planning of business operations and for example the risk management practicalities are not effectively implemented, investment proposals are more likely rejected already in initializing

phase. In this kind of situations, organization is most probably on reactive mode and prefers to react problems when they occur. These findings are also partly supported by previous studies and literature. According to Tsiakis and Pekos (2008), information security should not be seen as technological problem resolved only with technical means. Information security should be part of the business approach and in risk management that needs to identify significant costs (time, expense, reduced functionality, unavailability, etc. if a security incident take place) meaning economic reasoning that explains the investment in security (Tsiakis and Pekos, 2008). Tsiakis and Theodiosos (2014), also discussed about the importance of information security investments' alignment to business objectives. When the investment decision relates to information security, it is essential to know what areas of improvement are prioritized in the organization. There are multiple stakeholders in a company, whose needs and demands should be taken into account and who need to take appropriate actions.

According to the study findings the likelihood of getting the information security investment proposal rejected in definition phase relates to organizations' methods and capabilities to define an investment proposal, and to sufficient level of knowledge about information security. By organizational methods and capabilities is meant the organization's tools, resources and processes – how the organization manage information security investments. Study findings indicated, that there are lot of challenges in utilizing business arguments in defining the investment proposals for decision makers. Information security investment proposals are seen unmanageable via economical calculations, and also defining the investment value against estimated costs is seen challenging. According to Tsiakis and Pekos (2008) benefits that cannot be measured with quantitative values may mean less for company decision makers. They saw that to lead to situation, that company's management see information security as an inhibitor to daily business operations if the investment is not well aligned with current business activities or is presented in financial terms not relevant to their agenda. Also Magnusson et al. (2007), stated it difficult to identify and quantify the benefit of information security investment, especially in translating it into economic terms. They indicated, that the problem to motivate information security investments economically is partly a consequence of the difficulties to generally produce correct calculations for information technology investments while comparing to traditional investments (Magnusson et al., 2007). The greatest challenge seem anyhow to relate to resourcing, which was one of the new findings of this study. There are non-existence of knowledgeable information security resources, who could follow up existing trends, define requirements and proposals – and convince the management team about the relevancy of information security investment proposals. To definition phase affects also the management commitment and support. If information security lacks of priority, there are no dedicated resources and time for investment proposal's definition.

The study findings indicated that the likelihood of getting the information security investment proposal rejected in decision making phase also relates to organizations' methods and capabilities to argue an investment proposal, and to sufficient level of knowledge about information security in management lev-

el. Study findings indicated, that there are lot of challenges in utilizing business arguments in arguing the investment proposals for decision makers. As information security investment by its natural character is not returning any profit, its arguing should be carefully considered. Information security investments are in some organizations considered as a risk or an insurance for business operation and its continuity, which seemed to be effective way of arguing it for decision makers. Similar findings can be pointed out from previous studies. Fenz et al. (2011), found that the lack of information security knowledge at the management level is one major reason for inadequate or nonexistent information security risk management strategies. Tsiakis and Pekos (2008) defined, that if investments in information security are evaluated alongside other investment projects, it may help to consider them on an equal footing, implying the use of similar methods of calculating the financial costs and benefits. Benefits that cannot be measured with quantitative values may mean less for company decision makers. They saw that to lead to situation, that company's management see information security as an inhibitor to daily business operations if the investment is not well aligned with current business activities or is presented in financial terms not relevant to their agenda. Magnusson et al. (2007), also stated it difficult to identify and quantify the benefit of information security investment, especially in translating it into economic terms. They indicated, that the problem to motivate information security investments economically is partly a consequence of the difficulties to generally produce correct calculations for information technology investments while comparing to traditional investments (Magnusson et al., 2007). According to Lander and Pinches (1998), the results of existing decision making methods provide decision makers with inadequate or little intuitive and/or interactive decision support, which is not supporting them in identifying an appropriate risk versus cost trade-off when investing in information security solutions.

Study findings revealed as a new finding that organizations are not utilizing a proper way and processes to prioritize the investment proposals – or at least the processes to prioritize investment proposals are not straight forward and each stakeholder can promote proposals which have the greatest value for themselves. In prioritization, it should be critical to evaluate which proposals are business critical and can value and support the business continuity. Decision making can fail also due to lack of common language, which was pointed out as a new finding of the study. Most often the decision makers are people having no specialist level skills about information security. For that reason, investment proposals should be stated with common and understandable language.

Study findings also indicated that the organizational way of working and organizational culture and attitude affect to investment proposals' decision making. The organizational culture and attitude seem to be one of the most influential aspect. If there are no information security agenda implemented in the organization, information security management targets are not existing or they are not aligned with business strategy, also the investment proposals are more likely to be rejected. This reflects directly again to the management commitment,

attitude and support towards the information security. If management does not see information security important or is having for example immature or negative attitude towards it, the implementation of it in organizational level is challenging, as the investment proposals will not get priority in decision making. The level of knowledge about information security – and its importance might be unclear within the management team, which affects negatively to decision making process, as the management of the organization is in key role in organizing, planning, maintaining and developing the information security. Management should have proper understanding in general about the information security and especially how the information security investment proposal's implementation – or non-implementation of it affect to organization. These findings are partly supported by previous studies and literature. For example according to Whitman and Mattord (2013), the first and most influential variable is the organizational culture. They saw it challenging, if upper management and staff does believe that information security is a waste of time and resources, as then information security will remain small and poorly supported. If information security is seen important and there exists a strong, positive view of it – information security is likely to be larger and well supported, both financially and otherwise.

Also understanding the responsibility of information security is one affecting aspect to decision making phase, which is a new finding of the study. There seems to be attitude that information security is only on the responsibility of information technology department. This again reflects back to management commitment and support, as the management should understand that they have ultimate responsibility. This relates also directly to general awareness and knowledge about the information security, meaning that the information security is not something that can be managed only by means of the information technology department or third party service provider. If organization lacks of constant continuity planning of business operations and for example the risk management practicalities are not effectively implemented, investment proposals which main target is to guarantee the business continuity, are more likely to be rejected in decision making. In that kind of situations can be said, that management does not support investment proposals, which are seen more as costs than as enablers for business, and especially for business continuity in case of security breach. This might be due to fact that organization is working in reactive mode, meaning that problems are solved as they appear. It was also analyzed as a new finding, that for information security investments, there are no budgeted, so called "ear-marked" money available, which naturally affects to decision making, as investment decisions are made under strict budget control. It appeared to be quite common to bundle the information security requirements together with bigger information technology investments, as they are planned and budgeted beforehand and thus most often approved in decision making phase. These findings are also partly supported by previous studies and literature. According to Tsiakis and Pekos (2008), information security should be part of the business approach and in risk management that needs to identify significant costs (time, expense, reduced functionality, unavailability,

etc. if a security incident take place) meaning economic reasoning that explains the investment in security (Tsiakis and Pekos, 2008). Tsiakis and Theodiosos (2014), also discussed about the importance of information security investments' alignment to business objectives. When the investment decision relates to information security, it is essential to know what areas of improvement are prioritized in the organization. There are multiple stakeholders in a company, whose needs and demands should be taken into account and who need to take appropriate actions.

Also political aspects affect to decision making, which is a new finding of the study. If investment proposal's implementation for example decreases the amount of workplaces, it might be considered negatively within decision making process.

6.2 Implications on research and practice

From the perspective of research and theoretical understanding, this research produces new theory propositions, which comprise a theory framework for information security investment decision making. The previous research have not addressed specifically why information security investment decisions fail in decision making process and what are the key drivers behind the decision making. This study could be replicated with broader amount of case companies and interviewed stakeholders in order to re-consider the study findings. As this research provide as an outcome theory propositions, future research could test the theory propositions defined. This research neither addressed specifically why information security investment decision succeed in decision making process, which could be studied as well. Study results strongly indicated the lack of understanding about the ultimate responsibility in the organization of the information security. Future research could study, by what means the information security policy and procedures, including the defined responsibilities should be deployed in organization in order to increase both the knowledge and understanding about the information security and key responsibilities related to it. Study findings also indicated the importance of organizational culture and attitude from information security point of view. Future research could research, how the importance of information security and its implementation could be enhanced in organizations. Future research could also concentrate on small and medium sized companies, as it seems that smaller the company is the less importance the information security gets in the management level. Also utilizing the third party service providers in information technology services opens interesting research approaches within information security management, as especially small- and medium sized companies seem to have persuasion that they can outsource also the ultimate responsibility of information security. Future research could also study further the approach how to manage information security investment proposal, as according to the study results the investment

proposals which are presented as a risk are more often approved in decision making process.

From the practical perspective this study findings elaborate the challenges related to information security management decision making. Presented study findings and composed theory propositions formulate a theory framework, which affect behind the information security investment decision making process. By becoming aware of these affecting drivers, organization can develop its operation and contribute to successful decision making process of the information security investments. At the same time, the information security agenda in the organization would get more importance and visibility within the organization. According to the study findings, organization should consider how to increase the level of information security within the management team, and at the same time in the whole organization. Organization could for example organize an information security awareness program, and via that promote the importance of information security, share information about roles and responsibilities and deploy different information security specific ways of working, like a password policy. As important is also to make sure, that information security investment proposals are communicated with the common language to decision makers, and that they are aware of the consequences of rejected decisions. As the information security investment proposals are challenging to argue with economical methods and calculations, organization could evaluate them for example through risk management process. Organization should also define a clear and straight forward process for prioritization of the investment proposals. Prioritization should not be based on the individual stakeholder own interest, it should be considered from the business criticality point of view.

From the practical perspective this study findings indicate that organization should have proper process for business continuity management, risk management and prioritization of information security investment proposals. By implementing information security awareness program and promoting the importance of information security, organization can affect to organizational culture and attitude towards the information security. Organization could have the most powerful tools and techniques in place to protect information security, but it must be remembered that humans are the weakest link. By ensuring, that employees understand the criticality of information security, organizational culture and attitude towards positive thinking of information security can be achieved. The study findings also indicated the importance of management commitment and support. Like defined, the management of the organization is in key role in organizing, planning, maintaining and developing the information security. The successful management of information security requires managerial commitment to develop it further. Information security investments should be supported by the management, and they should be aligned with business objectives. Management should drive the cultural change to organization and promote information security as a key enabler of business continuity. The theory propositions defined by this research gives guidance to organizations what different drivers affect in the field of information security management, and in especially in information security investment decision making

process. These drivers should be considered in developing the information security management in organization.

7 CONCLUSION

This chapter presents the conclusions of this study by summarizing the research outcomes. This chapter also presents the contributions for research and the limitations of this study.

The focus of the research was to analyze the information security investment decision making process, and understand why information security investment decisions fail. The aim was to discover the influential drivers, which affect to decision making and create theory propositions which aim to answer to the research question. The research was executed as a qualitative case study. There were four case companies included, and in total fourteen stakeholders interviewed. Interviews were open interviews and interview results were analyzed utilizing inductive content analysis method. Study phase of thesis utilizes stage theory approach, which provided an approach to explain how and why a chronology of occurrences play out over time and finally lead to rejected decision in information security investment decision making process.

This study findings indicated, that the challenge of information security investment management is multilateral. In the phase of initializing of the information security investment the challenge relates to organization's capabilities of continuity planning of the business operations and to the level of knowledge and understanding about the information security and responsibilities related to it. In the phase of defining the information security investment proposal, the organizations' capabilities to define an investment proposal, and a sufficient level of knowledge about information security affects strongly. Still, the greatest challenge in definition phase seem to relate to resourcing. There seem to be non-existence of knowledgeable information security resources, who could follow up existing trends, define requirements and proposals – and convince the management team about the relevancy of information security investment proposals. In the phase of decision making, there are several affecting drivers. The study findings indicated that the likelihood of getting the information security investment proposal rejected in decision making phase relates to organizations' capabilities to argue an investment proposal, and to sufficient level of knowledge about information security in management level. Study

findings also revealed that organizations are not utilizing a proper way and processes to prioritize the investment proposals and decision making can fail also due to lack of common language. Study findings further indicated that the organizational way of working and organizational culture and attitude affect to investment proposals' decision making, which seem to be one of the most influential aspect. Also understanding the responsibility of information security at management level and political aspects are affecting to decision making phase.

By examining why information security investment decision fail and analyzing the study findings, it was extrapolated certain series of theory propositions, which comprise a theory framework affecting behind of the information security investments decision making process. The theory propositions and related sub-propositions were categorized according to stage model and its phases 1) Initializing an investment proposal, 2) Definition of investment proposal and 3) Decision making of investment proposal.

7.1 Contributions to research

This research has some contributions to research. This research aims to improve the understanding of information security investment management, and especially the decision making process from the failed investment proposals perspective. From the research point of view, one key contribution to the academic field is that this is one of the very first researches to examine the reasons behind the failed information security investment decisions, and thus fills the research gap in the academic literature. This research findings provide original information about reasons to explain failed decision making. In addition to that, this research also supports the previous literature by stating that the challenge of information security investment management is multilateral. From the perspective of previous researches, which have mainly approached the information security investment problems theoretically examining the optimal information security investment (for example Gordon and Loeb, 2002; Huang et al., 2008; Kort et al., 1999) and the efficiency of information security investment (for example Gordon and Loeb, 2006; Purser, 2004) (Karjalainen et al., 2014), this research findings indicated that information security investment management should be studied more from the perspective of risk management, as according to the research findings investment proposals which are presented as a risk are more likely to get approval in decision making process. This relates directly to the organizational methods and capabilities to manage information security investment proposals, as this study results indicated that organizations are lacking proper methods and capabilities both to define and argue investment proposals. This research findings revealed clearly as a new finding that, if there are no information security agenda implemented in the organization, information security management targets are not existing or they are not aligned with business strategy, investment proposals are more likely not even to be initialized. Research findings also indicated as a new finding that the non-existence of un-

derstanding and awareness about the responsibilities of information security, and lacking continuity planning of business operations are key affecting aspects in initializing phase of the information security investment proposal decision making process. According to the study findings the likelihood of getting the information security investment proposal rejected in definition phase relates to organizations' methods and capabilities to define an investment proposal, and to sufficient level of knowledge about information security. The greatest challenge seem to relate to resourcing, which is presented as a new finding of this study results. There are non-existence of knowledgeable information security resources, who could follow up existing trends, define requirements and proposals – and convince the management team about the relevancy of information security investment proposals. From the perspective of the decision making phase, the study results indicated that organizations are not utilizing a proper way and processes to prioritize the investment proposals, which is presented as a new finding. Decision making can fail also due to lack of common language, as most often the decision makers are people having no specialist level skills about information security. This is also new finding of the study. Study results further indicated as a new finding, that for information security investments, there are no budgeted, so called "ear-marked" money available, which naturally affects to decision making, as investment decisions are made under strict budget control. Lastly, this study results indicated as a new finding that political aspects affect to decision making.

7.2 Limitations

This research has some limitations. First of all, according to the researcher knowledge, this was a very first study of why information security investment decision fail in decision making process. The study findings are based on the empirical data, and the data coverage can be seen as limited, as there were only four case companies and in total fourteen interviews conducted. Case companies did represent different business operations and the size of the organizations varied, but still the sample size can be considered small. Also it must be taken into account that interviews were conducted in Finnish and afterwards during the analysis phase translated into English. This might have affected to the original meaning of the participants, as chosen words and terms might have altered during that process. It is also possible, that the study results may have been affected by interviewees' low level of knowledge and capabilities about information security investment management. Also due to the fact that information security is case sensitive, the data gathered during the interviews might be inadequate.

REFERENCES

Andreasson, A. and Koivisto, J. 2013. Tietoturvaa toteuttamassa. Tietosanoma Oy, Tallinna 2013.

Ariyachandra, T. R. and Frolick, M. N. 2008. "Critical success factors in business performance management – Striving for success," *Information Systems Management*, 25(2), pp. 113-120.

Bacon, J. 1994. "Why companies invest in information technology ?" *MIS Quarterly*. September, pp. 335-354.

Baker, W., Rees, L., and Tippet, P. 2007. "Necessary Measures : Metric-Driven Information Security Breaches," *Communications of the Association for Information Systems* (12), pp. 684-700.

Baker, W., and Wallace, L. 2007. "Is information Security Under Contorl ? Investigating Quality in Information Security Management," *IEEE Security and Privacy* (5), Piscataway, NJ : IEEE Educational Activities Department, pp. 36-44.

Bandyopadhyay, T., Liu, D., Mookerjee, V., and Wilhite, A. 2012. "Dynamic competition in IT security : A differential games approach," *Information Systems Frontiers*, 16(4), pp. 643-661.

Bardhan, I., Bagchi, S., and Sougstad, R. 2004. "Prioritizing a Portfolio of Information Technology Investment Projects," *Journal of Management Information Systems*, (21 :2), pp. 33-60.

Bleistein, S. J., Cox, K., Verner, J., and Phalp, K. T. 2006. "A requirements analysis framework for validating strategic alignment of organizational IT base on strategy, context, and process," *Information and Software Technology*, 48(9), pp. 846-868.

Brink, D. 2001. "A guide to determining return on investment for e-security," *RSA Security Inc.*

Burnard, P. 1991. "A method of analysing interview transcripts in qualitative research," *Nurse Education Today*, 11, pp. 461-466.

Cavanagh, S. 1997. "Content analysis : concepts, methods and applications," *Nurse Researcher* 4, pp. 5-16.

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

CISCO. The return on investment for network security. CISCO white paper, http://www.cisco.com/warp/public/cc/so/neso/sqso/roi4_wp.pdf.

Chowdhury, S.D. 2002. "Turnarounds : A Stage Theory Perspective," *Canadian Journal of Administrative Sciences*, 19(3), 249-266.

Cole, F.L. 1988. "Content analysis : process and application," *Clinical Nurse Specialist* 2(1), pp.53-57.

Davis, A. 2005. "Return on security investment-proving it's worth it," *Network Security*, November, pp. 8-10.

Dey, I. 1993. "Qualitative Data Analysis. A User-Friendly Guide for Social Scientists," *Routledge*, London.

Duh, R. –R., Chow, C. W. and Chen, H. 2006. "Strategy, IT applications for planning and control, and firm performance : The impact of impediments to IT implementation," *Information and Management*, 43(8), pp. 939-949.

Eisenhardt, K.M. 1989. "Building theories from case study research", *Academy of Management Review*, (14 :1), pp. 532-550.

Eisenhardt, K.M. 1991. "Better stories and better constructs : The case for rigor and comparative logic", *Academy of Management Review*, (16), pp. 620 – 627.

Eisenhardt, K.M. and Graebner, M.E. 2007. "Theory building from cases : opportunities and challenges", *Academy of Management Journal* (50 :1), pp. 25-32.

Faraj, S. & Sambamurthy, V. (2006). "Leadership of Information Systems Development Projects," *IEEE Transactions on Engineering Management*, 53(2), 238–249.

Fenz, S., Ekelhart, A., and Neubauer, T. 2011. "Information Security Risk Management : In Which Security Solutions Is It Worth Investing ?," *Communications of the Association for Information Systems* : Vol. 28, Article 22.

GAO. 1996. "Content Analysis a Methodology for Structuring and Analyzing Written Material," *Program Evaluation and Methodology Division, United States General Accounting Office*, Washington.

Gillham, B. 2010. Case Study Research Methods. London, GBR : Continuum International Publishing.

Goodhue, D., and Thompson, R. 1995. "Task-technology fit and individual performance," *MIS Quarterly*, 19(2), pp. 213-236.

Gordon, L. A., & Loeb, M. P. 2006. "Economic aspects of information security : an emerging field of research," *Information System Frontiers* (8 :5), pp. 335-337.

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

Hausken, K. 2006. "Returns to information security investment : The effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability," *Information Systems Frontiers*, 8(5).

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2009) Tutki ja kirjoita. (15. uud. painos) Helsinki: Tammi.

Hsieh, H. F. & Shannon, S. 2005. "Three approaches to qualitative content analysis," *Qualitative Health Research* 15, pp. 1277 – 1288.

Huang, C.D., Hu, Q., 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.

International Federation of Accountants. "The Capital Expenditure Decision : Statement on International Management Accounting Practice 2," *Financial and Management Accounting Committee*, 540 Madison Avenue, New York, NY 10022, September/October 1989.

Ioannidis, C., Pym, D., and Williams, J. 2011. "Fixed Costs, Investment Rigidities, and Risk Aversion in Information Security : A Utility-Theoretic Approach," in *Proceedings of the Tehth Workshop on the Economics of Information Security* (WEIS), pp. 171-191.

Jung, C., Han, I., and Suh, B. 1999. "Risk Analysis for Electronic Commerce Using Case-Based Reasoning," *International Journal of Intelligent Systems in Accounting, Finance & Management* (8), pp. 61-73.

Järvinen, P., and Järvinen, A. 2011. Tutkimustyön metodeista, Opinpajan kirja, Tampere.

Kambil, A., Henderson, J., Mohsenzadeh, H. 1992. Strategic Management of Information Technology Investments : An Options Perspective. *Researchgate.net,* pp. 1-24.

Karim, J., Somers, T. M., and Bhattacherjee, A. 2007. "The impact of ERP implementation on business process outcomes : A factor-based study," *Journal of Management Information Systems*, 24(1), pp. 101-134.

Karjalainen, M., Siponen, M., Kohli, R. & Shao, X. 2014. "What's in it for me ? A Stakeholder Theory perspective on Information Technology Security Investment," *Completed Research Paper*. pp. 1-30.

Kort, P., Haunschmied, J. and Feichtinger, G. 1999. "Optimal Firm Investment in Security," *Annals of Operations Research* (88 :0), pp. 81-98.

Kyngäs, H. & Vanhanen, L. 1999. "Content Analysis (Finnish)," *Hoitotiede* 11, pp. 3-12.

Lander, D.M., and Pinches, G.E. 1998. "Challenges to the Practical Implementation of Modeling and Valuing Real Options," *The Quarterly Review of Economics and Finance* (38), pp. 537-567.

Lauri, S. & Kyngäs, H. 2005. "Developing Nursing Theories (Finnish : Hoitotieteen Teorian Kehittäminen)," *Werner Söderström*, Dark Oy, Vantaa.

Liu, D., Ji, Y., and Mookerjee, V. 2011. "Knowledge Sharing and Investment Decisions in Information Security," *Decision Support Systems* (52 :1), pp. 95-107.

Lycett, M., Rassau, A., and Danson, J. 2004. "Programme management : Critical review," *International Journal of Project Management*, (22 :1), pp. 289-299.

Magnusson, C., Molvidsson, J., and Zetterqvist, S. 2007. "Value Creation and Return On Security Investments (ROSI)," in *IFIP International Fedaration for Information Processing 232, New Approaches for Security, Privacy and Trust in Complex Environments*, Venter, H., Eloff, M., Labuschagne, L., Eloff, J., and von Solms, R. (eds.), Boston, pp. 25-35.

Marchand, D. A., Kettinger, W. J., and Rollins, J. D. 2000. "Information Orientation: People, Technology and the Bottom Line", *Sloan Management Review* (41:4), pp. 69-80.

Matsuura, K. 2003. "Information Security and Economics in Computer Networks : An Interdisciplinary Survey and a Proposal of Integrated Optimization of Investment," *Computing in Economics and Finance* (48), pp. 1-13.

Mithas, S., Ramasubbu, N., and Sambamurthy, V. 2011. "How Information Management Capability Influences Firm Performance", *MIS Quarterly*, Vol 35 No.1, pp. 237-256.

Mithas, S., Tafti, A., Bardan, I., and Goh, J. M. 2012. "Information Technology and Firm Profitability : Mechnanisms and Empirical Evidence", *MIS Quarterly*, Vol 36 No.1, pp. 205-224.

Mizzi, A. 2010. "Return on information security investment – The viability of an anti-spam solution in a wireless environment, " *International Journal of Network Security* (10:1), pp. 18-24.

Niederman, F., Brancheau, J.C., Wetherbe, J.C., 1991. "Information systems management issues for the 1990s," *MIS Quarterly 15* (4), 475-502.

Purser, S. 2004. "Improving the ROI of the security management process," *Computers & Security* 23 (2004), pp. 542-546.

Reyck, B. D., Grushka-Cockayne, Y., Lockett, M., Calderini, S., R., Moura, M., and Sloper, A. 2005. "The impact of project portfolio management on information technology projects," *International Journal of Information Management* 23 (2005), pp. 524-537.

Schwarzer, R. 2008. "Modeling Health Behavior Change: How to Predict and Modify the Adoption and Maintenance of Health Behaviors". Applied Psychology, (57:1), pp. 1–29.

Shaughnessy, J.; Zechmeister, E.; Jeanne, Z. (2011). Research methods in psychology (9th ed.). New York, NY: McGraw Hill. pp. 161–175.

Shields, Patricia and Rangarjan, N. 2013. "A Playbook for Research Methods: Integrating Conceptual Frameworks and Project Management", *Stillwater, OK*: New Forums Press.

Siponen, M., Karjalainen, M,. Kohli, R., and Shao, X. 2014. "Examining the Mystery of Underinvestment in Information Security : Explaining Why Information Security Investment Proposals are Accepted or Rejected".

Smith, S. and Spafford, E. 2004. "Grand Challenges in Information Security : Process and Output," *IEEE Security & Privacy* (2), pp. 69-71.

Stamp, P., Penn, J., Adrian, M., and Gray, B. "Increasing Organized Crime Involvement means More Targeted Attacks, Forrester ResearchAvailable at", http://www.forrester.com/Research/Document/Excerpt/0,7211,37505,00.html August 2, 2005

Tatsumi, K. and Goto, M. 2010. "Optimal timing of Information Security Investment: A Real Options Approach, in Economics of Information Security and Privacy," Moore, T., Pym, D., and Ioannidis, C. (eds), *New York NY*: Springer US, pp. 211-228.

Trkman, P. 2009. "The critical success factors of business process management," *International Journal of Information Management* 30 (2010), pp. 125-134.

Tsiakis., T. and Stephanides, G. 2005. "The economic approach of information security," *Computers and Security* (2005) 24, pp. 105-108.

Tsiakis, T., and Pekos, G. 2008. "Analyzing and determining Return on Investment for Information Security," *International Conference on Applied Economics,* ICOAE, pp. 879-884.

Tsiakis, T., Kargidis, T., and Katsaros, P. 2014. "Approaches and Processes for Managing the Economics of Information Systems", *IGI Global book series Advances in Business Information Systems and Analytics* (ABISA).

Van de Ven, A.H. 1992. "Suggestions for studying strategy process : A reseach note," *Strategic Management Journal 13*, 169-188.

Wang, S.L., Chen, J.D., Stirpe, P.A., and Hong, T.P. 2009. "Risk-Neutral Evaluation of Information Security Investment on Data Centers," *Journal of Intelligent Information Systems* (36:3), pp. 329-345.

Weinstein, N. D., Rothman, A. J., and Sutton, S. R. 1998. "Stage Theories of Health Behavior: Conceptual and Methodological Issues," *Health Psychology* (17:3), pp. 290-299.

Westerlind, K. 2004. "Evaluating return on information technology investment," *Master Thesis*, School of Economics and Commerial Law, Gothethenburg University.

Whitman, M., and Mattord, H. 2013. "Management of Information Security," *Delmar Cengage Learning*.

Wood, C., C., and Parker, D., B. 2004. "Why ROI and similar financial tools are not advisable for evaluating the merits of security projects," *Computer Fraud and Security*, volume 2004, issue 5, pp. 8-10.

Yin, R., K. 1989. Case study research: Design and methods, Sage Publ., Beverly Hills Ca.

Yin, R., K. 1994. Case study research: Design and methods (2nd edition). Newbury Park, CA: Sage.

APPENDIX 1 OPEN INTERVIEW SCHEME

Why information security investment's decision fail or pass?

General questions:

- Interviewee's role in the case organization?
- Size of the organization?

Short case example(s) definition:

- Background information about the case example?

Case example:

- How do your work involve with information security investment decision making?
- From where does the information security investments come to your table?
- Process to manage information security investments?
    - How?
    - Why?
    - Who involved in decision making?
    - Why they pass?
    - Why they fail?

Further information:

- Other relevant contacts in the case organization who could be interviewed?