TALLINN UNIVERSITY OF TECHNOLOGY

School of Information Technology

Department of Software Science

ITC70LT

Tiiu Mamers

THE ART AND SCIENCE OF INFORMATION SECURITY INVESTMENTS FOR SMALL ENTERPRISES

Master's Thesis

Supervisor:

Prof. Olaf Manuel Maennel,

PhD (Dr. rer. Nat)

Tallinn 2018

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Tiiu Mamers

2.01.2018

Abstract

Academic literature provides a considerable amount of approaches solving different information and information system security investment problems by using various methods. The factors and conditions that are prevalent in the approaches and the investment problems that are solved indicate that the models are targeted to large organizations.

The share and the economic importance of small enterprises is considerable and the information system security issues of small enterprises should not be overlooked. The goal of the master thesis is to define the information and information security investment problem for small enterprises and propose how to solve the problem.

Before the investment problem is explained and defined the need and incentives for small firms to invest in information security are discussed. To find the methods that the small enterprises could apply, the existent information security investment approaches are analysed respect to whether the investment problem that is solved in that specific approach is relevant and would the method be applicable by small firms. A step by step process is proposed that the small firms could follow to make their information and information security investment decisions along with the Return on Risk Portfolio Investment (RORPI) model that allows to find the economically most efficient risk treatment alternative mitigating the risks in the risk portfolio.

This thesis is written in English and is 109 pages long, including four chapters, six figures and eight tables.

Lühikokkuvõte

Informatsiooni turvalisuse investeeringute kunst ja teadus väikeettevõtetele

Teaduskirjanduses on informatsiooni ja infosüsteemide turvalisuse investeeringuid käsitlevaid lähenemisi arvestatav hulk. Investeerimisprobleemid, mida lahendatakse, on erinevad ja erinevad on ka meetodid, mida probleemide lahendamisel rakendatakse. Tingimused ja faktorid, millega lähenemistes arvestatakse ning probleemid, mida lahendatakse, viitavad, et mudelid on suunatud suurettevõtetele.

Väikeettevõtete osakaal ja tähtsus majanduses on arvestatav, seega ei tohiks väikeettevõtete informatsiooni turvalisuse probleemidest lihtsalt üle vaadata. Magistritöö eesmärgiks on defineerida väikeettevõtete informatsiooni ja infosüsteemi turvalisusesse investeerimise probleem ning pakkuda välja probleemilahendus.

Enne investeerimisprobleemi selgitamist ja defineerimist analüüsitakse väikeettevõtete vajadust ja ajendeid informatsiooni turvalisusesse investeerida. Väikeettevõtetele sobilike lahenduste leidmiseks analüüsitakse olemasolevaid lähenemisi lähtudes investeerimisprobleemi olulisusest väikeettevõtetele ning meetodi rakendatavusest. Informatsiooni ja infosüsteemi turvalisuse investeeringu otsuste tegemiseks pakutakse magistritöös välja samm-sammuline protsess, millest väikeettevõte saaks juhinduda. Samuti esitatakse töös riski portfelli investeeringute hindamise mudel, mida saab kasutada riskide maandamise ökonoomseima alternatiivi selgitamiseks.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 109. leheküljel, nelja peatüki, kuue joonise ja kaheksa tabeliga.

List of Abbreviations and Terms

ALE – Annual Loss Expectancy of a specific risk

ALE Total – Annual Loss Expectancy of risks in a risk portfolio

ARO – Annual Rate of Occurrence

Cash flow – cash and cash equivalents that can be converted into cash within three months

GDPR – General Data Protection Regulation (regulation (EU) 2016/679)

IRR – Internal Rate of Return

Liquidity crises – lack of cash and cash equivalents

mALE – Annual Loss Expectancy of a specific risk when a risk treatment would be/is implemented

mALE Total – Annual Loss Expectancy of risks in a risk portfolio when a risk treatment alternative would be/ is implemented

mARO – Annual Rate of Occurrence when a risk treatment would be/is implemented

mSLE – Single Loss Expectancy when a risk treatment would be/is implemented

NPV – Net Present Value

ROI – Return on Investment

RORPI – Return on Risk Portfolio Investment

ROSI – Return on Security Investment

SLE – Single Loss Expectancy

Tagetier – an attacker launching a targeted attack (term proposed by Bellovin, 2015)

Table of Contents

List of Figures

List of Tables

1. Introduction

"Planning information security investment is somewhere between art and science." Böhme (2010:10)

Academic literature provides large amount of approaches concerning information and information system security investments. The approaches solve different investment problems that exist on different management levels in large organizations. The top-management in general solves the problem of optimizing information security budget, the next levels maximize the security respect to the budget constraint. There are various methods how to solve the different information security investment problems. But *what is the information security investment problem for a small enterprise where only one organizational level exists and what would be the method to solve that problem in this organization?*

The amount of research studying information security risk management in small enterprises is scarce. The author of the thesis has not discovered any study that has focused on the information security investment problem(s) of small businesses.

Small enterprises are not defined uniformly in the world, but the general categorization is made based on the number of employees and turnover. In the context of the thesis the exact distinction between micro, small or medium-sized enterprises based on number of employees and turnover does not have fundamental importance. A small enterprise in the context of the thesis is a business with single organizational-managerial level, having not enough resources to employ an information security expert, to implement or outsource the implementation of any classical information security risk management framework. The thesis is directed towards those small businesses that meet these conditions and whose business critical processes, value creation and protection is supported by information systems. It can be expected that the share of those firms meeting above described conditions is highest among the enterprises who are defined as small based on number of employees and turnover.

The share and the significance of small enterprises in the economy is considerable. Their information and information system security issues should not be overlooked.

The goal of the master thesis is to define the information and information system security investment problem for the small enterprises and propose a method to solve the problem. Three main questions should be answered to achieve the goal:

1. *Why to invest?* To understand whether the small businesses overall have an information security investment problem; the incentives to invest have to be explained.
2. *What is the information security investment problem for small enterprises?*
3. *How can they solve their investment problem?*

To answer these three main research questions the following objectives are set:

- to explain the important concepts related to information security investments;
- to discuss the significance of small businesses to the economy;
- to study how relevant the information systems for small firms supporting business processes and value creation are and how the security and data protection indicators look compared to that;
- to define the segment of the small enterprises for whom the thesis is addressed to;
- to propose the incentives that the small businesses might have to invest in information security;
- to define the information and information system security investment problem for small businesses;
- to analyse the existent approaches solving information security investment problems respect to its theoretical or practical nature, the relevance of the investment problem for small firms and the applicability of the method by the small firms;
- to propose the method that the small enterprises could use when making their information and information system security related investment decisions.

According to the objectives the thesis is divided to two main chapters – chapter 2 and 3. Chapter 2 explains the general concepts and approaches that are relevant in the context of the thesis. At the beginning of the chapter the concepts, like threat, vulnerability and risk are explained. The impact of security violation, the motivation of the attacker and the types of attacks are clarified. Subsequently the incentives to invest in information security are listed and the economic approaches motivating or demotivating the investments are explained. The different information security investment problems within a firm are discussed together with the factors that influence the investment decision making in different organizational levels. The common approaches that the organizations use to solve the information security problems are introduced. As the majority of the approaches require more or less profound understanding of risks, then the different risk assessment perspectives and risk treatment strategies along with accompanying costs are explained.

Chapter 3 consist of three subchapters. The first subchapter determines whether the small enterprises have an information security investment problem and what the problem is. The second subchapter analyses the existent information security investment approaches to find the methods that the small firms could use to solve their investment problem. The third subchapter suggests a method that the small businesses could follow to make their information security investment decisions.

When elaborating the content of subchapters of chapter three, then in the beginning of the first subchapter the significance of small enterprises to the economy is explained. Subsequently the importance of information systems creating business value is evaluated through the use of e-commerce and e-booking. Following the security and data-protection indicators of the firms are compared with the use of e-commerce among the firms distinguished on the basis of the size of the firm. The data that is used for the analysis originates from the database of Statistic Estonia. Next the small businesses that the thesis is targeted to are defined. The incentives of small firms to invest in information system security are discussed. The organizational structure as a shaper of the information security investment problems is explained. The information security investment problem for small enterprises is defined and explained.

In the second subchapter the information security investment approaches are grouped according to their investment problem. Each approach is briefly described and following aspects analysed: whether the approach is rather theoretical or could be used in practice based on the assumptions given and the methods used; whether the approach solves the investment problem for small enterprises and could it be implemented in practice by small firms.

In the third subchapter a step by step process is proposed and explained that the management of the small business could follow to make their information and information system security investment decisions. Instead of the commonly used asset identification and evaluation the analysis of cash flows is used to estimate the possible negative impact in case of security incident. Beside the well-known ROSI that can be used for calculating the highest return on single risk investment, the risk portfolio approach RORPI, which allows to find the highest return on risk portfolio, is proposed. To demonstrate the suggested information security investment decision making process and the difference of calculating ROSI and RORPI, an illustrative case study is provided. The case study is based on existent business but the business plan and financial measures are modified due to ethical reasons. The information system that is analysed in terms of security is hypothetical considering the circumstances when the firm was established. The security solutions that are proposed as the alternatives for risk treatment are existent security solutions provided in the market and calculated with given market prices.

The thesis contributes to the existent literature and information and information system security investment decision making in many ways:

- The thesis shows that small enterprises have their specifics compared to large organizations and the investment problem for small businesses is not just smaller or more limited, but it is different.
- A step by step method that the management of the firm could apply to make knowledgeable investment decisions concerning information security is developed and explained through case study.
- The use of cash flow analysis for estimating the need for information security investments and when evaluating the impacts of security violation is proposed.
- A risk portfolio investment valuation model RORPI that allows to find the risk treatment alternative which provides the highest return when treating all the considered risks is developed and explained.
- The thesis also provides an extensive analysis of different information security investment approaches that can be used in further research.

2. The Important Concepts Related to Information Security Investments

This chapter presents and discusses the concepts that are relevant in the context of information security investments. The reasons and incentives to invest in information security are explained. The factors that affect investment decisions are discussed. The decision makers and their scope of investment decisions are explored and the general approaches used for solving the information security investment problems are presented.

2.1. The Value and Violation of Information and Information System Security

“Information has become the key resource and even the lifeblood of many organizations.” (Halliday *et al.* 1996: 19) The operations of firms have become more and more dependent on networked computing systems. It is a necessity to maintain accessibility to the resources that are processed and stored in the information system. (Dewri *et al.* 2012) It is critical to provide access to confidential information only to the authorized persons and to guarantee that the information in the system is accurate and complete.

Any element of an information system that has value is defined as an asset (Tsiakis, 2010). Information assets can be tangible including physical infrastructure such as servers, workstations, network infrastructure and software elements or intangible such as relevant business operation information, organizational knowledge, reputation, intellectual property (Bojanc, Jerman-Blažic, 2008a; Bojanc, Jerman-Blažic, 2008b).

The value of an asset may be expressed in monetary terms or determined subjectively (Tsiakis, 2010). The valuation of tangible assets is easier than the valuation of intangible assets (Bojanc, Jerman-Blažic, 2008b). The value of assets is organization specific. The same asset may have different role and importance when providing or delivering particular services in organizations and therefore the value that is offered by or through that asset differs (Shameli-Sendi *et al.* 2016). According to Poore the following factors affect the value of information assets: exclusive possession (for example trade secret), utility (the essentiality to the business operation), cost of creation or re-creation (to create or acquire), liability (it is assumed to be protected due to its nature), convertibility (it has intrinsic value that can be converted to other assets) and operational impact (the effect of absence or incorrectness) (Su, 2006).

The assets are exposed to threats. A threat is any kind of potential harm to the information system, including network failures and natural disasters (Tsiakis, 2010). A threat may be defined as a potential violation of security (Tsiakis, Pekos, 2008). Information security is primarily concerned with protecting or preserving confidentiality, integrity and availability of the system (Gordon, Loeb, 2002b). Confidentiality is ensured when it is non-disclosed to unauthorized persons, integrity is the objective to have non-alteration of content and availability allows the authorized users to access and use the information assets without being restrained by unintentional or malicious acts (Bojanc *et al.* 2012).

The potential violation of any or all of the above mentioned security objectives is present when a threat is exploiting certain vulnerability in the system (Tsiakis, 2010). Vulnerability is a weakness in security procedures or in technical, physical or other controls of an asset (Bojanc, Jerman-Blažic, 2008b). The security failure of an asset has negative consequences – the impact. A threat in combination with vulnerability and impact creates an information security risk. (Schilling, Werners, 2015; Tsiakis, 2010) Risk is a measure of the probability of the undesirable security violation event and the impact or negative consequences of that event (Tsiakis, Pekos, 2008). Security risk of an organization is the sum of threats, vulnerabilities and asset values. Any change in any of these factors change the level of risk. (Jaisingh, Rees, 2001)

2.2. The Cost of Violation of Information and Information System Security

The impact of violation of information system security is not easily definable. Some of the costs related to a security incident are readily assessable, such as resources used for information recovery, others such as loss of reputation or trust, may not be that clearly quantifiable. (Soo Hoo, 2000) The loss due to the cyber breach is dependent on the organization. Identical incidents in different firms at the same industry may have different costs. (Farahmand *et al.* 2005) The cost is also highly dependent on circumstances – the confidential research and development information in the hands of competitor has different consequences than being accessed by a hacker who do not realize the potential value of that information (Soo Hoo, 2000). The information system being not accessible during the time when an organization has to fulfil its contractual obligations has different consequences than when the system is being down during a weekend when people are not working.

There is no standard about which costs have to be included when estimating the loss derived from the security breach. One firm may consider only the costs of replacing the affected resources and recovering data, another firm may value the lost intellectual property cost and IT support time instead. (Martin *et al.* 2014)

It is impossible to create a complete list of things that can go wrong and entail loss due to the cyber incident (Farahmand *et al.* 2005) but there are various loss categories that can be considered when estimating potential cost. Cavusoglu *et al.* (2008) classifies the costs as transitory or short-term and permanent or long-term. Transitory costs incur during the incident period and include the loss of productivity and the costs associated with incident handling. The permanent costs reveal after the incident and affect the future cash-flows of the firm. It includes the loss of existent customers who switch to competitors as well as loosing potential customers. The business partners may repeal the partnership due to the loss of trust. The firm may face legal liabilities and bear the damage from revealing business critical information. The business risk rating may increase to cause the raise of insurance cost and higher capital cost in depth and equity markets. (*Ibid*)

The classification proposed by Bojanc, Jerman-Blažic (2008b) divides the cyber breach costs as immediate and indirect. The nature of the division coincides with the approach presented by Cavusoglu *et al.* (2008). ISF Standard of Good Practice for Information Security classifies the costs according to the business impact which can be tangible or intangible. The impact categories are: financial, operational, customer-related and employee-related. (Su, 2006)

In addition to the difficulty of evaluating all the aspects that are negatively influenced due to the violation of security, the magnitude of the costs is also challenging to derive. Farahmand *et al.* (2005) for example measures the productivity loss as the full lost hours for the number of affected employees. Soo Hoo (2000) instead argues that there may be alternative ways how people can accomplish their work tasks so the productivity loss would not be counted as full lost hours. Soo Hoo (2000) suggests to compare two possible scenarios for cost estimation – one in which the security incident occurs and the second without the security incident. According to Martin *et al.* (2014) firms tend to overestimate the costs of security breach and lost productivity. They assume that employees have alternative tasks which do not depend on affected IT resources and can be executed. Their proposed methodology integrates risk and business continuity management into business process modelling. In order to assess the dynamic behaviour of process over time, they use simulation. Their results show smaller total costs than the outcome from generally used approach where the time during breach is considered as idle time.

The real quality data about costs of cyber incidents is hard to find. The statistics is collected by parties who have incentives to either under- or over-report the failures (Moore *et al*. 2009). The information security business has a motive to exaggerate the loss and the victims of cyber incidents rather downplay the harm fearing to damage their reputation or trust towards them (Moore, Anderson, 2012). A research about consumer attitudes toward data breach notifications showed that the effect of data breach had mild impact. Only 11 percent of the respondents that experienced data breach stopped business relations with the firm, 77 percent were highly satisfied with the response of the firm after the breach (Ablon *et al.* 2016).

2.3. The Attacker and the Nature of the Attacks

The attacks against information security are carried out by so called threat agents. A threat agent can be internal or external – a disgruntled employee, a competitor or anyone who has interests and motivation to attack the information system. (Shameli-Sendi *et al*. 2016) The motivation for different threat agents may differ. The attack may be triggered by revenge, personal satisfaction, gaining competitive information, financial gain, espionage, terrorism (Bojanc, Jerman-Blažic, 2008b). The main motivation is still believed to be the financial gain (Toivanen, 2015). Economically motivated threat agents are assumed to make their decisions to attack based on their effort or cost and the expected gain (Cavusoglu *et al*. 2004a; Dewri *et al.* 2012). Rationally acting attackers also minimize the probability to be targeted and caught by law enforcement (Anderson *et al.* 2013). Hacking has become a business that is engaged with research and development of variety of hacking tools, providing quality control and customer service (Anderson *et al.* 2009).

The strategies of threat agents when selecting their victims have been referred differently in the literature but the essence of those approaches coincides. The National Cyber Security Centre (NCSC, 2016a) divides the attacks as untargeted and targeted. Huang and Behara (2013) classify the attacks as opportunistic and targeted. In case of untargeted or opportunistic attacks the intention is to compromise as many devices, services and users as possible. It is not important who the victims exactly are. Targeted attacks to the contrary are aimed to exploit specific victims. The groundwork before penetrating the system may take months. Very motivated and skilled targeted attacker can also be labelled as advanced persistent threat (APT) for the organization (Bellovin, 2016).

An organization may become a victim of opportunistic and targeted attacks and that may happen simultaneously. Irrespective of the nature of the attack – targeted or untargeted/opportunistic – there are four main stages in common: survey, delivery, breach and affect. At the *survey* stage the threat agent is using available means to find weak points in the system called vulnerabilities that could be exploited. During the *delivery* stage the attacker selects the path to exploit the vulnerabilities. The vulnerabilities are exploited to gain unauthorized access to the system during *breach* stage. At the *affect* stage the threat agent is achieved its goal. The success of the attack depends on whether the attackers meet their goals at different stages or they are blocked. (NCSC, 2016a)

Empirical studies have found that special search engines are used by many attackers to find the targets with certain vulnerabilities – users of particular program or certain version of a program that has functionalities which can be misused (Moore, Anderson, 2012). The Verizon’s Data Breach Investigations Report has estimated that 79% of the security breach victims were attacked only because of having easily exploitable vulnerability present (Shameli-Sendi *et al.* 2016) and not due to their size or importance in the society. Any organization is a potential victim of cyber attack (NCSC, 2016a), no matter how large and famous or small and local an organization is (Gadyatskaya et al. 2016).

2.4. The Incentives to Invest in Information Security and the Economics Behind It

“If there were no threats, security resources would not exist, costs would be lower, profits higher, and entities would have higher equity values.” (Anderson, Choobineh, 2008: 23)

The main incentive to invest in information and information system security is to reduce risk. Risk can be reduced either by lowering the probability of security violation or lessen the impact in case of security incident or doing both. (Böhme, Nowey, 2008; Granadillo *et al.* 2012b) Some concentrate on defending against attackers (Cremonini, Nizovtsev, 2006) by making the life of attackers as difficult as possible (Dewri *et al.* 2012). Others are more focused on reducing the costs (Schilling, Werners, 2015), whether considering mainly the immediate incident costs (Toivanen, 2015) or having a wider perspective and feeling the pressure to invest in order to meet the government regulations (Dynes *et al.* 2005; Dynes *et al.* 2008, Moore *et al.* 2016), to avoid legal liability (Moore, 2010a; Moore, 2010b; Moore, Anderson, 2012; Toivanen, 2015) or the loss of market value (Cavusoglu *et al.* 2008; Böhme, Nowey, 2008).

Although information system security investment is mainly seen as the investment to avoid incidents and prevent loss and not as an opportunity to generate monetary returns (vom Brocke *et al.* 2007; Demetz, Bahlechner, 2013; Enisa 2012), it is also considered as a possibility to earn revenue from new ventures that would have been too risky to be launched without added security features (Kim, Lee, 2005; Magnusson *et al.* 2007; Schehter, 2004; Toivanen, 2015). The security investments can also be viewed as a qualification for business or a prerequisite to be considered as a business partner (Dynes *et al.* 2005; Dynes *et al.* 2008).

The information security investment does not affect only the security of the firm who is investing but it affects the security of its partners as well as the overall security in internet. The connectedness and interdependency of information systems create externalities. Externalities are defined as side effects or economic consequences for third parties. (Anderson *et al.* 2009; Camp, Wolfram, 2004, Moore, 2010a, Moore, 2010b) The externalities can be positive or negative. A compromised computer used to send spam, distribute malware or launch denial-of-service attacks harm others more than the host (Moore, 2010a; Moore 2010b; Anderson *et al.* 2009; Moore, Anderson, 2012). A firm investing in information security creates positive externalities to others keeping them more secure than otherwise. It may in turn discourage to take protective measures themselves and result free-riding. (Anderson, Moore, 2006; Anderson *et al.* 2009). The impact of security investments of a firm often depends not only on its own investment decisions but also on the decisions of others (Anderson, Moore, 2006). The investing firm does not perceive all costs and benefits that ensue from their security investment decisions (Bauer, van Eeten, 2009).

Varian (2004) distinguishes three baseline cases in the context of system reliability which also apply to system security: total effort, where the security depends on the sum of efforts invested by the firms; weakest link, where the security depends on the minimum effort and best shot, where the security depends on maximum effort. Moore *et al.* (2009) states that the security in internet is dominated by the weakest link model where free-riding is likely. Firms "do not bother investing in security when they know that other players will not invest, leaving them vulnerable in any case" (Moore, 2010b: 8).

Florencio and Herley (2013a) claim that the weakest-link game is suitable when a single attacker attacks a single firm, but in internet the crowd of users face a crowd of attackers and the total effort or sum-of-efforts describes the overall security better than the weakest-link model. It excludes the cases where the attacker is motivated to attack specific firm due to emotional, political or financial reasons and not due to the lack of or low level of existent security measures of the firm. In their model the attackers "seek victims in the population rather than targeting individuals" (Florencio, Herley, 2013a: 17).

The model relies on the assumption that the cost of an attack for the attacker decreases when the number of firms to be attacked increases. The attacks may have a fixed cost that is independent of firms to be attacked. Each attacker chooses the attack vector that maximizes his/her expected gain from successful attacks within the population. Different attackers may have different cost structures and therefore the most rewarding attack vector to one attacker may not be the best option for another attacker. However, it is likely that some attack vectors give the best expected return to many while some are most beneficial for almost none of the attackers. If the sum-of-effort of the firms is big enough to make the use of certain attack vector unprofitable or just not profitable enough for the attacker, the firms with low or no defence escape from the attack and can free-ride. (*Ibid*)

All in all rationally behaving firm who is not under targeted attack should ignore the attack vectors that most of internet users are protected against and consider the investments to the measures that deal with attacks where the sum-of-efforts is not big enough to make the attacks unprofitable for the attackers. The difficulty is that a firm does not know where and how much the other internet users have invested in security measures and what are the cost structures of attackers.

Sharing the information about threats and breaches of computer security between firms would lower the total investments that the firms should make to reach any particular level of information security. The hurdle is that firms do not have economic incentives to reveal truthful information. (Gordon *et al.* 2003b) Firms are reluctant to collect and reveal information about security incidents to avoid legal liability (Ryan *et al.* 2012; Soo Hoo, 2000), damage their reputation (Ryan *et al.* 2012; Wood, Parker, 2004; Moore, Anderson, 2012) or encourage the other attackers to choose them as targets (Ryan *et al.* 2012).

At the same time firms may not be even aware of being compromised. Verizon has reported that 69% of detected breaches were discovered by external sources and not by the victim (Gilligan, 2013). The amount of undetected breaches are highly uncertain (Soo Hoo, 2000). The statistics about information security incidents gathered and provided by security vendors or law enforcement agencies has been criticized to favour over- or under-reporting (Anderson *et al.* 2009; Moore *et al.* 2009). Florencio and Herley (2013b: 49) are harsh in their valuation about cyber-crime surveys: "… they are so compromised and biased that no faith whatever can be placed in their findings." The published data about cyber incidents and risks provide only broad indication and hints about the real environment (Biener *et al.* 2015; Magnusson *et al.* 2007). It does not necessarily mean that the amounts of security investments are excessive or not sufficient but it is likely that the investments are not in the right defences in the ideal proportion (Moore 2010a, 2010b). Even if the firms will be willing to share the information about information security incidents, they would preserve the incentive to free-ride on the information security expenditures of others (Gordon *et al.* 2003b).

2.5. Information Security Investment Decision Makers, the Scope of Their Decisions and the Factors that Affect the Decision Making

Information security investment decisions are mainly made to manage the information security related risks. Some researchers emphasize the importance of economic principles at least as much as important as the technical issues concerning information security (Anderson, Schneier, 2005; Böhme, 2005b). Broderick (2001) argues that risk reduction decisions are purely business decisions and frequently unrelated to technology. Dutta, McCrohan (2002) state that security is a management and not a technical issue. "With the increasing dependence of organizations on information and information technology, the borderline between security investment and general risk management is about to blur." (Böhme, 2010:22)

Information security investment decisions are made on strategical, tactical and operational level in organization. At the strategical level the overall security budget is decided. The security investments are weighed against alternative non-security investments (Anderson, Choobineh, 2008; Brecht Nowey, 2013) and decided “How much is enough?” for security spending (Soo Hoo, 2002). The finances of the firm are limited and the security investments have to compete with other projects for funding (Anderson, Choobineh, 2008; Gordon *et al.* 2015b; Huang, Behara, 2013). The problem with comparing the information system security investments with other traditional investments is the difficulty to quantify the economic benefits of security investments (Magnusson *et al.* 2007; Zhuo, Solak, 2014).

Top management has to weigh and decide the balance between the investments that generate revenue with the investments that enable them to earn revenue. There is no universal right balance. “The optimal security budget” for a single firm depends on the risk tolerance of the firm (Anderson, Choobineh, 2008; Radulescu, 2016). Risk tolerance of a firm is not a constant factor – it is dependent on the business goals and the economic context, which are changing over time. The apprehension of business goals and economic context together with the risk perception of the decision makers lead to the level of risk tolerance that the organization is willing to take. (Radulescu, 2016)

Economic theories model the decision maker as risk neutral or risk averse. Risk neutral decision maker accepts the probable losses around their expected values and favours equally the reduction of losses and security costs. Preventing a euro of losses is not preferred to a euro reduction in security costs and vice versa. The actual loss for one period exceeds or is less than the expected loss but over multiple periods the average loss is equal to the expected loss. The optimal budget for the risk neutral decision maker is found when the marginal (the incremental) cost of security measures is equal to the marginal value of expected loss. (Anderson, Choobineh, 2008)

The decision maker is seen as risk averse if the expected or potential loss (a period loss that is greater than the expected value) that is acceptable has upper limits. It is a realistic occasion when a security incident has for instance low probability but large impact. The firm may be seriously impaired or jeopardized if the incident occurs. The security budget of risk averse decision maker is larger compared to the optimal budget for risk neutral decision maker to limit the magnitude of possible losses. (*Ibid.*)

Malik (2001) has divided the decision makers to three categories: the informed, the risk takers and the security ignorant. The informed decision maker explores the security issues before making the investment decisions. The risk-taker is aware of the security issues but is willing to take the risk. The ignorant decision maker understands minimally and prefers to avoid funding the security issues. (Kim, Lee, 2005)

When the question of "How much to invest?" is answered and the security budget is decided, the next question is for the next level: "Where to invest?" To decide "What combination of plans, personnel, procedures, guidelines and technology will maximize the protection of information assets?" at the given security budget (Anderson, Choobineh, 2008: 27). The budget constraint does not allow to implement all possible security measures, instead a subset of the measures has to be chosen while estimating the potential damage to the system due to the unpatched weak points (Dewri *et al.* 2012).

The selection of security measures is a complex issue as it requires the consideration of huge range of interdependent factors where the actual impact to the factors with different countermeasure alternatives is difficult to know or predict (Baldwin *et al.* 2013). The benefits of the countermeasures depend on expectations about attack vectors, frequency of attacks and the efficacy of the countermeasures (Butler, 2002; Cremonini, Martini, 2005; Tsiakis, 2010), which are difficult to estimate (Schilling, Werners, 2015).

People tend to use heuristics or rules of thumb when making decisions under uncertainty. It is remarkably effective but may also lead to systematic biases in decision making. A well-documented bias is the tendency to find and see evidence that supports their viewpoint rather than contradicts it. The bias functions as a pre-existing preference which leads to disregarding contradicting information and supporting the preferred alternative. (Baldwin *et al.* 2013)

The information security managers and system administrators make the decisions about security investments intuitively (Butler, 2002) relying on their experience and knowledge (Bistarelli *et al.* 2007). The information security managers have affirmed in their interviews conducted by Dynes *et al.* (2005) that their decisions are based on their own past experience, experiences of trusted colleagues, consultants, trade magazines, web search and other mass media. Ryan *et al.* (2012) state that information systems can be reasonably secured if the budget is adequate and the responsible manager is appropriately educated. "However, not all managers are equally educated or experienced, nor are all adequately funded." (*Ibid:* 778)

An alternative to insourcing security related activities is to improve the security by outsourcing the functions or processes. There is Moral Hazard problem that is linked to security outsourcing (Böhme, 2010). The problem grounds on outsourcing partner’s impulse to shirk secretly in order to increase his/her profits (Ding *et al.* 2005). “Security is not visible, it’s a trust good.” (Böhme, 2005a: 1) It is also stated that the information systems are prone to fail when the person or organization who is responsible for defending the system do not suffer or bear the full costs that are caused due to the failure (Anderson, Moore, 2006; Moore, 2010a, Moore, 2010b, Moore, Anderson, 2012, Anderson *et al.* 2009).

Irrespective of the person or organization who protects the information security on operational level, the key role and the main responsibility lies on the management of the firm whose information system has to be protected. According to the stakeholder theory the information security investments are driven by three main stakeholders: end users, information specialists and organizational decision makers (Toivanen, 2015). The stakeholders have different needs and demands, they have different drivers for their decision making concerning information security investments. Each of them promote the proposals that have greatest value for themselves. It is essential for the business continuity that the investment proposals are aligned with business strategy. (*Ibid*) No other stakeholder has better understanding about long-term business strategy than the top management, therefore it is essential that the management understands the importance of information security and takes the key role protecting the information systems.

2.6. Approaches that Enterprises Employ to Make Information Security Investments

Firms have different views how to decide about information security investments. Dynes *et al.* (2008) distinguished three broad views based on the interviews with security managers: The Sore Thumb Paradigm, IT/Business Risk Paradigm and The Systemic Paradigm. According to The Sore Thumb Paradigm the investment decisions are made without detailed risk assessments, following general and incomplete risk information originating from mass media and peer groups. The information security investments are prioritized according to the harm that the attacks and incidents cause. It is considered as mainly reactive approach that is common in smaller firms and sectors which are less reliant on IT.

The IT/Business Risk Paradigm gets its input mainly from IT managers and staffers from its own organization. The prioritization of the investments is made by the director of information security based on estimates of likelihood of the attacks, the resulting loss and the costs of countermeasures. The IT risk portion of the paradigm considers the protection of information technology assets as networks, servers, desktops. The business risk portion of the paradigm examines the impact of the risks on business processes. The assets that are protected are business assets as customer order system, enterprise resource planning system. The security initiatives are related to ensuring business continuity. The IT/Business Risk approach can be reactive, proactive or combined. (Dynes *et al.* 2008)

The security initiatives in the third approach – The Systemic Paradigm – are not considered separately from business processes. The prioritization of investments evaluates IT projects which automatically include security considerations. The paradigm is proactive in nature. (*Ibid*)

Moore *et al.* (2016) have stated that historically, most firms have made their information system security investment decisions based on industry best practices, without necessarily understanding their cyber risks. The interviews with security officers have showed that the security of some firms is largely driven by best practices of the industry and “the must do approach”. If the business side has decided to be in the market, then the size of the compliance costs or return on security investment are not an issue. (Su, 2006)

A trade publication Secure Business Quarterly highlighted four approaches that were used for making decisions concerning information technology investments. The first and most popular approach was The Fear, Uncertainty, and Doubt (FUD) which motivated firms to invest in basic security solutions without understanding their actual needs for security investments. The second approach focused on costs of deploying security measures considering the costs as overhead for the organization. The third approach relied on the outcome of traditional risk or decision analysis, identifying the potential risks, estimating the likelihoods of attacks and calculating the expected loss. The fourth approach was considering investments to non-technical measures, such as insurance. (Cavusoglu *et al.* 2004a, Cavusoglu *et al.* 2008) Majority of the above introduced approaches involve more or less profound risk management which will be explained next.

2.7. Risk Management Process, the Costs and Challenges

Risk management is a process of assessing risks along with selecting and implementing security measures to reduce risk (Bojanc *et al.* 2012). Risk management involves analysis of risks, estimation of potential benefits and consideration of alternatives when dealing with risks and implementation of chosen security measures (Sklavos, Souras, 2006). Risk management is a continuous and challenging process as the risk factors are constantly changing (Shameli-Sendi *et al.* 2016). There are different frameworks about information security risk management. Many of them have been developed to manage the security in large organizations such as military or governmental institutions. (Halliday *et al.* 1996) Fenz *et al.* (2014) analysed current risk management approaches (NIST SP 800-30, ISO 27005, EBIOS, OCTAVE, CRAMM, FAIR, ISAMM, ISF) and showed that the differences between the methodologies are not significant.

National Institute of Standards and Technology (NIST, 2012) divides the risk management to four processes: framing risk, assessing risk, responding to risk, and monitoring risk. The first process – framing risk – is about developing the risk management strategy. It declares how the organization intends to assess, respond and monitor risk (*Ibid*). The second process – risk assessment – is a process to identify, characterize and understand risks (Soo Hoo, 2000). The third process involves mitigation, acceptance, transference/sharing or avoidance/rejection of risks and the fourth process implies the monitoring of implemented security controls and the existing risk levels (NIST, 2010).

2.7.1. Risk Assessment

Risk assessment is composed of risk analysis and risk evaluation. Risk analysis consists of three steps: resource identification and valuation, risk identification and risk measurement. There are three alternative perspectives how to analyse the risks: to have asset-driven, service-driven or business-driven perspective (Shameli-Sendi *et al.* 2016).

The asset-driven is the most common approach and the majority of the tools provided in the market support that perspective. Resource identification and valuation identifies the valuable assets. (Shameli-Sendi *et al.* 2016) Not all the assets should receive the same level of attention as the value of assets being under threat and the probability of being exploited differs (Demetz, Bachlechner, 2013). To facilitate the focus on most critical assets, the assets can be classified into discrete categories or class of assets. The amount of categories may vary. An example of three-class model is to group the assets under critical (for example financial data), moderate (such as purchase order data) or low-asset (such as product information release) class. (Bojanc, Jerman-Blažic, 2008b)

Risk identification recognizes all possible risks to the important assets. A risk in this stage is defined as a relationship between a vulnerability and a threat, thus the vulnerabilities of valuable assets and the threats that may endanger the assets are identified. There are different methods for identifying and assessing vulnerabilities: vulnerability scanning, penetration testing, code review enhanced with on-site interviews, questionnaires, document reviews and physical inspection. Threats are identified and documented through threat modelling (Shameli-Sendi *et al.* 2016). Each of the methods consider different factors and controls to give feedback about strengths and weaknesses of the system (Farnan, Nurse, 2016).

Risk measurement is the third step in risk identification process. For measuring the risks the organization needs to choose a model which specifies the relationship among the risk factors such as resource value, vulnerability effect, threat impact, threat likelihood. In order to avoid overestimating the risks it is essential to identify and consider existing and already planned security measures. (Shameli-Sendi *et al.* 2016)

“The focus of this (asset-threat-vulnerability) model is mainly within the IT department and does not take into account business issues.” (Halliday *et al.* 1996: 20) It is a time-consuming analysis that may become more expensive than the acceptance of risks (*Ibid).* It is assessed as an error-prone task if the amount of work dedicated to determine the monetary values to assets, to estimate the threat frequencies and cost of controls, is not sufficient. The output from risk assessment may show a pile of risks that have extremely close estimates which makes the prioritization of the risks difficult. The proximity of the risks makes the risk reduction phase inefficient as well. (Shameli-Sendi *et al.* 2016)

The service-driven approach identifies the important services and service packages in the organization. The threats and vulnerabilities are assessed in the context of services and not for individual assets. As there are less services than assets in the organization, the analysis is less time-consuming and better managed compared to asset-driven perspective. The service-driven perspective is better linked to business revenue earning. (Shameli-Sendi *et al.* 2016)

The business goals and the processes to support and achieve the goals are at the focus of **business-driven** risk assessment perspective. The idea is to identify and analyse the business processes and assign value to them according to how it is linked to the business goals. The vulnerabilities and threats that endanger those processes are identified and assessed. (*Ibid*) The impact of violation of availability, integrity and confidentiality to the critical business processes as well as to the information systems supporting those processes is evaluated (Halliday *et al.* 1996). The valuation of the processes are directly linked to the business revenue (Khanmohammadi, Houmb, 2010).

There are several advantages to business-driven perspective. As this framework is based on the classics of business management – Michael E. Porter's value chain model – it is much more comprehensible for the top management of the organization, compared to the conventional technology oriented asset-threat-vulnerability-model. It is effective in terms of time, cost and resources as the detailed analysis of assets, possible threats and vulnerabilities is not needed. The focus areas are set by the important business processes. It also supports business process re-engineering as well as the business continuity planning which would otherwise be performed as separate analysis. (Halliday *et al.* 1996)

Another important aspect in risk assessment is the chosen approach to appraisement, which can be quantitative, qualitative or the combination of those called as hybrid (Shameli-Sendi *et al.* 2016) or semi-quantitative (NIST, 2012). Quantitative analysis is a mathematical approach to assign numerical value to the object that is measured (Tsiakis, 2010). The use of quantitative metrics is well approved by management as the approach is based on independent objective processes and metrics such as monetary value, percentages and probabilities (Farahmand *et al.* 2005). The advantages of quantification in general are its accuracy, objectivity and comparability. "Quantification is the basis for calculations and statistical analyses." (Brecht, Nowey, 2013) The problematics of the issue is that the statistical information does not reflect the present neither the future situation as the evolution of quickly changing threat environment is ahead of statistics (Ryan *et al.* 2012). Quantitative risk analysis is also time-consuming and assigning costs to risks and numerical benefits to countermeasures can be complex (Farahmand *et al.* 2005).

An alternative to quantitative appraisement is qualitative risk analysis, which determines the relative values instead of exact financial values (Bojanc, Jerman-Blažic, 2008b). The proponents of qualitative risk analysis approve its simplicity (Farahmand *et al.* 2005). The risk assessment is based on non-numerical categories or levels such as very low, low, moderate, high, very high (NIST, 2012). The qualitative approach gives approximate estimations that are subjective in nature and heavily dependent on the quality of the knowledge and experience of assessors (Farahmand *et al.* 2005). The assessments performed by data and application owners may suffer from overconfidence effect which makes the outcome of risk, probability, threat and impact estimations biased. Overconfidence effect is the tendency to see the risk estimations far too optimistic. (Fenz *et al.* 2014) The biases and limitations derived from the assessors may make it difficult to rely upon the assessment (Ryan *et al.* 2012). The approximation can make the prioritization of risks difficult as the outcome from the assessment about different risks may range slightly (NIST, 2012).

The hybrid or semi-quantitative risk appraisement is the combination of quantitative and qualitative approach to overcome the main weaknesses of the above mentioned approaches (Shameli-Sendi *et al.* 2016). It applies a set of methods, principles or rules, using bins (such as 0-15, 16-35, 36-70, 71-85, 86-100), scales (1-10) or representative numbers, which can be easily translated into qualitative terms at the same time allowing also relative comparisons between and within bins or scales. The categories or levels need to be clearly defined and characterized to minimize the errors when determining the value during assessment. (NIST, 2012) The decision of the appraisement approach is organization-specific, depending on decision-makers preferences, availability of data and financial resources (Shameli-Sendi *et al.* 2016).

After the risk analysis is completed the risks should be evaluated. Risk evaluation is determining their significance to the organization. The identified risks should be prioritized according to their relative probability of occurrence and the magnitude of impact to make decisions about how to cope with the risks. (*Ibid*)

2.7.2. Responding to Risks

There are four strategies to manage the risks: accept, avoid, transfer or mitigate (Sklavos, Souras, 2006). **Risk acceptance** also named as “risk retaining” (Bolot *et al.* 2009) means that the organization is aware of possible consequences and chooses to do nothing about the risk (Shameli-Sendi *et al.* 2016; Sklavos, Souras, 2006). It is a reasonable strategy if dealing with the risk would cost more than the possible loss from the security incident (Bojanc, Jerman-Blažic, 2008b).

Risk avoidance entails elimination of the source of the risk or the possibility that the source could be attacked. It is a suitable strategy if the severity of the impact exceeds the benefit from using the source in that particular way. (*Ibid*) If a computer contains highly confidential information for an organization, keeping the computer without external or removable storage and disconnected from any network and allowing the access to the data only by authorized persons being physically present is not comfortable neither efficient, but the risk of violation of confidentiality through network attack or through the use of external or removable storage is avoided.

With the **risk transfer** an organization assigns the responsibilities and liabilities to a third party. It may imply that part or all of the activity and the accompanied risk is outsourced to another organization or the risk is transferred to an insurance firm. (Shameli-Sendi *et al.* 2016; Bojanc, Jerman-Blažic, 2008b)

The fourth and the most prevalent strategy is to **mitigate the risks** (Sklavos, Souras, 2006). Risk reduction means that the probability of the risks and/or the consequences are controlled and limited in some way. The risk level is reduced by implementing appropriate technologies, tools and executing security policies. (Shameli-Sendi *et al.* 2016)

Risk treatment in organizations may involve a combination of those strategies: some of the risks may be avoided, some of them may be transferred, certain risks are mitigated and the rest are accepted (*Ibid.*). There always remains a residual risk. Even the most advanced countermeasures cannot block attacks completely as new vulnerabilities and threats emerge (Sawik, 2013; Anderson, Choobineh, 2008). “Perfect security is impossible, but even if it were, it would not be desirable.” (Moore, 2010a: 7; Moore, 2010b: 6) There exists an optimal level of insecurity, where the benefits from additional security measures do not compensate the reduction of efficiency in operations. (*Ibid*) Complete information security of a firm is impossible without hindering the normal business activities (Huang, Behara, 2013). Another reason is the economic inefficiency if the investments in information security are above optimal level. The third reason is that the financial resources are always scarce and there is no incentives to invest in information security more than necessary.

Besides the inefficiency costs that result from implementation of security controls such as reduction of throughputs, access, transparency (Anderson, Choobineh, 2008; Al-Humaigani, Dunn, 2004) the main costs of mitigation are associated with acquiring, implementing and maintaining the countermeasures (Al-Humaigani, Dunn, 2004). It is not only about the technical cost factors as equipment purchasing and licencing price, repair and warranty but it also includes the costs of salaries and training costs of staff (Kim, Lee, 2005). It is also relevant to consider sunk costs, which cannot be recovered with withdrawal of countermeasures. The equipment could be sold or repurposed, the staff could be relocated or fired, but the expenses of training cannot be retrieved. (Böhme, 2010) Another challenge is the distinction of information security investments from overall information technology investments. Due to the cross-divisional nature of resources, it may not be easy to define what part of the total costs of information technology and related personnel are accountable to information security. (Brecht, Nowey, 2013)

Outsourcing of information security activities or processes appears to simplify the cost calculations. Outsourcing have a potential to achieve certain security level with lower costs (Ding, Yurcik, 2006). According to Rowe (2007) the economies of scale and improved information sharing allows the security providers achieve higher level of security with less costs. At the same time outsourcing for a firm is inherently costly as transaction costs are added (Hui *et al.* 2012). Security outsourcing is accompanied by following transaction costs: searching cost which refers to money, time and effort spent to find a suitable outsourcing partner; contracting cost that comprises money, time and effort to develop a service contract; setup cost that is a related to purchasing and configuring equipment to support the security services; monitoring cost that refers to money, time and effort to check the performance of outsourcing firm; coordination cost that includes money, time and effort spent on communication; switching cost that are expenses proceeding from switching from one outsourcing partner to another (Ding, Yurcik, 2005). High switching costs may create “lock-in” effect for the firm and may be the barrier for changing the security service provider even if the cost of alternative security service itself is lower than the existent service at the same security level.

Transaction costs are often hidden and forgotten and not related to information security (Brecht, Nowey, 2013).

The organization who has decided to mitigate the risks has various security measures available in the market. There are prevention measures which purpose is to reduce the success probability of the attacks and increase the cost to attack. Examples of those measures are antivirus protection, firewall, access control mechanisms. There are detective measures which should detect the attacks as fast as possible to disrupt the attack, catch the attacker and minimize the negative impact of the security incident. Examples of detective measures are IDS, IPS systems, secure log mechanisms. The third type of security measures are corrective also named as recovery measures. The purpose of corrective measures is to minimize the loss after an attack – to re-establish the normal functionality of the system, to have procedures and channels for communication with personnel and public. The examples of corrective measures are regular backups, free-of-charge replacement of equipment, redundant systems, insurance. (Buldas *et al.* 2006; Bojanc *et al.* 2012)

It is a challenge to choose the right strategy and right combination of security measures. It makes it even more difficult as the different layers of controls may result conflicting interactions reducing the overall security (Gilligan, 2014).

Only the risks that are accepted do not demand any investment decisions to be made. All other choices in order to be enforced need different amount of additional activities and resources by the organization.

2.8. Summary of Key Issues Concerning Information Security Investments

The importance of information and information systems along with their security has grown over the past years because more and more business critical processes and value creation is supported by information systems. At the same time the attacking has become a business too. The attackers conduct research, develop hacking tools and provide customer service. Although there exists different motives to attack the information systems, the main motivation is believed to be the financial gain. The organizations may be targeted by the attackers because of who they are and they may be attacked just because of having certain vulnerabilities present. Attackers take the advantage of the “open doors” and “windows” that are carefully looked for or opportunistically found.

Why to Invest?

- Reduce the risk
- Enable to do the business

The main incentive to invest in information and information system security is to reduce the risk of security violation either by lowering the probability of the security incident or lessen the negative impact in case the incident occurs or doing both. The negative impact may involve different costs. Some of the costs may be directly attributable to the security violation, like costs related to restoring the information system or legal liabilities, governmental penalties, others are not so obviously relatable, like loss of customers or market value due to the loss of trust.

Although the main motivation is to reduce the loss deriving from the security violations, the information security investment can be also seen as a business enabler – as an opportunity to earn revenue in a way that would not be possible without the security investments or an opportunity to be considered as a qualified business partner.

Why Not to Invest?

- To take the opportunity to free-ride
- To take the chance of having uncommon vulnerabilities

Security and lack of security of information systems affect not only the organization who decides to invest or not to invest in security but all its clients, partners and the overall security in internet. The connectedness and interdependency of information systems create externalities for third parties, which may discourage the firms to invest in information security and prefer to free-ride. According to the weakest-link model the free-riding is likely because the security depends on the organization who contributes to the security least and therefore none is willing to invest leaving everyone vulnerable.

Each financially motivated attacker wants to maximize his/her gain from successful attacks. The more common certain vulnerability is, the larger is the population that can be attacked and the more promising is the receivable gain. If the firm is not under targeted attack and the vulnerabilities that are present in the information system are uncommon, then the firm is quite safe because exploiting rare vulnerabilities is not profitable enough for the attackers. The difficulty is that an organization does not have information about how much and where the other organizations and internet users have been and will be investing as well as they do not have the information about the cost structures of different attackers.

What Are the Information Security Investment Problems?

Information security investment decisions are made on different levels of organization. Larger organizations have usually more levels of management whereas small firms have usually no levels between management and staff level employees. Each organizational level has its own needs and demands, responsibility as well as different drivers for decision-making.

Although the information security investment incentives may flow bottom up between the organizational levels, the financial resources that can be used for the investments are allocated top down. The investment problem for the top management is to decide: How much to invest in information security? At that level the information security funding is competing for the financial resources with other investments that the firm has. The optimal security budget for the firm depends on the risk tolerance of the firm which is dependent on the business environment, business goals and risk perception of the decision-maker.

When the size of the budget is decided, then the next level in the organization has the investment problem: Where to invest? What combination of plans, personnel, procedures and technology maximizes the security within the budget constraint? The selection of countermeasures is a complex issue where the level of uncertainty is high. The investment decisions are often made intuitively based on experience and former knowledge.

How Are the Investment Problems Solved in Practice?

Information security investment problems are solved proactively – before the risk occur or reactively – after the risk has occurred. Proactive essential investment allows to prevent the possible attack or minimizes the negative impact when the attack occurs. That implies investing in right measures at the right extent, which can be accomplished when the organization understands its risks well.

Despite knowing this, the level of understanding the risks before making the investments varies between having a good understanding and having no idea. The Traditional Risk-Decision analysis approach or IT/business Risk Paradigm together with the Systemic Paradigm where the security is already embedded to information technology investments represent the view where the risks are well analysed.

Making the investments based on industry's best practices or according to the Sore Thumb Paradigm do not mean that the risks are necessarily understood. The Fear, Uncertainty and Doubt (FUD) investment approach and solving the investment problem with buying the insurance can be performed without knowing anything about the actual risks.

Investment Decisions Concerning Risk Treatment: the Input and the Output

Good investment decisions concerning risk treatment require good risk assessment. Risk assessment and the strategies how to respond to risks are a part of risk management process. Conducting the risk assessment and responding to risks do not require full implementation of information security risk management framework.

The most common risk assessment approach is the asset-threat-vulnerability-driven approach which defines valuable assets, identifies the vulnerabilities of those assets and determines the threats that may endanger the assets through exploiting the vulnerabilities. The risk in terms of impact and likelihood is estimated. The service-driven risk assessment identifies important services instead of assets and the business-driven approach analysis the business processes and assigns the value according to the business goals.

The outcome from risk assessment is the input to investment decision making model. The decision making model may give the risk treatment investment answer with different level of refinement. The model may solve the investment problem defining the suitable risk treatment strategy or a combination of it – to mitigate, transfer, avoid or accept the risk. The model may solve the problem of overall allocation of resources – to choose the combination of preventive, detective or recovery measures; or it may give the answer which set of specific countermeasures to invest in. Every option that is weighed against its alternatives has its own benefits as well as costs.

3. Information Security Investment Approach for Small Enterprises

The third chapter has three objectives. The first objective is to determine whether the small enterprises have an information security investment problem and what the problem is. The second objective is to analyse the existent information security investment approaches to find the methods that the small businesses could use to solve their investment problem. The third objective is to suggest a method that the small firms could follow to make their information security investment decisions together with applying the risk portfolio approach proposed by the author of the thesis.

3.1. Small Businesses and Their Information Security Investment Problem

The goal of the subchapter is to explain: What is a small enterprise? What is the significance of small enterprises in the economy? What is the importance of information systems supporting the business processes of small enterprises and how is the security taken care of? What is the small enterprise in the thesis context? Does this small enterprise have reasons to invest in information system security and what is the investment problem for that firm?

3.1.1. Significance of Small Enterprises, the Importance of Information Systems Supporting Value Creation and the Security Issues

The Distinction and Distribution of Micro, Small, Medium and Large Enterprises

Defining the enterprises according to their size is not uniform all over the world. According to the EU recommendation (2003/361) the firms with less than 10 employees and with annual turnover not exceeding 2 million Euros are defined as micro enterprises. The amount of employees in small enterprises are ranging from 10 to 49 and in medium-sized firms between 50 and 249 on the condition that the yearly turnover in small firms remains below 10 million Euros and in medium-sized firms less than 50 million Euros. In European Union 92.8% of the firms who are economically active (excluding the financial sector) are micro enterprises; small enterprises account for 6%, which makes nearly 99% all together (Muller *et al.* 2016).

The situation in Estonia is largely the same. The share of micro enterprises is 91% and small enterprises 7.6% among the economically active firms, which makes also nearly 99% together. The proportion of firms according to their size is presented in Figure 1.

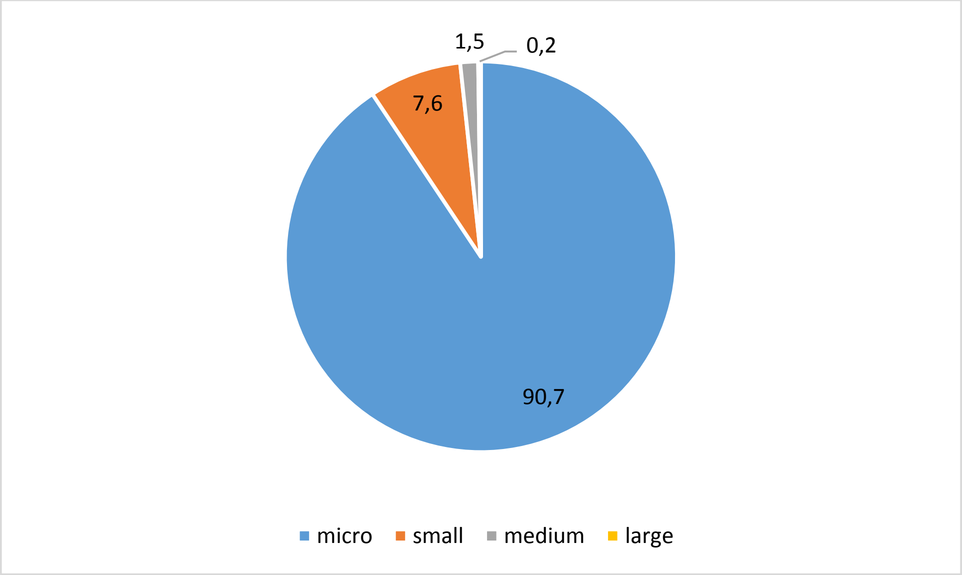


Figure 1. The proportion of micro-, small-, medium- and large enterprises in Estonia in 2015

Micro and small enterprises create together more than half of the total turnover that is generated by the firms in Estonia and they hire more than half of the employees working in Estonian economy (FS001, 2015). The share of turnover according to the size of the firm is presented in Figure 2.

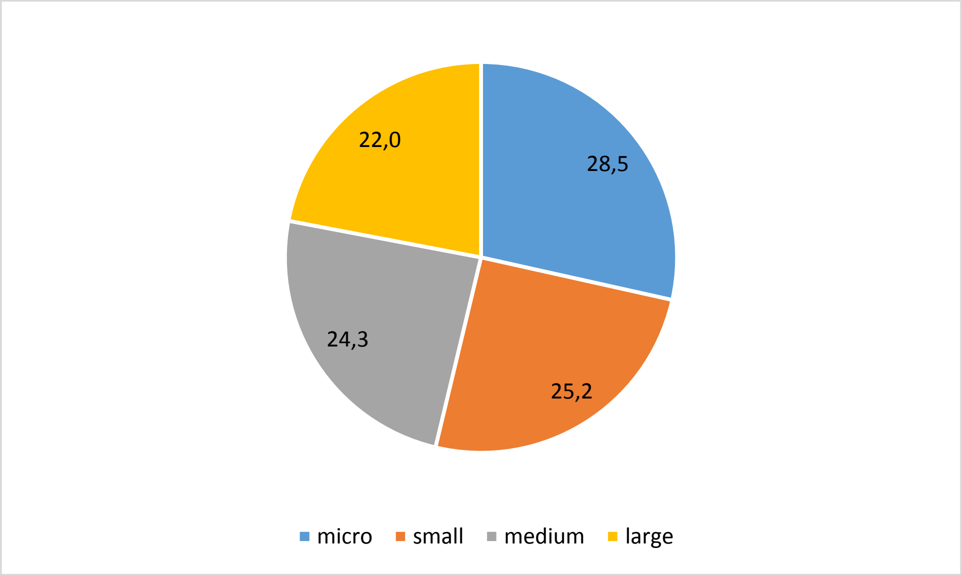


Figure 2. The share of turnover of micro-, small-, medium- and large enterprises from total turnover generated in Estonia in 2015

The proportion of employees working in micro, small, medium and large firms is presented in Figure 3. All the percentage-calculations concerning Figure 1-3 are done by the author of the thesis using the data set FS001 (2015).

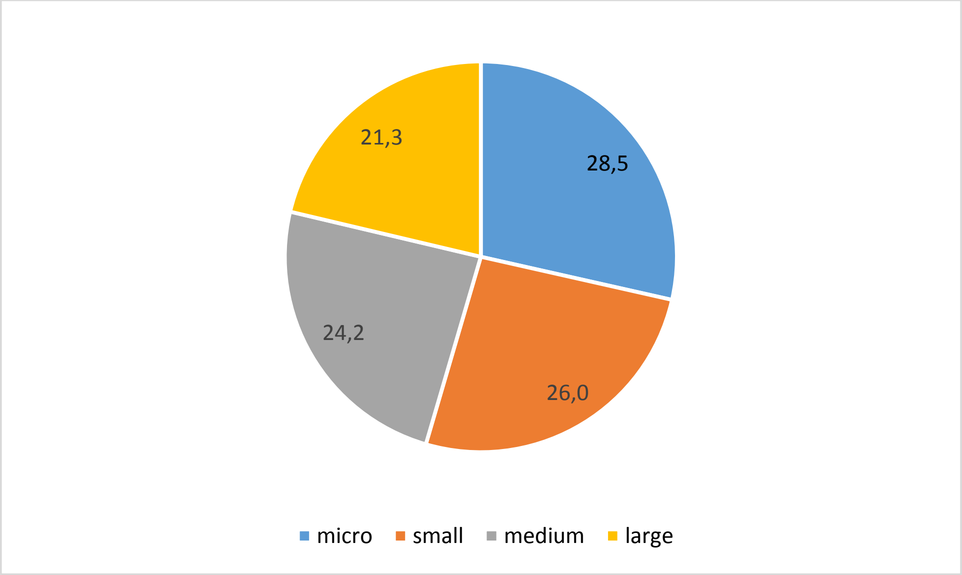
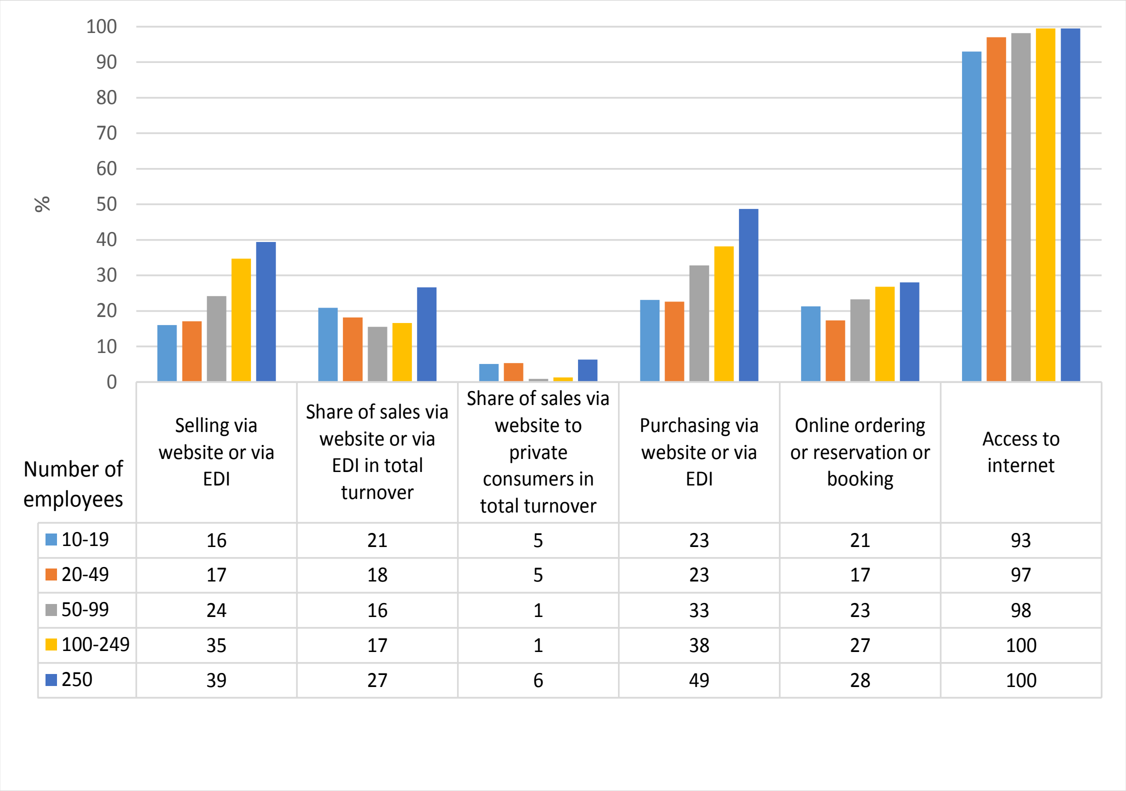


Figure 3. The allocation of employees among micro-, small-, medium- and large enterprises from the total of employees in Estonia in 2015

The Use of E-commerce, E-booking and Internet

There is no statistical data showing directly how embedded the information systems are to support the business critical processes and value creation. Nevertheless the use of e-commerce and having websites that allow online ordering or booking indicate how important the digital channels are for businesses. The "access to internet" shows how common is the use of internet in business communication. The use of e-commerce (IC0081, 2017), ordering or booking via websites (IC008, 2017) and access to internet (IC004, 2017) among the firms grouped according to the number of employees is presented in Figure 4.

Although the share of enterprises selling and purchasing via website or via Electronic Data Interchange (EDI) is two times higher among large firms than among the small firms, then the overall number of small firms selling and purchasing via those channels exceeds about three times the quantity of medium-sized firms and about 15 times the number of large firms. Among the firms who are selling via website or via EDI, the share of those sales in total turnover is almost no different on the basis of the size of the firm. The share of sales to private consumers via website in total turnover is the same among small firms and among large firms. The online ordering or booking option on their website is neither remarkably different among small, medium nor large firms. The high rate of “access to internet” shows that almost every firm regardless of its size uses internet for its business purposes.



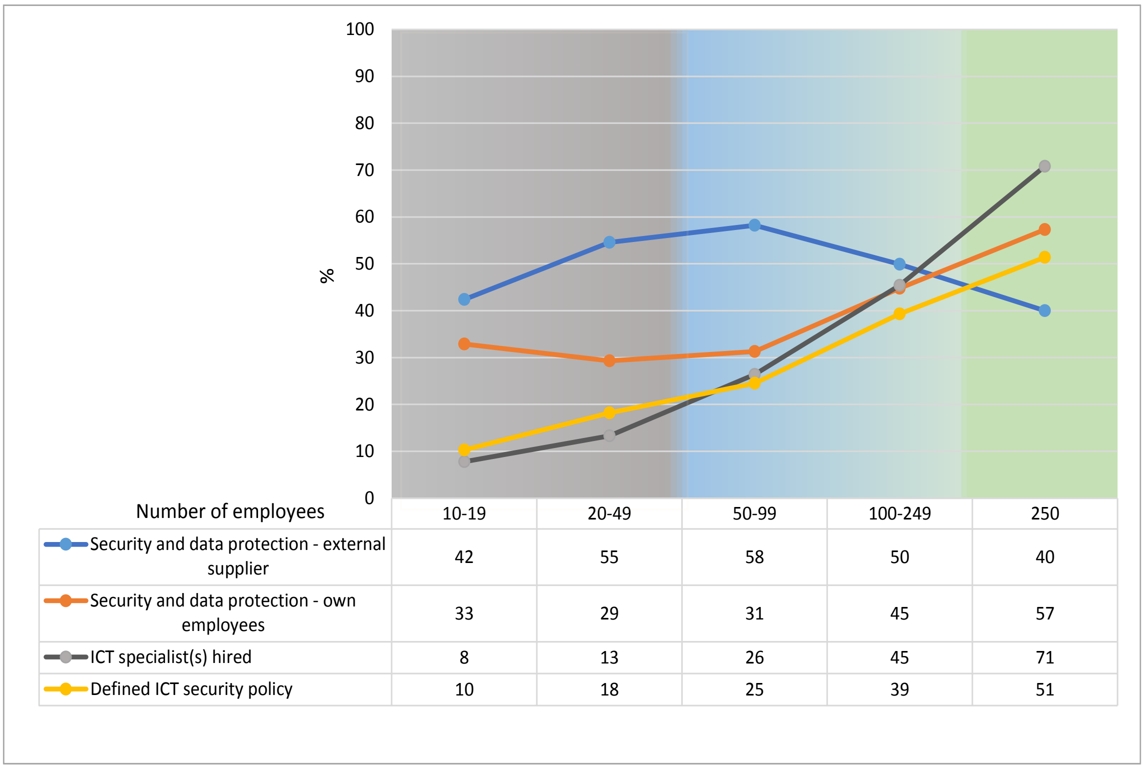
Number of employees	Selling via website or via EDI	Share of sales via website or via EDI in total turnover	Share of sales via website to private consumers in total turnover	Purchasing via website or via EDI	Online ordering or reservation or booking	Access to internet
🟦 10-19	16	21	5	23	21	93
🟧 20-49	17	18	5	23	17	97
⬜ 50-99	24	16	1	33	23	98
🟨 100-249	35	17	1	38	27	100
🟦 250	39	27	6	49	28	100

Figure 4. The use of e-commerce, ordering or booking via websites and access to internet

The Security Policy and the People Engaged in Security and Data Protection

When the utilization of e-commerce and e-booking possibilities do not show drastic differences among small, medium and large enterprises, then the resources and competence allocated to security have remarkable differences depending on the size of the firm. The data concerning the share of enterprises who have hired information technology specialist(s) (IC138, 2017), who have their own employees or external suppliers taking care of security and data protection (IC139, 2015) and who have formally defined security policy (IC140, 2015) is presented in Figure 5.

There is almost linear positive correlation between the size of the firm and the information technology specialist(s) hired. The almost same linear relation exists between the defined security policy and the size of the firm. It is interesting that the share of the small enterprises who have their own employees taking care of security and data protection exceeds substantially the share of small enterprises who have an information technology specialist hired. Unfortunately the data set do not clarify the profile of the employees who are engaged in security and data protection.



Number of employees	10-19	20-49	50-99	100-249	250
Security and data protection - external supplier	42	55	58	50	40
Security and data protection - own employees	33	29	31	45	57
ICT specialist(s) hired	8	13	26	45	71
Defined ICT security policy	10	18	25	39	51

Figure 5. Security policy and human resources allocated to security and data protection

When considering the share of the small firms that have their own employees and the share of the small firms who have external supplier taking care of security and data protection then there still exists 16-25% of small firms where the security and data protection is not covered by anyone.

The Relevance of Small Enterprises, the Importance of Information Systems and the Security

The volume and the scope of business activities of micro and small enterprises in Estonia are not micro neither small. It cannot be said how much the business processes and value creation in small firms is supported by information systems but the data about e-commerce can give some indication. Although the e-commerce among large firms is more widespread than among small firms, then the total amount of small firms selling or purchasing via website or EDI is many times higher. Small firms are also active providing online ordering and booking for clients. At the same time the level of security and data protection in small firms is dubious. While only one small firm out of seven has hired an information technology specialist, then it is questionable that the one third of the small firms who take care of their security and data protection can do it reliably. According to the statistics a quarter of small firms do not have anyone taking care of their security or data protection. There is no data about micro enterprises but there are no causes to believe that the information security in micro enterprises is better off compared to the small firms.

3.1.2. The Incentives to Invest in Security, the Context and the Information Security Investment Problem for Small Enterprises

The Small Enterprises that Are at the Focus of the Thesis

The precise distinction of micro, small or medium-sized firms according to the EU recommendation is not relevant in the context of the thesis. The thesis concentrates on economically active firms whose business critical processes and value creation is supported by information systems but who are small enough to:

- Not have resources for hiring a security competent IT specialist, not to mention to have resources for forming an IT department;
- Not have hierarchical structure and different departments with their own budgets;
- Not have resources for outsourcing the information security risk management;
- Not draw the attention of financially motivated targetiers, aiming specific organizations.

The (Non-)Existent Research about Information Security Investment Problem of Small Enterprises

The amount of research which is relevant in the context of the thesis concerning small businesses and information risk management is scarce. Dimopoulos *et al.* (2004) and Dimopoulos, Furnell (2005) have listed the main issues that small and medium-sized enterprises face when dealing with information security. The characteristics are following:

- They believe to be not targeted by attackers and the anti-virus software is considered as sufficient for protection.
- Information security does not have high priority.
- ICT staff is small and untrained.

- The SMEs have relaxed culture and the formal security policies are absent.
- They do not have either business continuity or disaster plans.
- They do not know where to start and the complex security solutions are confusing for them.
- They have constraints in terms of time and finances when investing in information security.
- When making information security investment decisions they rely on the information provided by the vendors, consultants or on a single system administrator.

The author of the thesis has not discovered any paper which focuses on the information security investment problem of small enterprises – the question that the small firms have to answer to make their information security investment decisions. The following work is the analysis of existent research presented in Chapter 2 in the context of small enterprises, backing it with the statistics discussed in subchapter 3.1.1.

The Information Security Investment Problem for Small Enterprises

More than 90% of the enterprises in Estonia have access to internet. About one fourth of the small firms are using e-commerce and are taking online orders or reservations from their clients. Being a part of interconnected information technology network opens the firms to potential attackers. It is reasonable to believe that the vast majority of small enterprises do not experience advanced persistent threat neither would they be targeted by financially motivated attackers because of who they are. Instead, they would be attacked by the opportunistic attackers due to the existent potential or known vulnerabilities in their information system.

The Incentives to Invest

The main incentive to invest in information and information system security is to reduce the risk of security violation and that is not dependent on the size of the firm. Rather it depends on the potential negative impact that the organization may experience in case of security incident. The more the information system supports the business processes and value creation the larger the motivation of the firm to invest in information security. Although the larger enterprises experience larger amount of loss compared to small enterprises, the larger organizations also have more resources to cope with the consequences. The additional financial resources that are required to recover the information system together with the decrease or loss in income as business processes are interrupted, the orders are not fulfilled and the payments from clients are not received may lead the small firm easily to liquidity crises.

The government or legal regulations as the incentives to invest in information security may or may not be different on the basis of the size of the firm. At the moment it is not related to the size of the firm rather it is related to the specifics of information that has to be protected. According to the statistical data about the share of sales to private consumers via website or EDI from the total turnover is the same for small and for large firms showing that the investments in private data protection in compliance with the General Data Protection Regulation (GDPR) is relevant for large as well as for small firms.

The incentive to invest in information security to be considered as a qualified business partner is more relevant motivation factor for small than for large firms. When small organizations want to have partnership with larger organizations they may be required to improve their information security capabilities to be aligned with the security that is already present in larger organizations. The information security investments may also be triggered by the customer expectations about security if they or the firm's competitors are capable of assessing it.

The Investment Problem

Large organizations have many levels of management. Each level makes the investment decisions within their scope of responsibility. The investment problem on every level is different at least to some extent as the goals, responsibility and resources differ. Small businesses are flat in their structure and investment decisions are made in one level. They have one information security investment problem whereas the large organization have generally one for each decision-making level.

The top management of the large firm needs to allocate the financial resources between different departments. Every department has its own budget and every department is competing for the resources with other departments. The information security (InfoSec) budget may be a separate budget decided by the top management or it is included in information technology (IT) budget by the top management and the next management level decides the size of the InfoSec budget within the IT budget. The investment problem for the top level management is to find the optimal budget for InfoSec (or IT and the next level to InfoSec).The next management level in the large organization has fixed amount of resources which should be used to maximize the outcome. The investment problem for information security is to maximize the security within the budget constraint. Large information security investments may also be decided separately at the top management level to solve a specific information security problem or mitigate a specific information security risk.

The small firm has only one budget and every investment is planned within that limited budget. Every single information security investment is competing for the resources with all the other investments and expenses that the firm has. There is no definite budget constraint for information security investments. There is overall budget constraint for all the investments and expenses. The small firm does not need to define an overall share of security investments within the existent budget and afterwards maximize the security within that constraint. The security investment problem for small firm is to minimize the costs to information security subject to the accepted risk tolerance level. In other words the investment question for the management of the small enterprise is: *Where to invest to minimize the costs to information security to keep the information security risks at the accepted risk tolerance level?*

The accepted risk tolerance level is the extent of the information security risks that the enterprise is willing to bear if the risks occur. The willingness should reflect the ability to cope with the negative impacts in case of security violation both in terms of single incident and multiple incidents within certain period of time. The liquidity issue is much more critical for small businesses than for the large firms to be sustainable in case of information security violation.

3.2. Analysis of Existent Approaches Solving Information Security Investment Problems

The aim of the subchapter is to find the approach(es) that could be used for solving the information security investment problem for small enterprises. Different information security investment models are proposed and discussed in academic literature. All of the approaches have certain investment problem and different methods are used to solve the problem.

The author of the thesis has grouped the approaches according to their investment problem. Each approach is shortly described and following aspects analysed: whether the approach is rather theoretical or could be used in practice based on the assumptions given and the methods used; whether the approach solves the investment problem for small firms and could it be implemented in practice by small firms. The type of the attacker and the profile of the small firm together with its investment problem considered in the analysis is summarized in Table 1.

Table 1. Type of the attacker and the profile of the enterprise

The Attacker:	Financially motivated opportunist
The firm	
Investment problem: *Where to invest to minimize the costs to information security to keep the information security risks at the accepted risk tolerance level?*	
Risk Management System	Absent
Enterprise Management System	Absent
Resources: Financial	Scarce
Resources: Human for InfoSec	Absent
Resources: Time	Limited

3.2.1. What Is the Optimal Budget and the General Allocation of the Budget for Information Security?

The classics of information security investment models is the **Gordon and Loeb (2002b)** single period model (GL) which determines the optimal amount to be invested to protect information and information systems. According to GL the optimal level of investment is achieved when the marginal benefit from the investment is equal with the marginal cost of investing. Their proposed theoretical economic model demonstrated that under the given breach probability functions the maximum amount that a risk-neutral firm should invest in information security does not exceed 37% of its expected loss due to the security breach. They also state that the firms with limited financial resources should concentrate on protecting the information with midrange vulnerabilities as the defence of extremely vulnerable information may be immensely expensive. Extended range of authors in addition to Gordon and Loeb (Gordon *et al.* 2015a) broadened the scope of GL model incorporating the externalities and showing that the socially optimal information security investment increases by no more than 37% of the expected externality loss.

The GL model is primarily a theoretical framework helping security practitioners to understand economics behind information security investments. Although the authors of GL model have provided an illustrative example **(Gordon *et al.* 2016)** about how to derive the appropriate level of information security investments in real case, the limitations of finding applicable data for the variables in a model is a big constraint to use it in practice. Another limitation stems from the simplification of the model that an investment protects a single information set in an organization. In reality an investment may protect different information sets as there are correlated risks in the system and as contemporary practical solutions are often multifunctional. The third and existential weak point is brought out by Willemson (2006, 2010) who questioned the suitability of chosen function families in the model. According to Willemson there is no reason to assume that the applied functions reflect any real vulnerability decrease scenario.

When GL model considered risk-neutral decision maker, **Huang *et al.* (2008)** examines the optimal security investment in case of risk-averse decision maker. Likewise the GL model, the optimal level of investments is dependent on the asset that has to be protected, the vulnerability of the asset and the potential loss related to them. It also models a single attack of a single attacker within single period with fixed potential loss which is an excessive simplification of reality. Compared to the results of GL model with risk-neutral decision maker, the risk-averse decision maker increases his/her investments concurrently with the increase of expected loss but never more than the size of the loss. With risk-averse decision maker there exists a minimum potential loss below which the optimal investment is zero.

Another study by **Huang *et al.* (2006)** examines the optimal security investment level under various attack scenarios – in case of targeted and opportunistic attacks. When there are no budget constraints the total investment drops when specific vulnerability reaches above certain level. There exists also a minimum vulnerability level below which the investment is zero. When the total budget is limited, the investment to protect against a specific type of attack increases when the potential loss from the attack increases or when the size of the budget is enlarged. The outcome of the analysis shows that a limited budget is allocated to mitigate the vulnerabilities that cause the biggest harm which are often related to targeted attacks, leaving the organizations with very limited security budgets exposed to opportunistic attacks. The same results with similar approach based on GL model have been presented by **Wang, Zhu (2016)**.

The GL model (Gordon, Loeb, 2002b; Gordon *et al.* 2016), GL extended model (Gordon *et al.* 2015) and the studies by Huang *et al.* (2006, 2008), Wang Zhu (2016) are theoretical frameworks that provide good economic reasoning behind information security investment decisions concerning the optimal level of investments and the allocation of the budget to treat or not treat certain vulnerabilities. Nevertheless the simplifying assumptions are too extensive to use those approaches in practice irrespective of the size of the firm who is planning the investments. An information set is seldom exposed to a single threat or attacked by a single attacker. The investment decisions in those approaches are made based on the combination of vulnerability and the size of the loss, the latter treated as constant. The models deal with one variable in the total risk equation and that is the reduction of the extent of the total vulnerability to decrease the probability of the attacks that cause most of harm. In reality the risk equation can be solved by dealing with the level of impact instead, or by using a combination of preventive, detective and corrective measures.

Another analytic model by **Huang, Behara (2013)** that considers the optimal level of information security investments has more realistic assumptions such as the existence of concurrent diverse attacks, but as the purpose of the model is to analyse the allocation of investments with respect to targeted and opportunistic attacks, it is not further elaborated as the likelihood for small firms to be under targeted attack is rather low.

Even if exclude the theoretical nature of the above analysed models and assume that these could be used in practice, the approaches would not be suitable for small firms. Defining and allocating security budget is for larger firms who have many management levels. The top-level decides the amount of finances that can be used for information security and the next levels in the organization select the measures according to the budget constraint. A small firm has one budget for all of its investments and expenses. Every single information security investment has to compete for the scarce financial resources with other investments. The models that optimize the budget of the information security are irrelevant for the small firms.

3.2.2. Where to Invest Using the Fixed Information Security Budget?

Bodin *et al.* (2005) have suggested Analytic Hierarchy Process (AHP) approach to evaluate information security investment alternatives in order to use the limited security budget most effectively and also to justify additional investments in security if possible. AHP is a mathematical method developed by Saaty (1987) that can be used to „analyze multi-criteria decision problems involving both quantitative and qualitative criteria" (Bodin *et al*. 2005: 80). The authors suggest to use the ratings method variant of the AHP, under which the criteria and sub-criteria and the weights for those criteria are listed. Each alternative for maintaining and enhancing security is evaluated against each criterion and sub-criterion. Each alternative obtains a score which reflects how well the alternative accomplishes particular criterion or sub-criterion. The proposed criteria are: Confidentiality, Data Integrity and Availability. The latter can be divided to three sub-criteria: Authentication, Non-repudiation, and Accessibility. Each criterion and sub-criterion can have different intensities. The proposed intensities used by Bodin *et al.* (2005) are: exceptionally high, extremely high, very high, high, reasonably high and moderately high. The AHP approach to decide upon the different information security investment alternatives is also used by **Kanungo (2006)**, who combined it with linear programming to obtain the results.

The AHP methodology requires a lot of assessing – to start with finding the criteria, sub-criteria and intensities. The essence of intensities are needed to be defined which are subjective in nature and can be interpreted differently by different assessors. It is challenging to set boundaries between intensities. For instance the given: exceptionally high, extremely high, very high, high, reasonably high and moderately high have very close connotation. Even if the intensities are well defined the nature of uncertainty in case of information security risks may make the estimation problematic. The use of AHP for estimating information security investment alternatives requires good expert knowledge in security as well as profound understanding of the methodology.

The AHP approach could be used without security budget constraint. It could be used by small firms to evaluate investment alternatives if they have clear security objectives, which is doubtful. They also need to find security experts as consultants who have a knowledge, better have an experience with the model and work closely together with the CEO of the firm to decide upon the criteria, sub-criteria and intensities. It is a time-consuming process and the economic justification of using the approach is questionable. The analyses itself may turn to be more expensive than the needed security solution.

Ojamaa *et al.* (2008) have proposed an optimization model that binds together the cost of chosen security measures and the level of confidence of achieving the security goals. They use discrete dynamic programming to obtain a Pareto optimality tradeoff curve containing alternative security solutions. The budget constraint dictates the best approachable security solution on the tradeoff curve. According to **Kirt and Kivimaa (2010)** the proposed method is limited and does not allow to find equivalent security alternatives at the same confidence level. Kirt and Kivimaa (2010) use an evolutionary algorithm for optimization to identify equivalent security profiles at the same cost level.

The shortcoming of both models is the lack of consideration of interaction of the measures in a security profile. The security measures in a profile seem to be aggregated mechanically without considering joint effectivity. In general the methods could be applicable in big firms for aligning alternative sets of security measures. The methods are not suitable for small firms as these require thorough understanding of the security goals of the organization and the needed activities and resources to achieve the goals. The methods do not articulate the connectedness of security goals and business goals. Even if a small firm finds a security expert to apply the method, the outcome is not applicable by the CEO of the small firm as it does not show the business relevance of the information security investments.

Dlamini *et al.* (2011) focus on finding the adequate mix of different types of security controls. They categorize the security measures as administrative, operational and environmental controls. Administrative controls are to guide users' actions when meeting business goals and objectives. Operational controls are implemented through software and hardware systems and environmental controls through physical protection. Their proposed Broad Control Category Cost Indicators (BC3I) model relies on the results of Gordon and Loeb (2002b) (GL) model. According to GL model the investment in information security should not exceed 37% of the expected loss. The first step when implementing the BC3I model is to determine the weights of the control categories based on the applied security standard – ISO 27002 or any other standard. The next step is to determine the weights of importance of each category within the organization. The third step is to estimate the expected loss and derive the overall objective function based on the results of GL model. The fourth step is to find the division of the budget between security control categories using the weights that is given to each category by the specific organization.

The model by Dlamini *et al.* (2011) solves the question of division of the security budget between broad categories of security controls according to the compliance to standards and estimated weights of importance of those categories for specific organization. Leaving aside the limitations that the model does not consider interaction between those broad control categories and the question of validity of the GL model in different real security environments, the issue of division of security budget in such a way is irrelevant for small firms. Small firms do not engage themselves allocating given financial resources for information security according to the broad control categories based on security standards. They do not have information security budget defined and most likely they have not implemented security standards in their organization.

Dewri *et al.* (2012) address the system administrator dilemma to select the security controls within budget limitation and at the same time minimizing the residual damage. They consider the security problem as a number of sequential attacks by the attacker to achieve its goal. The attacker is looking for vulnerabilities that can be exploited to infiltrate to the system finding new vulnerabilities within the system to progress. It is also assumed that the attacker may bypass defence with accrued costs. The authors argue that the decision about security controls has to consider the attacker's possible benefits. The attacker is not motivated to attack if the effort exceeds the gains. At the same time the authors state that the attacker's goal may be just to cause damage thus the benefit does not have to be monetary gain. Dewri *et al.* (2012) use attack tree to model the dynamic interaction between the attacker and the defender. Multi-objective optimization and competitive co-evolution has been chosen to conduct cost-benefit analysis. The authors emphasize the importance of long-term security policy and that the selection of the countermeasures should not be made based on cost-benefit calculations of intermediate policies.

The description of the attacker and his/her motivation and actions indicate that the approach is more suitable for analysing targeted attacks than random attacks. It is computationally challenging approach meaning that an organization using the model for its practical purposes has to be good at game theory computations. In spite of its complexity the model is overly simplistic in covering the cost aspects of security controls. The model assumes that the security measures are independent of each other which is not a practical assumption. The effectivity in security can be achieved when the chosen set of security controls takes the interdependencies into account. The authors define the security controls as preventive measures to stop the attacker reaching his/her goal. The focus is on attacker's costs and benefits. The model does not explicitly consider the selection of recovery measures to diminish the costs that occur for the organization in case of attacks. In some cases it may be rational for the organization not to invest in preventing the attacks but to invest in minimizing the costs that occur in case of attacks instead. It is not a model that small firms could use for making their information security investment decisions.

Khouzani *et al.* (2016) consider the problem of information security investments respect to monetary cost of implementation, indirect costs accompanied by the investments and mitigation of the risks. They differentiate "passive" and "active" threats. The former representing attacks being independent of defence, the latter showing adaptability of the attacker and response to implemented security defence. They consider multi-stage attacks and potential correlations in the success of different stages. The combined efficiency of countermeasures is solved by choosing the efficiency which is highest among them. They use non-linear multi-objective integer programming and mixed integer linear programming conversions to find the Pareto optimal solutions. The shortcoming of the model is that it finds the "best-of" the controls mitigating certain vulnerability and did not consider that a control that may not be the "best of" mitigating any specific vulnerability could be economically the most effective measure when it deals with many vulnerabilities. The model has not been tested in practical setting and would not be an easy to use approach for small firms.

Panaousis *et al.* (2014) also provide a methodology to find optimal combination of security controls within given budget. The first step would be risk analysis and the estimation of effectivity of countermeasures against different vulnerabilities. Based on the results of the risk assessment the control-games between the defender and the attacker exploiting different vulnerabilities are modelled. The multi-objective and multiple choice Knapsack optimization techniques are used on the solutions of different control-games to decide upon the allocation of the security budget. **Zhuo and Solak (2014)** use stochastic programming for making investment decisions about different types of countermeasures within the range of given budget. In addition to the security competence that is needed to use the approaches, the expertise of mathematical modelling is also required. The models are not further explained and analysed as being complex and unsuitable for small firms.

The models presented above deal with solving the issue of finding the best set of countermeasures that maximize the security within given limited financial resources. Small firms do not have a fixed security budget that they have to allocate to maximize the security. That is not the investment problem for small firms and the models are not relevant for them.

3.2.3. Where to Invest When Certain Level of Security Is Needed?

Butler (2002) proposes a risk management approach called The Security Attribute Evaluation Method (SAEM) that contains risk assessment, mitigation technology estimation and selection. Risk assessment does not consider monetary value of threats and assets, instead it estimates the relative value of negative consequences to the organization. The approach does not calculate the optimal size of information technology security budget, neither it weighs risk transfer or risk avoidance as an alternative strategy for risk treatment – it is either risk mitigation or risk acceptance. SAEM compares different technologies in terms of their effectivity to mitigate risks as well as it considers the complementarity of technology to achieve defence in depth. All of the outcomes from the different stages are in relative values that are dependent on the chosen attributes and weights that are given by the security experts. It is not explicitly stated how the trade-off analysis that considers the cost of technology and limitations is executed and therefore it is not possible to estimate how effective the final decision is in economic terms. It is stated that the security technologies can be compared and ranked but it is not expressed whether the method allows to compare the exact final security alternatives that are provided by the competitors in the market. The approach is static in nature but allows to conduct what-if scenario analyses.

The implementation of SAEM requires different people with various capabilities and expert knowledge to be involved. According to the authors it requires a multi-attribute analyst who facilitates the process by interviewing, analysing the results and conducting sensitivity analysis, and a lead security specialist who interprets the results. Each step may involve additional participants who provide information as an input to the model. The outcome from SAEM depends on the quality of the knowledge of security specialists

– their expertise and experience with the threat and security environment in their organization.

Small firms do not have resources to implement SAEM and if they do the cost of implementation of the risk management system could easily exceed the cost that is needed for mitigating the risks. Using the relative values in the approach does not help the CEO of a small firm to understand the business value of the information security investments.

Buldas *et al.* (2006) in their article about selection of security measures use the attack-tree approach to analyse information security risks and estimate the cost and success probability of attacks from the attacker perspective. They consider rational gain-oriented attackers who weigh their success and benefits against the cost of executing the attack and possible penalties if caught and punished. The rational attacker is unlikely to attack if the expected costs exceed the benefits. The authors also propose a simple method for economic justification of security measures – to find the adequate set of measures that are sufficient in terms of security. Being sufficient in the model means to make at least one primary attack unlikely. The adequacy implies that the cost of defence measures should not exceed the value of the assets that would be protected.

The model considers two players – an attacker who is targeting specific organization. In reality the attacker may have several targets on table. The rational attacker would attack the company where he/she expects the highest benefit. Thus any security measure that makes the attack more costly for the attacker may prevent the attack happening. It is also questionable whether the sufficiency condition set in the model is economically rational. The ultimate goal for the rational company would not be to prevent attacks but minimize the risk. It may be more costly for the company to prevent an attack than to invest in security measures that minimize the impact of the attack. Therefore the sufficiency condition in that model could lead to overinvestments in security.

From the perspective of the small firm the dynamic attack-tree approach to assess the risks and the possible moves of an attacker is excessive. The likelihood for the small firm to be under targeted attack is low. The opportunistic attacker does not bother to search for different attack paths to penetrate the information system of a particular small firm. It would be sufficient for small firms to focus on protecting their business critical processes, value creation and protection and not to make the risk assessment and investment decisions overly complicated by starting to model the attack paths of a potential attacker.

Conditional Preference networks (CP-nets) as a qualitative approach for selecting the best information security countermeasures from among possible ones has been proposed by **Bistarelli *et al.* (2007)**. Before the CP-nets are applied, possible attack/defence scenarios using defence trees are modelled. Defence tree combines the action of an attacker with the set of countermeasures to mitigate the possible damages. The scenarios represent the vulnerabilities being present in the system. Diverse attacks have different consequences for the organization. Various countermeasures work against the same or distinct, single or multiple vulnerabilities. CP-nets express the preferences over certain threats and countermeasures by using conditional preference relations that form an induced preference graph. Bistarelli *et al*. (2007) propose two different methods for the composition of preferences – the *and*-composition and the *or*-composition. The *and*-composition includes sequential actions of an attacker to achieve his/her goal. The CP-nets combines the order of preferences for the countermeasures associated with the actions. The *or*-composition contains alternative actions that can be taken by the attacker to achieve his/her goal. In case of *or*-attack a countermeasure against each of the action should be selected. Therefore the countermeasure that mitigates more than single action is preferred.

The approach focuses on finding the countermeasures that are technically most effective mitigating the information security risks. The financial resources that can be used for countermeasures are limited but the selection of the controls in CP-nets does not consider monetary restrictions neither cost-benefit efficiency. The qualitative conditional preference relations are incapable of ranking the countermeasure alternatives according to economic efficiency. The dynamic analysis of interactions between attacker and defender that is used in the approach is also redundant for small firms.

Kumar *et al.* (2008) have proposed a framework to evaluate the value of portfolios of different types of countermeasures. The simulation model allows to combine preventive, detective and recovery measures and model interaction between different business, threat and countermeasure parameters. The countermeasures in the portfolio act in sequence and the effect of countermeasures in portfolio is not necessarily the sum of the effects of the measures. According to the authors, the countermeasures in a portfolio may add additional value, have marginal value, have no additional value and in some cases even have negative value compared to the situation when the countermeasures operate independently from each other.

Countermeasures may be positively or negatively correlated. Positive correlation shows similar capabilities to prevent attacks, for example overlapping signatures. Negative correlation appears when countermeasures have complimentary capabilities. In addition to the characteristics of countermeasures that have been combined in the portfolio, the value of the portfolio depends also on the characteristics of business and threat environment. An advanced countermeasure portfolio shows higher value, high synergy when business grows and/or the threat environment is fierce. When the organization is small and/or the threat environment is mild, the multiple countermeasures in a portfolio give less value, have low synergy.

The research about the value of countermeasure portfolio by Kumar *et al.* (2008) gives good insight to understand the possible effects on efficiency of the measures when multiple countermeasures have been combined to a portfolio. It also indicates that small firms when evaluating their information security investment alternatives have to take their possible growth into consideration and not only their size at the moment. However the estimation of parameters for the model is difficult and it is unlikely that the small firms have enough resources to make predictions about the estimates and run the simulations. Another drawback is the absence of cost considerations of different countermeasures.

The goal of above analysed methods was to find the best set of countermeasures to achieve certain level of security. Buldas *et al.* (2006) suggest to invest in measures that provide sufficient security and are least expensive unless the cost of the measures do not exceed the value of the assets protected. Butler (2002, 2003) selects the controls to be invested in according to the relative values which are based on security attributes and weights. The monetary values of risks and countermeasures are not considered. Bistarelli *et al.* (2007) and Kumar *et al.* (2008) do not consider the cost aspect of security measures either. Small firms do not have a clear understanding about what their optimal security level should be, rather they want to see the impact of the security investments to their business viability in monetary terms.

Second aspect that shows the unsuitability of the models for small firms is the amount of resources in the form of security expertise, mathematical modelling and time that are required for obtaining meaningful results from the models. Small firms do not have the needed resources. The third aspect is that small firms do not need that thorough approaches. Dynamic attack/defence scenarios suit well to analyse the information security risks and responses to them in case of advanced persistent threat, when the adversary is consistent with finding the vulnerabilities to penetrate that particular system. It is excessive to use resources for those methods in case of small firms.

3.2.4. Where to Invest When the Cost-Benefit Aspect Is Important?

The cost-benefit perspective in information security has its roots in computer-related risk analysis and metrics combined with the concepts adapted from finance management.

There are models that estimate the cost-benefit of specific countermeasure and can be used to evaluate the soundness of the investment to that specified control. For example Wei *et al.*, (2001) propose methodology and model to assess the cost-benefit trade-off of network intrusion detection system (IDS). Lee *et al.* (2002) also define cost-sensitive models to optimize the cost of use of IDS. Cavusoglu *et al.* (2005) studies the value of IDS. The issue of interaction of countermeasures and the positive or negative effect of the combination of the measures using the sample of IDS and firewalls is discussed by Cavusoglu *et al.* (2004b, 2009). Böhme and Felegyhazi (2010) model the benefits of investing in penetration testing as a reducer of uncertainty which allows to increase the efficiency of security spending. As the thesis considers investment decisions to information security as a whole the research focusing on the investments of specific controls or specific actions dealing with information security are not further elaborated.

Soo Hoo (2000) in his doctoral dissertation proposed an analytical decision-making framework for the selection of security countermeasures based on cost-benefit perspective. According to the approach the consequences of “the bad events” are estimated. Secondly policy index is given to different baskets of safeguards and the consequences of “the bad events” in case of different policies are estimated. For calculation of consequences of “bad events” Soo Hoo uses the metric called Annual Loss Expectancy (ALE) (Equation 1) proposed by the National Bureau of Standards of the United States in 1979 (Today named as National Institute of Standards and Technology

(NIST)), where $\{O_1, \dots, O_n\}$ is a set of harmful outcomes, $I(O_i)$ is the impact of outcome i in monetary value and F_i is the frequency of outcome i.

$$ALE = \sum_{i=1}^{n} I(O_i)F_i \tag{1}$$

The benefit of investing in different security policies or baskets of countermeasures is found by subtracting the calculated ALE with security policy from the ALE without policy (Equation 2). The policy with largest benefit should be selected.

$$Benefit_k = ALE_0 - ALE_k \qquad \forall\, k = \{1, 2, 3, \dots l\} \tag{2}$$

The safeguard baskets in this approach are compiled mechanically not considering the complementarity of different measures. The effectivity of each measure is estimated as standing alone against the threat and not in combination with other countermeasures that are in the portfolio. The decision-maker in the model is rational and risk-neutral. The model does not describe the selection of appropriate policy if the decision maker is risk-averse. In sum, the approach is simple and could be used by small firms if the complementarity of countermeasures is considered. The difficulty with estimating the frequencies of security incidents, the effectivity of the countermeasures and consequences of security incidents, which is also discussed by Soo Hoo, still remains.

As the next approaches are derived from the financial performance measures, the financial concept are explained first. Performance measurement methods in finance are static or dynamic, expressed in residual term (like revenue – cost) or as a profitability concept (like profit/capital). The cash flow return on investment (CFROI) is a static profitability measure showing the profitability of a project, business unit or firm (Equation 3). The project is profitable when it exceeds the pre-defined return on capital. (Locher, 2005) It is often used to calculate the (expected) profitability in a single period.

$$CFROI = \frac{inflows - expenses}{capital} \tag{3}$$

For multi-period investments the finances used for the investment are factored in time-value. The time value of money principle used in finance management states that any amount of money now is worth more than the amount later as the money received now can earn interest for tomorrow.

Net Present Value (NPV) is a dynamic performance measurement concept, which is calculated by discounting all the expenses (A_t) and inflows (E_t) related to the project within the expected n lifetime periods (Equation 4). Internal rate of discount is denoted as i. (Locher, 2005) The larger the NPV, the more profitable the project, business unit or firm is.

$$NPV = \sum_{t=0}^{n} (E_t - A_t) \frac{1}{(1+i)^t} \qquad (4)$$

Both financial methods in that general form consider cash flows and allow to compare different investments within an organization. These equations do not explicitly use the terms that are current in the context of information and information system security. Different authors have modified those general equations by using the concepts and variables relevant in information security.

Pfleeger and Pfleeger (2003) suggest a model to show the benefits of information security investments that they denote the Return on Security Investment (ROSI) (Equation 5) (Locher, 2005).

$$ROSI = monetary\ risk\ mitigation - cost\ of\ control \qquad (5)$$

Their concept has turned from the classical profitability concept to residual concept, which shows the benefit in absolute value and not the financial effectivity of the investment.

Al-Humaigani and Dunn (2004) propose a model to quantify Return on Security Investment (ROSI) (Equation 6). They suggest that ROSI is the difference between the costs that occur if organization do not invest in information security and the costs that occur if organization chooses to mitigate security risks.

K_T : The probability of the security incident if security measures are not implemented.

C_{T6} : The cost of recovery measures.

C_{T7} : The loss due to business interruption.

C_{T8} : The loss in human casualties or injuries.

C_{T9} : The business loss and legal claims due to data loss.

C_{T10} : The loss of reputation and goodwill.

C_{T11} : Pay-outs from insurance due to the security incident.

C_{T1} : Purchasing cost of security tools, software, licenses and upgrades.

C_{T2} : The cost of extra physical hardware, rooms and facilities needed.

C_{T3} : The HR costs including training, to force security policies and implement security tools.

C_{T4} : Loss of business productivity due to implemented security measures.

C_{T5} : The cost of adopting secured-by-design strategy.

$$ROSI = \sum[K_T \times (C_{T6} + C_{T7} + C_{T8} + C_{T9} + C_{T10}) + C_{T11} - (C_{T1} + C_{T2} + C_{T3} + C_{T4} + C_{T5})] \qquad (6)$$

In their formula they have proposed risk mitigation and risk transfer options to deal with the risks. They do not consider residual risk which is an unrealistic assumption in reality. Generally the information security risks cannot be mitigated and transferred totally. The model does not consider the effectivity of countermeasures when mitigating the risks neither it considers the financial efficiency of security investments.

Purser (2004) derives a Total Return On Investment (TROI) (Equation 7) concept from the general financial performance measure Return On Investment (ROI).

$$TROI \ \frac{Generated\ revenue + Generated\ cost\ saving - Value\ of\ change\ in\ risk}{Investment} \qquad (7)$$

Purser suggests that the calculation of TROI does not require detailed analyses to provide accurate estimates, instead it should offer an order of magnitude calculations for decision making. According to him TROI allows to compare information security alternatives with other alternative investment projects that the firm has with one exception: all the initiatives that are necessary for legal or regulatory requirements have to be carried out, irrespective of TROI. Purser does not explain how the numerical variables for the equation should be found.

Dimopoulos and Furnell (2005) use the term ROI (Equation 9) for calculating the benefits of information security investment relating the concept of Annual Loss Expectancy (ALE) (Equation 8) with the cost of countermeasure (CmC). The information security investments should be rejected if the result is less than 1.

$$ALE = occurrence\ of\ certain\ threat\ \times\ damage \qquad (8)$$

$$ROI = \frac{ALE}{CmC} \qquad (9)$$

Their approach allows to measure the economic reasonability based on the principle that the security investment should not exceed the calculated annual loss expectancy. The problem with the model is that it does not consider neither technical nor financial effectivity of proposed security measure. The concept of residual risk is absent.

Sonnenreich *et al.* (2006) derive their proposed return on investment for a security investment (ROSI) (Equation 11) from the following ROI (Equation 10).

$$ROI \ = \frac{Expected\ Returns - Cost\ of\ Investment}{Cost\ of\ Investment} \qquad (10)$$

$$ROSI = \frac{(Risk\ Exposure \times \%\ Risk\ Mitigated) - Solution\ Cost}{Solution\ Cost} \qquad (11)$$

The Expected Returns in the ROI model is elaborated in the ROSI model to determine the reduction of expected loss through the investment. Risk Exposure is the Annual Loss Expectancy (ALE) which is calculated as Single Loss Expectancy (SLE) multiplied by the expected Annual Rate of Occurrence (ARO) (Equation 12).

$$Risk\ Exposure = ALE = SLE \times ARO \qquad (12)$$

They emphasize the importance of measurement of lost productivity to provide a meaningful estimate for risk exposure through downtime assessment of the information system as well as to understand the scope of possible lost productivity due to the restricted use of information system when security measures are implemented.

The paper published by European Network and Information Security Agency (**ENISA) (2012**) targeted to CERTs to assist them with the assessment of cost effectiveness of information security investments suggests the ROSI model which is essentially the same model proposed by Sonnenreich *et al.* (2006). ALE in the model is the Annual Loss Expectancy without security investment and mALE is the Annual Loss Expectancy when security measure is implemented (Equation 13).

$$ROSI = \frac{ALE - mALE - Cost\ of\ the\ solution}{Cost\ of\ the\ solution} \qquad (13)$$

Bojanc *et al.* (2012), Bojanc and Jerman-Blažic (2013) propose a mathematical model that integrates risk assessment and selection of information security technology to invest in. The quantitative risk assessment focuses on core business processes and the value of information system assets is related to the value that the assets have in that process. The vulnerabilities and the threats are determined and evaluated for every asset. The target security levels are attributed to the core business processes. The output from risk assessment is the risk-parameter that includes the probability and consequences of security incident. The selection of risk treatment strategies – whether to avoid, reduce, transfer or accept – is made based on risk-parameter values. The calculated values are compared with pre-defined values of maximum risk and maximum one-time loss that the organization is willing to accept and with minimum risk that is still plausible for the organization.

The authors use ROI (Equation 14), NPV (Equation 15) and the Internal Rate of Return (IRR) (Equation 16) concepts to evaluate the economic efficiency of different investment alternatives of security measures. The ROI is expressed as an investment profitability measure where the total cost (C) of the investment is subtracted from the benefits (B) from the investment and divided by the cost (C). The investment is economically justified if the value of ROI is positive.

$$ROI = \frac{B-C}{C} \tag{14}$$

The NPV equation used for estimating the investments considers the time factor denoting the discount rate as "i". The length of time period is denoted by "n". The investment is economically justified if NPV > 0.

$$NPV = \sum_{t=0}^{n} \frac{B_t - C_t}{(1+i)^t} \tag{15}$$

IRR gives the discount rate when NPV = 0, showing the breakeven rate of the investment or the point where the present value of inflows of the investment equals to the present value of outflows.

$$\sum_{t=0}^{n} \frac{B_t - C_t}{(1+IRR)^t} = 0 \tag{16}$$

The calculations of ROI, NPV and IRR are modified integrating the security-incident probability function that is chosen as being „very popular among researchers in the field“ (Bojanc *et al.* 2012: 1040).The ROI, NPV and IRR equations differ according to whether it involves preventive, corrective or detective security measure.

The model also attempts to address the complex relationship between risks, vulnerabilities, threats and security measures, indicating that a threat may target different vulnerabilities, a countermeasure can protect against several threats and an asset may be protected by multiple controls. The equation of risk and ROI, NPV and IRR varies depending on the scenario whether a security measure protects against multiple threats or a threat attacks several vulnerabilities or several security measures protect against a threat et cetera.

The applicability and usability of the model was tested with a simulation of a hypothetical case where the annual losses were calculated in the presence of different security measures and the results were compared with the calculated theoretical values of ROI, NPV and IRR for the same measures (Bojanc *et al.* 2012). It was assumed that when these coincide, the model gives correct results. The authors conclude that the similarity of the measures confirm the correctness of the theoretical model as the security measures with the smallest value of potential loss from the simulation have also maximum value of ROI, NPV and IRR calculated.

The assumption and the conclusion about the proof of the model does not hold as the calculated loss in simulation shows the benefit in absolute value, but ROI as it is defined by Bojanc *et al.* (2012) is a measure of economic efficiency of the investment. A security measure that is technically most effective at reducing risk and resulting smaller loss in absolute value is not automatically and definitely most efficient financially.

The effort of Bojanc *et al.* (2012) Bojanc and Jerman-Blažic (2013) to grasp the complex relationships between risks, vulnerabilities, threats and security measures has led to numerous parameters and equations. In practice and especially for small firms it would be too time-consuming and complicated to estimate all the parameters, to evaluate the appropriateness of the proposed probability function and to derive the equations depending on the security scenarios that are present in the organization.

Gonzalez-Granadillo *et al.* (2012a, 2012b, 2014a, 2014b) propose a countermeasure selection model called the Return On Response Investment (RORI) (Equation 17) which adds Annual Infrastructure Value (AIV) variable to the investment profitability model. ALE is Annual Loss Expectancy, RM refers to Risk Mitigation level associated with specific countermeasure, ARC is the Annual Response Cost and AIV refers to the fixed costs related to the uphold of infrastructure which exists regardless of the implemented countermeasures.

$$RORI = \frac{(ALE \times RM) - ARC}{ARC + AIV} \times 100 \qquad (17)$$

The first paper (Gonzalez-Granadillo *et al.* 2012a) provided the individual countermeasure selection system based on RORI index. The following paper (Gonzalez-Granadillo *et al.* 2014a) combined RORI index with technical effectivity to select countermeasures. The remaining papers (Gonzalez-Granadillo *et al.* 2012b, 2014b) explain the optimization of the combination of countermeasures based on RORI calculations and using the concept of surface coverage. According to the authors the surface coverage is a work in progress field that allows to map the coverage of different countermeasures on the attack surface to find the overlapping and not covered areas in defence. A combined security solution is analysed as a single countermeasure with the combined cost and effectiveness.

The quantification of the parameters for calculating RORI requires expert knowledge, statistical data, simulations and risk assessment tools. Specific knowledge and tools are also needed for carrying out the countermeasure surface coverage analysis. It is not a plain and affordable approach for small firms.

Summarizing the approaches analysed above it can be concluded that the cost-benefit perspective, whether in absolute monetary terms or expressed as effectivity ratio, is the most informative and useful concept for small firms to understand the importance of information security investments and make decisions about where exactly or in which measures to invest. The above analysed methods have minor differences but in essence their outcome is either the expected benefit or the cost-benefit ratio of the investment. Despite the closeness of the concepts, the outcomes of NPV or IRR and ROSI or ROI calculations may favour different security solutions. Bojanc, Jerman-Blažic (2008a), (2008b), (2013) suggest to use all of them and in case of inconsistencies consider additional parameters and decide upon subjective terms. In order to decide which measurement method is preferable, the drawbacks of ROI, ROSI and NPV, IRR are discussed below.

The use of profitability measure ROI and ROSI have three drawbacks. The first drawback is the problematics of estimation of variables for the calculation, the uncertainty and lack of real data that could be used for calculating the benefits of information security (Berinato, 2002; ENISA, 2012; Schneier, 2008; Wood, Parker 2004). The second shortcoming is that it is a static single-period model that do not consider the time value of money (Bojanc, Jerman-Blažic, 2008a, 2008b, 2013; Brotby, 2009). The third problem lies in its essence – it is a profitability measure that does not reflect the magnitude of the investments (Bojanc, Jerman-Blažic, 2008a, 2008b, 2013).

The biggest problem of using NPV as well as IRR when calculating the benefits of information security investment is the difficulty of estimating the exact timing of the benefits – the points of time when the loss is avoided. If the expected probability of certain attack is once within four years, then the outcome of NPV calculation is very different depending on which year the attack occurs.

The accuracy in calculations coping with uncertainty for making the investment alternatives comparable is much more critical for NPV than for ROSI calculations. "While ROSI doesn't factor in the time value of money, it can at least provide comparable figures with inaccurate (but consistent) data" (Sonnenreich *et al.* 2006: 64). Sonnenreich *et al.* (2006) claim that even if the data used in the ROSI model is inaccurate, repeatable and consistent use of the method and results of ROSI calculations allow to compare the relative value of security solutions.

At present time when the interest rates in Europe and Japan are negative and in the USA close to one percent, the principle of time value of money is not even relevant to consider when comparing multi-period information security investment alternatives. Therefore the author of the thesis suggests to prefer ROSI and calculate the measure for different time-intervals making certain expectations about the security risks and costs of mitigating the risks. Investment alternatives with same expectations and time-interval can be compared irrespective of the lack of interest rate calculation. Even if/when the interest rates increase, the possible inaccuracy when comparing multi-period information security investments due to not using discounted value of money has less influence to the efficiency of use of financial resources than the inaccuracy when making expectations about information security risks. Using the time-accuracy requiring NPV calculations with the uncertainty may lead to more inefficient use of financial resources than using the static ROSI concept.

The third drawback of ROSI that it does not reflect the magnitude of the investments can be overcome when it is used together with security benefit calculation (for example Equation 2).

3.2.5. When to Invest in Information Security?

Several information security investment approaches study the right timing of making investments. **Gordon *et al.* (2003a)** calling their method "Wait-and-See Approach" propose that deferred investment in information security may be economically rational. The security budget is limited and all the assets cannot be protected all of the time. The authors suggest that only a portion of the security budget could be initially invested and the rest could be invested when the breaches in reality occur. The proposed real options „wait-and-see" approach assumes that the uncertainty associated with possible attacks can be overcome by waiting for some real incidents to happen and then invest. The real options theory shows that the timing of the investment depends on the calculated net present value (NPV). The investment should be made today if the NPV value is greater compared to the NPV value when the investment is deferred.

Uncertainty which is the main cause for waiting with investments is also the biggest challenge to calculate valid NPV. It is difficult to estimate which kind of and when exactly the security incidents occur and what are the consequences in monetary terms within the calculated time-frame. Gordon *et al.* (2003a) suggest that the extent of uncertainty could be reduced by conducting penetration testing. Penetration testing on the other hand can be very costly and the economic justification should be critically evaluated. The economic reasonability of penetration testing for small firms is highly questionable.

The real options theory has been applied to information security investments also by **Herath, Herath (2008-2009)**. Their approach makes use of Bayesian statistics, incorporates active learning and can be used for valuation and *ex post* analysis of investments. The model could be used in bigger organizations where the investments can be made partially in some location of the organization. The values of the parameters for the model could be taken from that particular location to analyse the benefits of the investment in order to decide about the necessity of further investments. As it is not applicable for smaller organizations for *ex ante* analysis of investments, the model is not further analysed.

The game-theoretic adaptive security investment approach developed by **Böhme and Moore (2009)** use the concepts of under-investment and reactive investment. The model studies the case where information security depends on its weakest link. When the weakest link is improved, new weakness is identified and exploited by the attacker. When the uncertainty about weakest point(s) that can be attacked is high for the defender, the organization has difficulties deciding where to invest and may choose to not invest at all. The authors conclude that under-investment is reasonable if reactive investment is a possible option for the organization, if there exists uncertainty about attacker's capabilities to exploit variety of threats, if the consequences of successful attacks are not catastrophic and if the sunk costs – the costs that once done cannot be repealed – for upgrading the security, are relatively small.

A learning-based approach to reactive security is another game-theoretic model that studies the rationality of reactive security investment. The results of the model developed by **Barth *et al.* (2010)** showed that under given conditions the learning-based reactive strategy can be as good as the best fixed proactive defence and outperform the proactive defence when the attacks that are defended against never occur. The authors conclude that reactive security investments would be a reasonable option for agile, learning organizations who use monitoring tools to detect and analyse the attacks. Reactive security investments are not suitable for dealing with attacks that have critical impact to the operations of the organization.

Tatsumi and Goto (2010) use the continuous real options analysis to analytical modelling of timing of information security investment. Their study is an attempt to formulate the needed parameters and functions for the theoretical model to describe the matter. The model cannot be used by small firms and therefore it is not further elaborated.

The game-theoretic models provide insight into strategic options of timing the investments. Waiting with information security investments is not about ignoring information security. It involves prior risk assessment and evaluation of risk treatment options. The final decision about magnitude and exact location of the investment could be deferred waiting for the trigger from the real incidents. Strategic choice to wait with investments has to be supported by the well-implemented monitoring systems. Understanding of and response to real attacks may be excessively delayed and can cause wider problems if proactive security is absent and no monitoring exists. Implementing monitoring in small firms is problematic due to the very limited resources in terms of finances and people with expert knowledge.

3.2.6. Enterprise Management System as the Basis of Information Security Investment Decisions

Tallau *et al.* (2010) and Kong *et al.* (2012) consider the information security investment decisions in the context of strategic enterprise management system Balanced Scorecard (BSC). BSC is developed by Kaplan and Norton at the beginning of the nineties to formulize the vision and the strategy of the firm in Key Performance Indicators (KPI) that measure the Critical Success Factors (CSF) of the firm (Kaplan, Norton, 2002). BSC measures performance of reaching the goals and enables to evaluate the execution of objectives that are not easily measurable in monetary terms such as customer satisfaction or the learning outcome of employees.

The information security has quantitative as well as qualitative aspects to measure and evaluate. According to Tallau *et al.* (2010) and Kong *et al.* (2012) the BSC method allows to link the information security investment decisions to the strategy of the firm through key performance indicators. It is unlikely that small firms have implemented enterprise management systems like BSC or any other in their organization. If they had, they would still require a security specialist to assist with setting the perspectives, goals and measures for the security.

3.2.7. Summary of Information Security Investment Approaches in the Context of Small Enterprises

The amount of approaches concerning information security investments in academic literature is notable. There were theoretical approaches to provide better insight to the factors that should be considered when making investment decisions along with the models intended to be used in practice. Some of the models were static, some of them dynamic, modelling the interaction between attacker and the defender or considering different time-frame of investments.

The discussed and analysed methods were organized according to the investment problem that these methods were intended to solve. The proposed categorization reflects well the variety of issues and the information security investment goals that the organizations have. A vast majority of the approaches are not suitable for small firms – whether the problems that are solved are not relevant for small organizations or the implementation of the method would not be economically justified or the execution would demand resources that are not available for small firms.

The main reasons why certain information security investment problems do not exist in small firms compared to large organizations are the differences in financial resources available and the differences in the structure of the organizations. The issue of optimal security budget and general allocation of the budget which is relevant in large organizations to administrate the finances and empower the investment decision making along organizational levels, is not relevant in small firms. Small firms do not have and they do not need to have separate budget for security. The investment decisions are not delegated along the flat organization. Every single information security investment in a small firm has to compete for the resources with all the other investment alternatives that the organization has. According to the non-existent security budget they also do not need to solve the problem of maximizing the security with respect to the fixed security budget.

Large organizations have often implemented risk management frameworks or follow certain security guidelines, defining the security levels for the organization. Those frameworks and guidelines dictate the security goals for the firm. Investment decisions are made to meet those goals. Small firms do not generally follow risk management frameworks, they do not have defined security levels which would guide them in their security investment decisions. Therefore the information security investment approaches that solve the investment problem of achieving certain level of security are not needed in small organizations. It is also unlikely that small firms have implemented any enterprise management system for instance Balanced Scorecard that would be used as a basis for making investment decisions concerning information security.

The question of right timing of the information security investments would be interesting for small firms but it is unlikely that a vast majority of the small firms could afford the deferral of the investments as a strategic choice. Waiting with the investments is not about ignoring the security issues. In order to use agile investment strategy, the organization has to invest in monitoring systems and personnel to be able to respond to the attacks as fast as possible.

The summary of approaches analysed according to whether the approach is rather theoretical or could be used in practice; whether the approach solves the investment problem for small firms and could it be implemented in practice by small firms is presented in Appendix 1.

The main issue concerning information security investments for the small firms is to use their scarce financial resources as effectively as possible. The investments which purpose is to enable to create positive cash flow for the firm are competing for the resources with the investments which purpose is to create positive cash flow. The second issue is to decide the level of risk that is accepted. That means finding a balance between the resources that should be invested now and the resources that should be made available if the remaining risk occurs and the organization bears loss. Hence the cost-benefit perspective to information security investments including setting the remaining risk level is the approach that is relevant for the small firms.

3.3. The Information Security Investment Decision Making Approach Suitable for Small Enterprises

Information security risk management is the responsibility of the CEO of the small business. Scarce financial resources do not allow to employ information security experts and even if the small organization has hired a security competent information technology specialist, the responsibility still remains on the management of the organization.

The scarce financial resources also imply that small organizations have to make smart decisions when investing in information security. How can a small firm solve its information security investment problem: Where to invest to minimize the costs to information security to keep the information security risks at the accepted risk tolerance level?

The first thing that has to be done is the risk assessment. Good information security investment decision cannot be made without knowing what needs to be protected and what would be the benefit of making the investment. The outcome from risk assessment is the input to the investment decision making equation.

Small firms have likely difficulties to find resources to hire consultants who would conduct the most common asset-driven risk assessment for them. But they can use less consultancy time of security experts if they make a part of the risk assessment themselves. They can start with analysing whether they overall have an information security problem.

Step 1: Risk Assessment – Does the Information System Supports Business Critical Processes, Value Creation and Value Protection?

Performed by the Management of the Firm

Instead of figuring out what the information assets are for them and what is the value of those assets, they need to understand the existent and planned business processes that generate value for the firm and determine which value creating or value protecting processes are supported by the information technology. The value creation and protection is well determined through analysing the existent and future cash flows of the firm. The cash inflows from operating activities of the firm show the value creation. The value protection can be viewed as the prevention of abnormal cash outflows – the cash outflows that are not relevant for normal business activities. The analysis of cash flows is done anyway in the firm to manage the business. What is additional is reaching to understanding whether or which part of information system is supporting the value creation and protection.

If the value creation is and will not be supported and business value not protected significantly by the information technology then the inclusion of security expert for further analysis is not needed. The information system that is not supporting the business critical processes can be protected by following the general protection recommendations explained also via mass media. If the information technology is the business enabler and value preserver then the business critical information system should be audited against common threats and vulnerabilities.

Step 2: Risk Assessment – Analysis of Business Critical Information System

Performed by a Security Expert

The threat and vulnerability assessment together with the estimation of the probability of penetration of the system should be conducted by an information security expert because it requires technical expertise. The security expert can state the risks, explain the technical consequences if the security incidents occur and propose the required time and other needed resources to recover the system.

Step 3: Risk Assessment – Impacts and Risk Tolerance Levels

Performed by the Management of the Firm

When the output from step 2 shows that the system is not secure, then the firm should continue with step 3. The impact of the potential security incident to the business should be estimated by the management of the firm. It is important to understand what the factors are which affect the cash flows and what is the short-term and long-term influence to the cash flows. For example, how fierce is the competition in the field and how difficult and costly it is for customers and for partners to switch? Will the clients that could not buy from the firm today because of the unavailability of the system purchase tomorrow or will they buy from the competitor of the firm? Do they come back a week later or they will never return. It shows whether the decreased cash inflow today due to the security incident will be compensated tomorrow or week later or it will never be compensated. What if the negative impact to the cash flows does not expose today but half a year later when the ongoing projects are finished but new contracts are not signed due to the loss of trust because of the security incident? Another factor that may affect the cash flows and more specifically cash outflows is the existence of legal regulations, for example General Data Protection Regulation (GDPR), which may bring remarkable cash outflow due to the stipulated penalty when the firm is violating data privacy.

Using the incident probability (ARO) information provided by the security expert together with the impact analysis (SLE) performed by the management of the firm, the Annual Loss Expectancy (ALE) can be calculated (Equation 12). ARO stands for Annual Rate of Occurrence measuring the probability of the risk in a year. SLE represents the Single Loss Expectancy which is the expected loss in monetary terms when the risk occurs.

$$ALE = ARO \times SLE \tag{12}$$

Despite the critics of the metrics that the exact values for ARO and SLE are difficult to estimate, it is a good metric for small firms to use when it is used wisely. The precision of the estimations of ARO and SLE does not have to be punctual. The consistency in estimations and the scale of the precision is more important to obtain meaningful results. It is also a good metric for performing What-If analysis. Testing different assumptions affecting the impact and probability allows to see wider picture of the security influencing the business. At last the most probable scenario and security strategy should be selected.

Although the previous works explaining ALE metrics do not remarkably emphasize the importance of SLE, then in the context of small firms the magnitude of SLE is critical. From the sustainability and viability aspect of the small firm the low probability high-impact risks should be considered not as if these risks occur but instead when the risks occur. A low probability high-impact risk may lead the small firm to liquidity crisis when the normal cash inflow is interrupted and the outflow is increased due to the expenses related to the security incident. With high-impact risks the firm should definitely not only weigh the alternatives to minimize the probability of the event but also to evaluate the measures minimizing the impact in case the event occurs.

In case of high probability but low-impact risks the frequently occurring risks may materialize at the same time and also cause liquidity problems for the small firm. Another aspect that should be considered when using ALE metrics for investment decision making is that SLE may be correlated with ARO. A single incident happening once may have different consequences compared to the same incident when it happens several times. If the purchasing system is unavailable due to the security incident only once, the clients may not even notice it but if it happens several times the irritation grows and switching to the competitive firm is more likely. There may also be correlation of SLEs of different risks. If there are different information security related problems present in the firm, the firm is perceived as unsecure, not trusted and the clients and partners are more likely to switch to other suppliers.

On the basis of its expected cash inflows and outflows, the firm should set the level of tolerance to SLE and ALE for all the major risks in order to not cause liquidity crises or generate operating loss. The probability of a security risk cannot or is not economically justified to eliminate totally and in case of high-impact risks, the firm should also consider the acceptance level for ARO below which the SLE that is exceeding the level of tolerance of SLE would be accepted. The set criteria can be used for deciding about which risks should be treated and when evaluating the risk treatment options whether the risks would be treated sufficiently. Although the given criteria contain exact monetary and probability estimates, the decision-maker should understand that the calculations are based on expectations and the results should be considered with prudence.

The firm may for example accept the high-impact risk which value of SLE exceeds the tolerance level but the probability of the security event to happen is 5%, which means it is expected to happen once within 20 years and that is the risk level that the firm is willing to take. If the probability is higher, then the firm needs to treat the risk. If the tolerance level of SLE and ARO is not met or economically justified after evaluating the risk treatment alternatives, then the firm should consider to change its business processes or even business plan to avoid the risk.

The firm should mitigate or transfer the risk if the following conditions are not met until the conditions are satisfied or avoid the risk if reaching to the set criteria would be economically unjustified:

- The value of calculated SLE exceeds the level of tolerance of SLE and the ARO that is accepted for high-impact risks exceeds the predefined level.
- The value of calculated SLE is within accepted tolerance level, but the ARO exceeds the maximum level that is accepted.
- The sum of ALE of all the risks exceeds the predefined level of tolerance for ALE Total.

In sum, ALE metrics should not be calculated and used mechanically. It is relevant to understand the content behind the numerical variables. It is not only the value of ALE that should be evaluated but also the values of ARO and SLE. The risks that are high in ALE, ARO or SLE should be listed and the potential impact to cash flows and liquidity should be evaluated to decide about the risk treatment, whether to accept, avoid, transfer or mitigate specific risks.

Step 4: Risk Treatment Considerations – What Are the Risk Treatment Options and Their Technical Effectivity?

Performed in Cooperation with the Security Expert and Management of the Firm and Security Vendors and Management of the Firm

When the risks that need to be treated are decided, the risk treatment alternatives should be determined and estimated. The management of the firm needs technological advice recommending risk treatment alternatives for them. As the security expert that conducted the risk assessment has the understanding of the existent vulnerabilities in the system, then the expert can also give suggestions how to prevent attackers exploiting the vulnerabilities. In order to prevent the penetration and/or minimize the resulting negative impact, the firms have usually different alternatives to choose between. Some of the alternatives may act as substitutes, others may operate as complements. There are technical and non-technical measures. Implementing the technology of encryption is a technical solution, implementing the policy to encrypt files and training people to use encryption and decryption is a non-technical measure. Both require financial resources to enact. In order to make the security measure alternatives comparable, their technical or operational efficiency should be assessed.

The difficulty is that the quality and efficiency of the security products mitigating the risks is not visible. Small firms do not have resources to test the capabilities and efficiency of security solutions. They mostly have to rely on the information that is available in the market concerning the efficiency of the controls. They could try to verify the information about security products by gaining the knowledge from different sources – from the security expert, different vendors – and being critical about the effectivity that is introduced.

When multiple measures are combined, then their joint efficiency should be assessed. If desktop security solution is estimated to prevent 50% and the firewall security solution is estimated to prevent 80% of certain attacks, then their joint efficiency may also be 80% when the signatures and functionalities of those measures coincide. If the measures complement each other in some aspect, then their joint effect exceeds 80%. When choosing the alternative measures and estimating the efficiency of the measures it is also important to consider the length of the licence or support provided by the supplier of the solution. Security landscape changes fast and having up-to-date security is essential. Small firms also have to consider the human resources they have or need to have for implementing certain controls. If they do not have a specialist to monitor their information system daily then they should not consider solutions which require daily monitoring.

Step 5: Investment Decision Making – Solving the Information Security Investment Problem: ROSI or RORPI?

Performed by the Management of the Firm

At this stage the input information is at hand to solve the information security investment problem for small firms: Where to invest to minimize the costs to information security to keep the information security risks at the accepted risk tolerance level? The cost minimization problem can be solved by finding the risk treatment alternative which mitigates the expected annual loss per invested monetary unit the most and satisfies the determined risk tolerance level conditions. The more Euros of Annual Loss Expectancy (ALE) an invested Euro decreases, the more effective the solution financially is. All the costs that are related to the implementation and operation of the security measures should be counted.

The general method for calculating benefit-cost ratio of investments is Return on Investment (ROI). According to the CSI Computer Crime and Security Survey in 2010, 54% of the respondents used ROI calculations as economic justification to information security investments. Nevertheless the reported use of ROI may not be entirely correct as the authors of the survey suggest that the calculation of ROI may be interpreted and calculated differently (Richardson 2010/2011). The analysis in previous sub-chapter showed that the derived concept Return on Security Investment (ROSI) has also many variations. In principle some models calculate the benefit of the information security investment in absolute terms, showing the technical efficiency of the security solution, other models calculate the ratio, showing the financial effectivity of the investment.

Return on Security Investment – ROSI

In order to solve the investment problem for small firms, the cost-benefit ratio needs to be calculated, therefore the ROSI proposed by Sonnenreich *et al.* (2006) and suggested also by ENISA (2012) (Equation 13) is the most suitable equation out of the presented cost-benefit methods explained in previous subchapter 3.2.

$$ROSI = \frac{ALE - mALE - Cost\ of\ the\ solution}{Cost\ of\ the\ solution} \qquad (13)$$

The explanations and examples of ROSI equation in literature has been used for either justifying the investment in specific countermeasure or evaluating countermeasure alternatives mitigating specific risk. The clarifications do not discuss how to solve the investment problem when multiple risks need to be treated and the security controls could be cross-used to mitigate those risks.

The comparison of ROSI results mitigating a specific risk may lead to prefer certain security control that is not preferred when the ROSI results are compared for mitigating another risk using the same controls. Risk A may be most effectively mitigated with firewall having license A, The risk B may be most effectively mitigated with the firewall having license B. The firm does not need two firewalls with two different licenses. Risk C may be most effectively dealt with transferring the risk to security service supplier. But if the firm decides to invest in firewall with licence B, the shared costs to mitigate Risk B and Risk C will lead to prefer the investment to firewall B instead of transferring Risk C.

Return on Risk Portfolio Investment – RORPI

In order to get most value out of the money invested in information security the author of the thesis suggests to aggregate the multiple risks to a risk portfolio and estimate how effectively the risk treatment alternatives containing different controls mitigate the risks in the risk portfolio. The risk treatment alternative that creates the highest return on risk portfolio investment should be selected satisfying the conditions that are predefined for the ALE, SLE and ARO. If the conditions are not satisfied then the next best alternative should be selected until the conditions are satisfied subject to RORPI > 1.

A risk treatment alternative should treat every single risk in the risk portfolio. An alternative may contain a single control if that control reduces the risk level of every risk in the portfolio or it may contain multiple controls.

The proposed security controls can act as substitutes or complements. Substitutes are the same types of controls, for example firewalls which can provide simple or advanced functionalities and features. Only one substitutable control at a time can be added to a mitigation alternative from the range of the controls of that specific type. Complementary controls do not exclude each other and multiple of them may be added to a single alternative. A desktop security solution and a firewall security solution is an example of complementary controls – both of them could be added to a mitigation alternative.

When the risk treatment alternatives are formed, then the next step is to calculate the Annual Loss Expectancy for risk portfolio denoted as *ALE Total*. ALE Total is the sum of ALEs of each risk in that portfolio. The ALE of each risk is already calculated in Risk Assessment process Step 3.

The following step is to estimate the ARO and SLE and calculate the ALE for each risk in that portfolio as if the specific risk treatment alternative were implemented. If multiple controls are present in that alternative, then their joint-effect to the ARO, SLE or both should be considered. The calculated ARO, SLE and ALE with security controls are denoted respectively as *mARO*, *mSLE* and *mALE*. When the mALEs of each risk in the portfolio is calculated, then the value is summed up and denoted as *mALE Total*. mALE Total is calculated for every risk treatment alternative denoted as $mALE\ Total_k$, where 'k' is referring to specific risk treatment alternative.

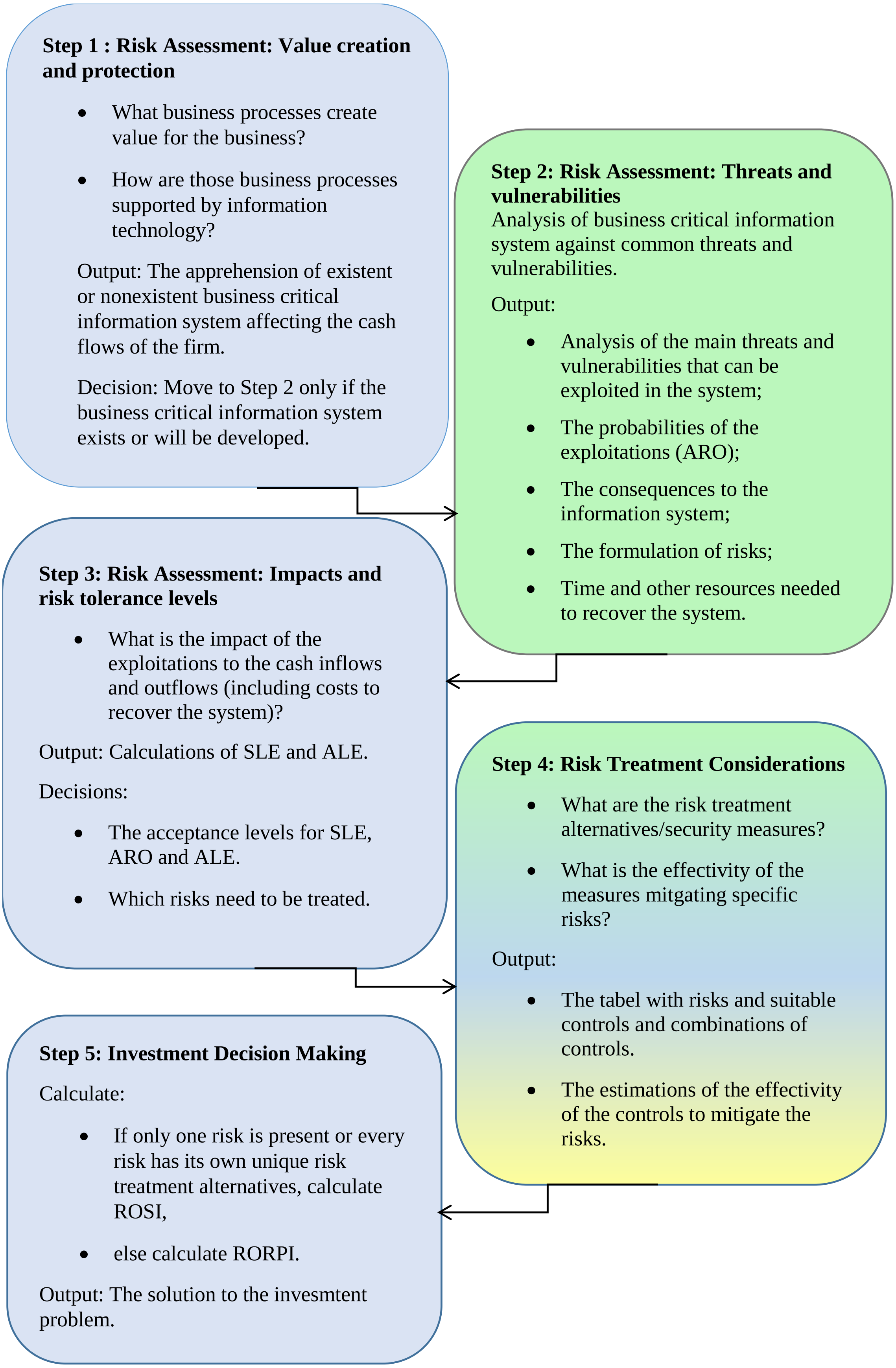
The next step is to compute the Return on Risk Portfolio Investment (RORPI) for each risk treatment investment alternative using the equation (18). The Cost of Treatment is the sum of all the relevant costs to implement and operate the controls that are present in that particular mitigation alternative (k). If there is only one control in the mitigation alternative, then there are only costs that are related to that one control, if there are multiple, then all the costs of those multiple measures are aggregated.

$$RORPI_k = \frac{ALE\ Total - mALE\ Total_k - Cost\ of\ Treatment_k}{Cost\ of\ Treatment\ _k} \qquad (18)$$

$$\forall\ k = \{1, 2, 3, \dots l\}$$

The RORPI with highest result shows the best investment in terms of delivered value, which is the amount of information security risks mitigated in monetary value per invested unit of money. If the security treatment alternative with highest RORPI does not meet the predefined conditions regarding ARO, SLE and ALE, then the next best RORPI result should be assessed towards the conditions until the best RORPI which meets the set requirements is found subject to RORPI > 1.

The summary of the information security investment decision making approach is presented in Figure 6. The boxes with blue background show questions, activities, outcomes and decisions that are solved by the management of the firm. The green background presents the activities and outcomes of security expert and the box with green-blue-yellow denotes the questions and results were the management of the firm, the security expert and vendors are involved.



Step 1 : Risk Assessment: Value creation and protection

- What business processes create value for the business?
- How are those business processes supported by information technology?

Output: The apprehension of existent or nonexistent business critical information system affecting the cash flows of the firm.

Decision: Move to Step 2 only if the business critical information system exists or will be developed.

Step 2: Risk Assessment: Threats and vulnerabilities
Analysis of business critical information system against common threats and vulnerabilities.

Output:

- Analysis of the main threats and vulnerabilities that can be exploited in the system;
- The probabilities of the exploitations (ARO);
- The consequences to the information system;
- The formulation of risks;
- Time and other resources needed to recover the system.

Step 3: Risk Assessment: Impacts and risk tolerance levels

- What is the impact of the exploitations to the cash inflows and outflows (including costs to recover the system)?

Output: Calculations of SLE and ALE.

Decisions:

- The acceptance levels for SLE, ARO and ALE.
- Which risks need to be treated.

Step 4: Risk Treatment Considerations

- What are the risk treatment alternatives/security measures?
- What is the effectivity of the measures mitgating specific risks?

Output:

- The tabel with risks and suitable controls and combinations of controls.
- The estimations of the effectivity of the controls to mitigate the risks.

Step 5: Investment Decision Making

Calculate:

- If only one risk is present or every risk has its own unique risk treatment alternatives, calculate ROSI,
- else calculate RORPI.

Output: The solution to the invesmtent problem.

Figure 6. The information security investment decision making process

An illustrative case study is provided to demonstrate the suggested information security investment decision making process and the difference of calculating ROSI and RORPI. The case study is based on existent business but the presented business plan and financial statements are modified due to ethical reasons. The information system that is analysed in terms of security risks is hypothetical, considering the circumstances that the firm was developed more than 15 years ago. The security solutions that are proposed as the alternatives of risk treatment are existent security solutions provided in the market and calculated with given market prices. The cost of training the employees in case of one control option is taken as a market price for existent comparable trainings.

Case study – a Translation Agency

The translation agency has been in the market for 17 years. Their yearly turnover is 600 000 Euros. They have 10 employees. In addition to the hired people they use the services of additional 39 contract-based translators. The agency provides translation services for corporate clients and private persons. The firm has not hired an information technology specialist. They use the services of an IT specialist when they undergo abnormalities or dysfunctionalities in their information system or they need changes in their system.

Step 1: Risk Assessment – the Value Creation and Protection

The firm has the strategic business plan to grow 30% next year. In addition to the growth of the volume of the translations of technical, economic and medical texts they start to provide legal translations certified by a notary or sworn translators. To improve the quality of the translations the translated texts are proof-read by two translators. They also aim to widen the provision of the confidentiality clause to their clients concerning the content of the materials to be translated. They also need to meet the requirements of General Data Protection Regulation (GDPR) concerning the data of their private clients.

According to the analysis of the business processes and the information technology systems supporting the processes as well as the statement of existent and planned cash flows, the major negative impact to short term as well as long term cash flows is caused by disclosure, loss or unavailability of corporate and private customer data and materials. The confidentiality commitment, especially when it is promoted to clients as well as the GDPR requirements would have severe negative impact to cash flows if violated. The competition in translation business is fierce and clients can easily switch to competitors. The decision for the firm is that an external information security expert is required to analyse the information system security.

Step 2: Risk Assessment – Threats and Vulnerabilities

The security expert listed following Information Technology assets supporting the business critical processes:

- Wired and Wireless LAN network
- Microsoft Server, including Active Directory and file server
- Microsoft Exchange
- Server hardware
- Internet connection provided by local Internet Service Provider (ISP)
- Router with integrated firewall provided by ISP
- Windows 7
- Windows Office
- Web-based external service: translation memory programs

The main threats listed:

- Ransomware
- Viruses, spyware or malware
- Fraudulent emails or being directed to fraudulent websites
- Unauthorized access to file server through router

The main attack vector to penetrate the information system of the case study firm is by sending an email containing viruses, malware, ransomware or providing a link to the websites incorporating malware. Due to the nature of the business, the firm is receiving lots of emails that contain links and attachments to the texts that need the quotation for translation or the texts that need to be translated. Therefore the risk of opening an attachment or link containing malicious content is very high. Another considerable way to access the confidential customer data that is stored in file server is through exploiting the vulnerabilities or misconfiguration of router which is provided to the firm by Internet service provider. The existent system is poorly secured against the main threats. The Annual Rate of Occurrence (ARO) of different risks is estimated based on the information about business processes, the existent state of security of those processes supported by information technology and publicly available threat reports provided by CERTs and security vendors.

Step 3: Risk Assessment – Impacts and Risk Tolerance Levels

Considering the information given by the security expert, the management estimates the impact of the risks to cash flows (SLE), sets the tolerance level conditions for SLE, ARO and ALE and calculates the ALE. The main risks and major impacts, the results of calculation of AROs, SLEs and ALEs, together with the existent and planned turnover, are presented in Table 2. The risk tolerance conditions set for SLE, ARO and ALE are presented in Table 3.

Step 4: Risk Treatment Considerations

The proposed alternatives of security measures of the case study presented in Table 4 are real options provided in the market and calculated in market prices. The cost of training the employees and contract-translators in option I is taken as a market price for existent comparable trainings.

Step 5: Investment Decision Making

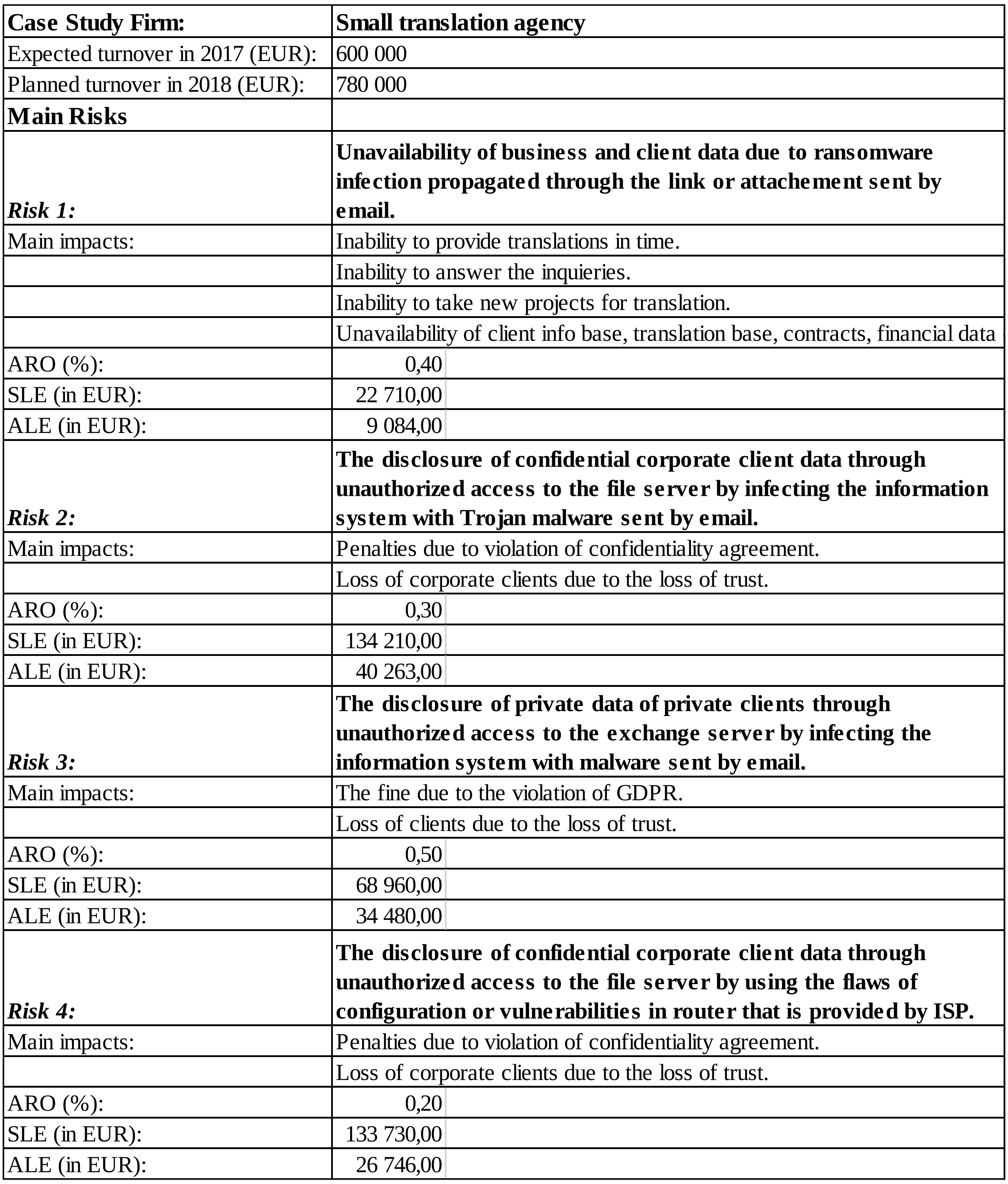
ROSI

The first method that is used to calculate the benefit-cost ratio of the investments is the traditionally calculated ROSI (Equation 13). Every reasonable combination of security measures to treat each risk is formed. The proposed seven security controls to mitigate the four risks form 42 different alternatives all together to be estimated and calculated.

$$ROSI = \frac{ALE - mALE - Cost\ of\ the\ solution}{Cost\ of\ the\ solution} \qquad (13)$$

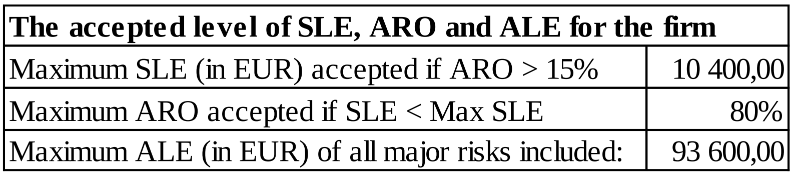
For every alternative the impact of the control(s) to SLE and ARO should be estimated. If the alternative has multiple controls then the joint effectivity should be evaluated. The results of the ARO and SLE estimations, ALE and ROSI calculations are presented in Appendices 2-5. The alternative is denoted as “Mit” as an abbreviation of Mitigation.

Table 2. The turnover of the firm, the main risks and their impacts, calculated AROs, SLEs and ALEs.



Case Study Firm:	**Small translation agency**
Expected turnover in 2017 (EUR):	600 000
Planned turnover in 2018 (EUR):	780 000
Main Risks	
Risk 1:	**Unavailability of business and client data due to ransomware infection propagated through the link or attachement sent by email.**
Main impacts:	Inability to provide translations in time.
	Inability to answer the inquieries.
	Inability to take new projects for translation.
	Unavailability of client info base, translation base, contracts, financial data
ARO (%):	0,40
SLE (in EUR):	22 710,00
ALE (in EUR):	9 084,00
Risk 2:	**The disclosure of confidential corporate client data through unauthorized access to the file server by infecting the information system with Trojan malware sent by email.**
Main impacts:	Penalties due to violation of confidentiality agreement.
	Loss of corporate clients due to the loss of trust.
ARO (%):	0,30
SLE (in EUR):	134 210,00
ALE (in EUR):	40 263,00
Risk 3:	**The disclosure of private data of private clients through unauthorized access to the exchange server by infecting the information system with malware sent by email.**
Main impacts:	The fine due to the violation of GDPR.
	Loss of clients due to the loss of trust.
ARO (%):	0,50
SLE (in EUR):	68 960,00
ALE (in EUR):	34 480,00
Risk 4:	**The disclosure of confidential corporate client data through unauthorized access to the file server by using the flaws of configuration or vulnerabilities in router that is provided by ISP.**
Main impacts:	Penalties due to violation of confidentiality agreement.
	Loss of corporate clients due to the loss of trust.
ARO (%):	0,20
SLE (in EUR):	133 730,00
ALE (in EUR):	26 746,00

Table 3. The acceptance limits of SLE, ARO and ALE set by the firm



The accepted level of SLE, ARO and ALE for the firm	
Maximum SLE (in EUR) accepted if ARO > 15%	10 400,00
Maximum ARO accepted if SLE < Max SLE	80%
Maximum ALE (in EUR) of all major risks included:	93 600,00

Table 4. The alternative security controls

Notation	Security measure	Capabilities
A	LAN-connected NAS backup	Network-connected storage + backup
B	Advanced desktop security solution	Endpoint security
D	Threat prevention firewall solution	Total security
F	Exchange e-mail security solution	Exchange server mail security
G	Threat extraction firewall solution	Total security + document sanitizing
I	Implementation of encryption solution; including introducing the policy; training 10+39+10 people to use it.	Encryption of highly confidential texts, agreements

According to the method the best security alternative is chosen for each risk separately. Considering the tolerance level conditions for SLE, ARO and ALE and the computations of ROSI, then the best investment alternative for risk 1, 2 and 3 is the firewall denoted as “G” and the best option for risk 4 is to invest in firewall “D”. The firm does not need two firewalls but only one. The risks 1 – 3 have the same vulnerabilities to mitigate therefore the results that the most cost-efficient solution for all three risks is the same alternative is somehow expected. The fourth risk uses a different attack vector and leads to prefer another firewall with different functionalities. In this case the firm has to choose between the two firewalls and the final solution is not that difficult to make.

The situation could be much more complex if the attack vectors were different using different vulnerabilities at the same time the alternatives of security measures could be used to mitigate multiple risks. That could lead to the situation were the best choice of mitigating every single risk is different and incompatible when the alternatives act as substitutes to each other. The calculations of ROSI to compare the alternatives of mitigating a single risk at a time are time-consuming, may lead to prefer inconsistent security measures when considering all the risks or favour the alternatives that would not lead to the best use of financial resources when investing in information security.

RORPI

The alternative method to calculate the cost-benefit ratio is to compute the Return on Risk Portfolio Investment (RORPI) (Equation 18), where the risks are aggregated to risk portfolio and the risk treatment alternative which creates the highest return is found.

$$RORPI_k = \frac{ALE\ Total - mALE\ Total_k - Cost\ of\ Treatment_k}{Cost\ of\ Treatment_{\ k}} \qquad (18)$$

$$\forall\ \mathrm{k} = \{1, 2, 3, \dots \mathrm{l}\}$$

Before the RORPI can be calculated, the risk treatment alternatives should be formed. The risks and the controls that mitigate the risks are presented in Table 5. The complementary controls in the table are distinguished by the blue background. The substitutable controls of same type have light-grey background.

Table 5. The risks and suitable controls

	Controls					
Risk 1	A	B	D	F	G	
Risk 2		B	D	F	G	I
Risk 3		B	D	F	G	
Risk 4			D		G	I

The combinations of controls in different mitigation alternatives are showed in Table 6. There are 20 different risk treatment alternatives compared to 42 alternatives when the most effective solution was found for each risk separately.

Table 6. The combination of controls in risk treatment alternatives

Alternatives	**Controls**			
Mit1	D			
Mit2	G			
Mit3	A	D		
Mit4	A	G		
Mit5	B	D		
Mit6	B	G		
Mit7	B	I		
Mit8	D	I		
Mit9	F	I		
Mit10	G	I		
Mit11	A	B	D	
Mit12	A	B	G	
Mit13	A	F	I	
Mit14	A	G	I	
Mit15	B	D	I	
Mit16	B	F	I	
Mit17	B	G	I	
Mit18	A	B	D	I
Mit19	A	B	F	I
Mit20	A	B	G	I

The following step is to estimate how the risk treatment alternative containing specific controls affect the ARO and SLE of each risk in the portfolio. In this case study there are 36 unique combinations of controls affecting the four risks in the portfolio – that means the ARO and SLE should be evaluated 36 times – whether the combination affects ARO and if yes, then how much. The same holds for SLE. The ROSI calculations had 42 unique combinations and the ARO and SLE was required to be estimated 42 times.

After the AROs and SLEs are estimated, denoted as mARO and mSLE, the ALE for each risk in the portfolio can be calculated and summed up as mALE Total. mALE Total shows the Annual Loss Expectancy if the security measures in that particular alternative where implemented. Each risk treatment alternative has its own mALE Total with respect to the risk portfolio.

Now the RORPI for each risk treatment alternative can be calculated using Equation 18. The Cost of Treatment in the equation is the sum of all the relevant costs related to the purchase, implementation and operation of the controls that are present in that particular risk treatment alternative. The RORPI is calculated for 20 alternatives compared to 42 ROSI calculations in the case study. All the calculation results: mAROs, mSLEs, mALEs, mALE Totals and RORPIs are presented in Appendices 6-7.

According to the RORPI calculations and the acceptance limitations set for SLE, ARO and ALE, the best risk treatment alternative for the risk portfolio in the given case study is firewall “G”, having the highest RORPI as well as meeting the tolerance levels presented in Table 2. The best outcome that is presented in Table 7 shows that one invested Euro mitigates approximately 81 Euros of Annual Expected Loss.

Table 7. The results of the calculated best alternative for treating the risks in the portfolio

	Risk 1	**Risk 2**	**Risk 3**	**Risk 4**	**ALE Total**		
ARO	0,40	0,30	0,50	0,20			
SLE	22 710,00	134 210,00	68 960,00	133 730,00			
ALE	9 084,00	40 263,00	34 480,00	26 746,00	110 573,00		
Alternative 2: Control "G"					**mALE Total**	**Cost**	**RORPI**
mARO	0,10	0,05	0,10	0,05			
mSLE	22 710,00	134 210,00	68 960,00	133 730,00			
mALE	2 271,00	6 710,50	6 896,00	6 686,50	22 564,00	1 076,00	80,79

The RORPI calculations allow to find the most cost-efficient security treatment alternative for the risk portfolio, whereas the ROSI calculates the best alternative for every risk separately. In this case study the results do not differ much as the risks 1 – 3 have the same vulnerabilities to be exploited and therefore the calculations of ROSI lead to the same best solution for all three risks and the three risks have also greatest effect on the results of RORPI.

The results of cost-benefit calculations of security measures are organization-specific depending on the business processes, business value creation, the risks, the security of the existent information system and the security measures to be evaluated and calculated. The investment decision making is a process with sequential steps that lead to the final investment decision. The cost-benefit calculation method – whether to use ROSI or RORPI depends on the output from previous steps. RORPI allows to find the combination of information security controls that return most value respect to the amount that is invested in information security when multiple risks are present and security controls are cross-used to treat multiple risks. The risk portfolio approach is not relevant if every single risk has its own specific controls that cannot be used for mitigating any other risk. The RORPI is also not needed if there is only one information security risk present in the organization. The use of ROSI in case of multiple risks may lead to inconsistent and ineffective investment decisions. The important differences of ROSI and RORPI are summarized in Table 8.

Table 8. The main differences of ROSI and RORPI

	ROSI	**RORPI**
Purpose:	To find the highest return on single risk investment	To find the highest return on risk portfolio investment
When to use:	Single risk present	Multiple risks present
	Multiple risks present but every risk has it's own specific countermeasure alternatives.	Countermeasure alternatives are cross-used to mitigate multiple risks.
The main difference:	The cost of risk treatment alternative is not shared between different risks.	The cost of risk treatment alternative is shared between the risks.
Amount of computations:	More computations compared to RORPI	Less computations compared to ROSI

The Limitations and Challenges when Applying the Approach

The first challenge is the will and time of the management to apply the method. The management has to consider the information security as an important issue and information security risk management as their responsibility, otherwise they would not consider the method useful. The second factor is the limited time that the management has. The impact valuation, the search of security expert needed for the technical part of risk assessment, the communication with the security expert, the search for risk treatment alternatives and valuation of the alternatives require time.

The second challenge is the communication between the management and the security expert, so that everyone knows what needs to be analysed and what is the expected outcome.

The third challenge is the difficulty of estimating the risks and the efficiency of risk treatment alternatives. The threat environment is constantly changing and the estimations are always static based on certain expectations. The use of the method allows to understand the existent most probable threats and possible negative impacts, which allows to deal with known-factors and also to be better prepared for unknown.

The fourth challenge is to understand that the use of the method do not provide better security unless the risk treatment that is chosen and invested in is implemented and operated according to the best practices and the people in the firm follow the set security policies.

When the business grows, the method may not be any longer reasonable to use mainly for two reasons. The decision-making in larger firms is distributed and the person being responsible of information security risk management may not be anymore the person who is familiar with the cash flows. The second reason is that at certain point of time the firm may draw the attention of targetiers, and the more thorough risk assessment as well as more advanced risk management would be needed.

4. Conclusions

A quarter of the yearly turnover created in Estonia is generated by small enterprises. A quarter of the Estonian employees are working in small enterprises. It is not possible to say how much the information systems support the business processes and value creation in small firms, but the calculations using the data from Statistics Estonia database (FS001, 2015; IC0081, 2016) show that there are twice as many small firms than medium and large firms together using e-commerce or providing e-booking for their clients.

At the same time the amount of small businesses using the opportunities of e-commerce is larger than the amount of small businesses having security policies defined or information technology specialists hired (IC140, 2015; IC138, 2017). The gap between the use of e-commerce and security indicators is not present in case of medium and large enterprises.

Being a part of interconnected information technology network opens the firm to potential attackers. The small firms may not draw the attention of financially motivated targetiers but they are definitely potential victims of opportunistic attackers who take the advantage of existing vulnerabilities in information systems irrespective of who the victims are.

The main incentive to invest in information and information system security is to reduce the risk of security violation. The larger the negative impact to business critical processes, the business value creation and protection when the risks occur, the more motivated the firm is to invest in information and information system security. The negative impact in absolute value is generally higher in larger firms compared to small firms but the relative negative impact to business continuity may be larger for small firms. The loss of income due to interrupted business processes and additional costs required to recover the information systems may easily lead the small business to liquidity crises.

The investments in information security may also be motivated by the incentive to avoid the possible fines and penalties due to not following the legal regulations concerning security issues. For example the non-compliance of GDPR applied from May 25th 2018 may entail sanctions including fines as well as claims for damages from European Union residents. The GDPR is an important issue for small businesses. The sales to private persons via e-channels constitute the same proportion from their turnover than it constitutes in large firms (IC0081, 2016).

The third incentive to invest in information system security may be the chance to create new business opportunities. The small firms may be required to improve their information security in order to be considered as a qualified business partner or service provider.

The information and information system security investment decisions can be made without understanding the benefits (or waste) of the investment – without understanding whether the business critical processes and value creation or protection is better secured after the investment is made. Good information security investment decisions cannot be made without knowing what needs to be protected and what would be the benefit of making the investment. Good investment decisions require appropriate risk assessment. The outcome from risk assessment is the input to investment decision making formula to solve the information security investment problem that the enterprise has.

Academic literature provides a considerable amount of approaches solving different information security investment problems by using various methods. There are theoretical approaches providing better insight to factors that should be considered when making investment decisions along with the models intended to be used in practice. A vast majority of the approaches and methods are not suitable for small firms because either the investment problem that is solved is irrelevant for small firms or the implementation of the method would not be economically justified or the resources that are needed for the implementation are not affordable for the small firms.

Large organizations have many levels of management. Decision making is delegated and every managerial level in its domain has its own goals, responsibility, resources and investment problem(s). Large firms in general have implemented information security risk management framework or enterprise management system. They have established understanding about their needed security levels and have set information security related goals. These are the general conditions that are present in the approaches provided in academic literature.

At the same time the small enterprises have flat structure. All the investment decisions concerning the business as well as information security is made by the CEO of the firm or the management team. Small firms have unlikely implemented any security risk management or enterprise management framework. They have unlikely defined their needed security levels and set information security goals. All the investment decisions that are made are directly linked to the business goals and needs. They have one budget for all the investments and they have to find the balance between the investments that are intended to create the value and the investments that are intended to enable the value creation and protection. They do not allocate a certain share from their overall budgets to security investments and maximize the security subject to the share of the budget constraint as the next step. Their investment problem is to minimize the costs to information and information system security subject to the accepted risk tolerance level measured in monetary terms. The accepted risk tolerance level shows the level of the risks that the firm is willing to take and should be able to bear when the risks occur.

From the approaches and methods analysed, the cost-benefit approach calculating the cost-benefit ratio is suitable for small enterprises as it allows to assess the benefit of the investment to the business in monetary terms. The classical Return on Security Investment (ROSI) calculation has been used to justify the economic relevance of certain security measure or finding the risk treatment alternative which provides the highest return on mitigating a specific risk. When multiple risks are present and the alternative security measures can mitigate different risks then calculating the ROSI for each risk separately may lead to inconsistent and ineffective investment decisions.

The author of the thesis proposes to aggregate the risks to risk portfolio and calculate the Return on Risk Portfolio Investment (RORPI). If the remaining risk level with the risk treatment alternative with highest RORPI would stay above the accepted risk tolerance level, then the next highest RORPI should be assessed towards the predefined risk tolerance conditions until the highest RORPI satisfying the accepted risk tolerance level conditions is found subject to RORPI > 1. If none of the risk treatment alternatives satisfy the predefined conditions or the alternatives are not economically justified (RORPI ≤ 1), then the business critical processes supported by the information systems should be revised. RORPI calculations are valuable if the information system of the small enterprise supports business critical processes, value creation and protection.

Input to RORPI calculations comes from risk assessment and risk treatment considerations that are advisable to perform as a combined effort between the management of the business and an information security specialist. It is also reasonable to involve security vendors when considering the risk treatment alternatives.

The management of the firm can best assess the impact of security violations to its business and that can be done through estimating the impact of the violations to cash flows. Cash flow analysis shows not only the overall impact but also the impact to the liquidity of the firm which is essential for small businesses who have scarce financial resources.

The technical risk assessment can be best performed by a security expert as it requires knowledge about the threat landscape, auditing the existent information system in terms of its vulnerabilities and assessing the probability of the security violations. The security expert can also determine the possible consequences to the information system when the risks occur and propose the time and resources that are needed to recover the system. Based on the vulnerability and threat assessment the risk treatment alternatives can be proposed and their effectivity of mitigating the risks should be estimated.

There are three main challenges when applying the method. The first challenge is that the management of the small enterprise has to have a will and time to apply the method. The second challenge is to ensure smooth and constructive communication between the management and the security expert, so that everyone knows what needs to be analysed and what is the expected outcome. The third challenge is to cope with the uncertainty. The threat environment is constantly changing and the estimations are always static based on certain expectations. Estimating the risks and the efficiency of risk treatment alternatives is not an easy task.

The relative accuracy of the estimations is more important than the punctuality of the estimates. The content behind the figures is more important than the numeric values themselves. Making good information and information security investment decisions is somewhere between art and science.

References

1. Ablon, L., Heaton, P., Lavery, D. C., Romanosky, S. (2016). Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information. – RAND Corporation. www.rand.org/t/rr1187 (17.01.2017)

2. Al-Humaigani, M., Dunn, D. B. (2004). A Model of Return on Investment for Information Systems Security. – IEEE, 0-7803-8294-3/04, 483-485.

3. Anderson, E., Choobineh, J. (2008). Enterprise information security strategies. – Computers & Security, 27, 22-29.

4. Anderson, P. Schneier, B. (2005). Economics of Information Security. – IEEE Security & Privacy, 24-25.

5. Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T., Savage, S. (2013). Measuring the Cost of Cybercrime. – The Economics of Information Security and Privacy, Böhme, R. (Eds), Springer, 265-300.

6. Anderson, R., Böhme, R., Clayton, R., Moore, T. (2009). Security Economics and European Policy. – Managing Information Risk and the Economics of Security, Johnson, M. E., Springer, 55-80.

7. Anderson, R., Moore, T. (2006). The Economics of Information Security. – Science, Vol. 314, 27. Oct, 610-613.

8. Baldwin, A., Beres, Y., Duggan, G. B., Mont, M. C., Johnson, H., Middup, C, Shiu, S. (2013). Economic Methods and Decision Making by Security Professionals. – Economics of Information Security and Privacy III, Schneier, Springer, 213-238.

9. Barth, A., Rubinstei, B. I. P., Sundararajan, M., Mitchell, J. C., Song, D., Bartlett, P. L. (2010). A Learning-Based Approach to Reactive Security. – R. Sion (Ed.): FC 2010, LNCS 6052, 192-206.

10. Bauer, J. M., van Eeten, M. J. G. (2009). Cybersecurity: Stakeholder incentives, externalities and policy options. – Telecommunications Policy 33, 706-719.

11. Bellovin, S. M. (2016). Thinking Security: Stopping Next Year’s Hackers. – Addison-Wesley.

12. Berinato, S. (2002). Finally, a Real Return on Security Spending. – http://www.cio.com/article/2440999/metrics/finally--a-real-return-on-security-spending.html (7.11.2016)

13. Biener, C., Eling, M., Wirfs, J. H. (2015). Insurability of Cyber Risk: An Empirical Analysis. – Working papers on Risk Management and Insurance No. 151; Schmeiser, H. (Ed); Institute od Insurance Economics, University of St. Gallen.

14. Bistarelli, S., Fioravanti, F., Peretti, P. (2007). Using CP-nets as a guide for countermeasure selection. – Proceedings of the 2007 ACM symposium on Applied computing, 300-304.

15. Bodin, L. D., Gordon, L. A., Loeb, M. P. (2005). Evaluating Information Security Investments Using the Analytic Hierarchy Process. – Communication of the ACM, February, Vol. 48, No 2, 79-83.

16. Böhme, R. (2005a). Vulnerability markets. – The 22nd Chaos Communication Congress: 2005 December, Berliner Congress Center, Berlin, https://events.ccc.de/congress/2005/fahrplan/attachments/542-Boehme2005_22C3_VulnerabilityMarkets.pdf (28.10.2016)

17. Böhme, R. (2005b). Cyber-Insurance Revisited. – WEIS.

18. Böhme, R. (2010). Security Metrics and Security Investment Models. – Advances in Information and Computer Security; Lecture Notes in Computer Science Volume 6434, in Echizen (Ed), 10-24.

19. Böhme, R., Felegyhazi, M. (2010). Optimal Information Security Investment with Penetration Testing. – Decision and Game Theory for Security (Alpcan, T., Buttyan, L, Baras, J. S. (Ed)), 21-37.

20. Böhme, R., Moore, T. (2009). The Iterated Weakest Link: A Model of Adaptive Security Investment. – WEIS 2009.

21. Böhme, R., Nowey, T. (2008). Economic Security Metrics. – "Dependability Metrics", Advanced Lectures, LNCS 4909 Eusgeld. I., Freiling F., Reussner, R. (Eds), 176-187.

22. Bojanc, R., Jerman-Blažic, B. (2008a). Towards a standard approach for quantifying an ICT security investment. – Computer Standards and Interfaces 30, 216-222.

23. Bojanc, R., Jerman-Blažic, B. (2008b). An Economic modelling approach to information security risk management. – International Journal of Information Management 28, 413-422.

24. Bojanc, R., Jerman-Blažic, B. (2013). A Quantitative Model for Information-Security Risk Management. – Engineering Management Journal, Vol. 25, No. 2, June, 25-37.

25. Bojanc, R., Jerman-Blažic, B., Tekavcic, M. (2012). Managing the investment in information security technology by use of a quantitative modeling. – Information Processing and Management 48, 1031-1052.

26. Bolot, J., Lelarge, M. (2009). Cyber Insurance as an Incentive for Internet Security. – Managing Information Risk and the Economics of Security, Johnson, M. E., Springer, 269-290.

27. Brecht, M., Nowey, T. (2013). A Closer Look at Information Security Costs. – Böhme (ed) The Economics of Information Security and Privacy, Springer

28. Broderick, J. S. (2001). Information Security Risk Management – When should it be managed? – Information Security Technical Report, Vol 6, No. 3, 12-18.

29. Brotby W. Krag. (2009). Information Security Management Metrics. – A Definite Guide to Effective Security Monitoring and Measurement, Auerback Publications.

30. Buldas, A., Laud, P., Priisalu, J., Saarepera, M., Willemson, J. (2006). Rational Choice of Security Measures via Multi-Parameter Attack Trees. – In: Critical Information Infrastructures Security. First International Workshop, CRITIS, 235-248.

31. Butler, S. A. (2002). Security Attribute Evaluation Method: A Cost-Benefit Approach. – Proceedings of the 24th International Conference on Software Engineering, Orlando. ACM, 232-240.

32. Camp, L. J., Wolfram, C. D. (2004). Pricing Security: Vulnerabilities as Externalities. – Economics of Information Security, Vol. 12, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=894966 (11.05.2016)

33. Cavusoglu, H., Mishra, B., Raghunathan, S. (2005). The Value of Intrusion Detection Systems in Information Technology Security Architecture. – Information Systems Research, Vol. 16, No. 1, March, 281-304.

34. Cavusoglu, H., Raghunathan, S., Cavusoglu, H. (2009). Configuration of and Interaction Between Information Security Technologies: The Case of Firewalls and Intrusion Detection Systems. – Information Systems Research Vol. 20, No. 2, June, 198-217.

35. Cavusoglu, H., Raghunathan, S., Yue, W. T. (2008). Decision-Theoretic and Game-Theoretic Approaches to IT Security Investment. – Journal of Management Information Systems, Fall, Vol. 25, No.2, 281-304.

36. Cavusoglu, H., Cavusoglu, H., Raghunathan, S. (2004a). Economics of IT security Management: four improvements to current security practices. – Communication of the Association for Information Systems, Vol. 14, 65-75.

37. Cavusoglu, H., Mishra, B., Raghunathan, S. (2004b). A Model for Evaluating IT Security Investments. – Communications of the ACM July / Vol. 47 No. 7, 87-92.

38. Cremonini, M., Martini, P. (2005). Evaluating Information Security Investments from Attackers Perspective: the Return-On-Attack (ROA). – Proceedings of the 4th Workshop on the Economics of Information Security (WEIS).

39. Cremonini, M., Nizovtsev, D. (2006). Understanding and Influencing Attackers' Decisions: Implications for Security Investment Strategies. – WEIS. http://www.econinfosec.org/archive/weis2006/docs/3.pdf (15.11.2016)

40. Demetz, L., Bachlechner, D. (2013). To Invest or Not to Invest? Assessing the Economic Viability of a Policy and Security Configuration Management Tool. –

The Economics of Information Security and Privacy, Böhme, R. (Eds), Springer, 25-47.

41. Dewri, R., Ray, I., Poolsappasit, N., Whitley, D. (2012). Optimal security hardening on attack tree models of networks: a cost-benefit analysis. – International Journal of Information Security. 11, 167–188.

42. Dimopoulos, V., Furnell, S. (2005). A Protection Profiles Approach to Risk Analysis for Small and Medium Enterprises. – Dowland P., Furnell S., Thuraisingham B., Wang X.S. (eds) Security Management, Integrity, and Internal Control in Information Systems. IFIP International Federation for Information.

43. Dimopoulos, V., Furnell, S., Jennex, M., Kritharas, I. (2004). Approaches to IT Security in Small and Medium Enterprises. – Conference paper, Proceedings of the 2nd Australian Information Security Management Conference, Securing the Future Perth, Western Australia, November 26th, 2004.

44. Ding, W., Yurcik, W. (2005). Outsourcing Internet Security: The Effect of Transaction Costs on Managed Service Providers. – In Proceedings of the International Conference on Telecommunication Systems, Modeling and Analysis. Dallas, TX.

45. Ding, W., Yurcik, W. (2006). Economics of Internet Security Outsourcing: Simulation Results Based on the Schneier Model. – In: Proceedings of the Workshop on the Economics of Securing the Information Infrastructure, Washington DC.

46. Ding, W., Yurcik, W., Yin, X. (2005). Outsourcing Internet Security: Economic Analysis of Incentives for Managed Security Service Provider. – Internet and Network Economics, Vol. 3828 of the series Lecture Notes in Computer Science (Deng, X, Ye, Y (Ed)), 947-958.

47. Dlamini, M.T., Eloff, M.M., Eloff, J. H. P., Venter, H.S. (2011). A Budget Model for Information Security. – Proceedings of the Fifth International Symposium on Human Aspects of Information Security & Assurance.

48. Dutta, A., McCrohan, K. (2002). Management's Role in Information Security in a Cyber Economy. – California Management Review, Vol. 45, No.1 Fall, 67-87.

49. Dynes, S., Brechbühl, H., Johnson, M. E. (2005). Information Security in the Extended Enterprise. Some Initial Results From a Field Study of an Industrial Firm. http://infosecon.net/workshop/pdf/51.pdf (1.12.2016)

50. Dynes, S., Goetz, E., Freeman, M. (2008). Cyber Security: are economic incentives adequate? – IFIP International Federation for Information Processing, Vol. 253, Critical Infrastructure Protection, eds. E. Goetz and S. Shenoi (Boston, Springer), 15-27.

51. ENISA (2012). Introduction to Return on Security Investment, – https://www.enisa.europa.eu/activities/cert/other-work/introduction-to-return-on-security-investment/at_download/fullReport (4.01.2017)

52. EU Recommendation (2003/361). http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003H0361&from=EN (8.10.2017)

53. Farahmand, F., Navathe, S. B., Sharp, G. P., Enslow, P. H. (2005). A Management Perspective on Risk of Security Threats to Information Systems. – Information Technology and Management 6, 203-225.

54. Farnan, O. J., Nurse, J. R.C. (2016). Exploring a Controls-Based Assessment of Infrastructure Vulnerability. – Risks and Security of Internet and Systems, 10th Int Conference CRISIS 2015, Lambrinoudakis, C., Gabillon, A. (Eds), 144-159.

55. Fenz, S., Heurix, J., Neubauer, T., Pechstein, F. (2014). Current challenges in information security risk management. – Information Management & Computer Security, 13-33.

56. Florencio, D., Herley, C. (2013a) Where Do All the Attack Go? – Economics of Information Security and Privacy III, Schneider, 2013, Springer, 13-33.

57. Florencio, D., Herley, C. (2013b) Sex, Lies and Cyber-Crime Surveys. – Economics of Information Security and Privacy III, Schneider, Springer, 35-53.

58. FS001. (2015). Enterprises' income statement by economic activity (EMTAK 2008) and number of persons employed. – Statistics Estonia. (29.09.2017)

59. Gadyatskaya, O., Harpes, C., Mauw, S., Muller, C., Muller, S. (2016). Bridging Two Worlds: Reconciling Practical Risk Assessment Methodologies with Theory of Attack Trees. – Graphical Models for Security, Vol 9987 of the series Lecture Notes in Computer Science, 80-93.

60. Gilligan, J. (2013). The Economics of Cybersecurity: A Practical Framework for Cybersecurity Investment. – http://www.afcea.org/mission/intel/documents/EconomicsofCybersecurityFinal10-24-13.pdf (11.05.2016)

61. Gilligan, J. (2014). The Economics of Cybersecurity Part II: Extending the Cybersecurity Framework. – http://www.afcea.org/committees/cyber/documents/EconomicsofCybersecurityPartII-Final4-2-14.pdf (11.05.2016)

62. Gonzalez Granadillo, G., Belhaouane, M., Débar, H., Jacob, G., (2014b). RORI-based countermeasure selection using the OrBAC formalism – International Journal of Information Security, Feb, Vol 13, Issue 1, 63-79.

63. Gonzalez Granadillo, G., Débar, H., Jacob, G., Coppolino, L. (2012b). Combination Approach to Select Optimal Countermeasures based on the RORI Index. – Innovative Computing Technology (INTECH), Second International Conference.

64. Gonzalez Granadillo, G., Débar, H., Jacob, G., Gaber, C., Achemlal, M. (2012a). – Individual countermeasure selection based on the return on response investment index. – Computer Network Security, MMM-ACNS 2012, Kotenko, I., Skormin, V. (Ed), 156-170.

65. Gonzalez Granadillo, G., Ponchel, C., Blanc, G., Débar, H. (2014a). Combining Technical and Financial Impacts for Countermeasure Selection. – J. Garcia-Alfaro, G. Gür (Eds.): Advanced Intrusion and Prevention Workshop (AIDP 2014), 1-14.

66. Gordon, L. A., Loeb, M. P. (2002b). The Economics of Information Security Investment. – ACM Transactions on Information and System Security, Vol. 5, No. 4, November, 438-457.

67. Gordon, L. A., Loeb, M. P., Lucyshyn, W. (2003a). Information Security Expenditures and Real Options: A Wait-and-See Approach. – Computer Security Journal, Volume XIX, No 2, 1-7.

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

69. Gordon, L. A., Loeb, M. P., Lucyshyn, W., Zhou, L. (2015a). Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model. – Journal of Information Security, 6, 24-30.

70. Gordon, L. A., Loeb, M. P., Lucyshyn, W., Zhou, L. (2015b). Increasing cybersecurity investments in private sector firms. – Journal of Cybersecurity, 1(1), 3-17.

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

72. Granadillo, G. G., Debar, H., Jacob, G., Coppolino, L. (2012b). Combination Approach to Select Optimal Countermeasures based on the RORI Index. – Innovative Computing Technology (INTECH), Second International Conference, 38-45.

73. Halliday, S., Badenhorst K., vonSolms R. (1996). A business approach to effective information technology risk analysis and management. – Information Management & Computer Security 4/1, 19-31.

74. Herath, H., Herath, T. (2008-2009). Investments in Information Security: A Real Options Perspective with Bayesian Postaudit. – Journal of Management Information Systems, Winter, Vol.25, No. 3, 337-375.

75. Huang, C. D., Behara, R. S. (2013). Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints. – International Journal of Production Economics 141, 255-268.

76. Huang, C. D., Hu, Q., Behara, R. S. (2006). Economics of Information Security Investment in the Case of Simultaneous Attacks. – WEIS.

77. 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 Production Economics 114.

78. Hui, K.L., Hui, W., Yue, W. T. (2012). Information Security Outsourcing with System Interdependency and Mandatory Security Requirement. – Journal of Management Information Systems, 29:3, 117-156.

79. IC004. (2017) Enterprises using computers by economic activity (EMTAK 2008) and number of persons employed. – Statistics Estonia. (29.09.2017)

80. IC008. (2017). Enterprises having websites by economic activity (EMTAK 2008), number of persons employed and facilities provided by the website. – Statistics Estonia. (29.09.2017)

81. IC0081. (2016). Enterprises using e-commerce by economic activity (EMTAK 2008) and number of persons employed. – Statistics Estonia. (29.09.2017)

82. IC138. (2017). Presence of ICT specialists by economic activity (EMTAK 2008) of enterprise and number of employed persons – Statistics Estonia. (29.09.2017)

83. IC139. (2015). Enterprises by economic activity (EMTAK 2008), number of persons employed, IT-activity and the main performer. – Statistics Estonia. (29.09.2017)

84. IC140. (2015). Use of formally defined ICT security policy in enterprises by economic activity (EMTAK 2008) and number of persons employed. – Statistics Estonia. (29.09.2017)

85. Jaisingh, J., Rees, J. (2001). Value at Risk: A methodology for Information Security Risk Assessment. – CERIAS Tech Report 2001-127. https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2001-127.pdf (17.01.2017)

86. Kanungo, S. (2006). Portfolio approach to information technology security resource allocation decisions. – The Tenth Pacific Asia Conference on Information Systems, 286-299.

87. Kaplan, R. S., Norton, D. P. (2002). Fokus på strategier: Balanced scorecard som strategiværktøj i organisationer. – Børsens Forlag.

88. Khanmohammadi, K., Houmb, S. H. (2010). Business Process-based Information Security Risk Assessment. – Fourth International Conference on Network and System Security, 199-206.

89. Khouzani, MHR., Malacaria, P, Hankin, C., Fielder, A., Smeraldi, F. (2016). Efficient Numerical Frameworks for Multi-objective Cyber Security Planning. – Computer Security – ESORICS 2016, Part II, (Askoxylakis, I (Ed)), 179-197.

90. Kim S., Lee H. J. (2005). Cost-Benefit Analysis of Security Investments: Methodology and Case Study. – ICCSA 2005, LNCS 3482, 1239-1248.

91. Kirt, T., Kivimaa, J. (2010). Optimizing IT Security costs by evolutionary algorithms. – Conference on Cyber Conflict Proceedings, C. Czosseck and K. Podins (Eds.) CCD COE Publications, Tallinn, Estonia, 145-160

92. Kong, H.-K., Kim, T.-S., Kim, J. (2012). An analysis on effects of information security investments: a BSC perspective. – Journal of Intelligent Manufacturing. Aug, Vol. 23, Issue 4, 941-953.

93. Kumar, R., Park, S., Subramaniam, C. (2008). Understanding the Value of Countermeasure Portfolios in Information Systems Security. – Journal of Management Information Systems, Fall, Vol. 25, No. 2, 241-179.

94. Lee, W., Fan, W., Miller, M., Stolfo, S. J., Zadok, E. (2002) Toward Cost-Sensitive Modeling for Intrusion Detection and Response. – Journal of Computer Security, Vol 10, issue 1-2.

95. Locher, C. (2005). Methodologies for evaluating information security investments – what Basel II can change in the financial industry. – ECIS Proceedings Paper 122.

96. Magnusson, C., Molvidsson, J, Zetterqvist, S. (2007). Value creation and Return On Security Investments (ROSI), – IFIP International Information Security Conference, SEC 2007: New Approaches for Security, Privacy and Trust in Complex Environments, 25-35.

97. Martin, C., Kadry, A., Abu-Shady, G. (2014). Quantifying the Financial Impact of IT Security Breaches on Business Processes. – Twefth Annual Conference on Privacy, Security and Trust (PST), IEEE.

98. Moore, T. (2010a). Introducing the Economics of Cybersecurity: Principles and Policy Options. – Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S Policy, 3-23.

99. Moore, T. (2010b). The Economics of Cybersecurity: Principles and Policy Options. – International Journal of Critical Infrastructure Protection, Dec, Volume 3, Issues 3-4, 103-117.

100. Moore, T., Anderson, R. (2012). Internet Security. – The Oxford Handbook of the Digital Economy, Security; CSE5390/7390: Economics of Information Security; Peitz, M., Waldfogel., J. Eds Oxford University Press, New York, NY, 572-599.

101. Moore, T., Clayton, R., Anderson, R. (2009). The Economics of Online Crime. – Journal of Economic Perspectives – Vol 23, No. 3, Summer, 3-20.

102. Moore, T., Dynes, S., Chang F. R. (2016). Identifying How Firms Manage Cybersecurity Investment. – Workshop on the Economics of Information Security, Berkley, CA WEIS.

103. Muller, P., Devnani, S., Julius, J., Gagliardi, D., Marzocchi, C. (2016) Annual Report on European SMEs 2015/2016. – European Commission.

104. NCSC (National Cybersecurity Center). (2016a). Common cyber attacks: reducing the impact. – Cyber Attacks White Paper, January. https://www.ncsc.gov.uk/white-papers/common-cyber-attacks-reducing-impact (19.01.2017)

105. NIST (2012). Guide for Conducting Risk Assessment. – http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf (11.04.2016)

106. Ojamaa, A., Tõugu, E., Kivimaa, J. (2008). Pareto-optimal situation analysis for selection of security measures. – IEEE.

107. Panaousis, E., Fiedler, A., Malacaria, P., Hankin, C., Smeraldi, F. (2014). Cybersecurity Games and Investments: A Decision Support Approach. – Decision and Game Theory for Security (Poovendran, R., Saad, W. (Eds.), 266-286.

108. Purser, S. A. (2004). Improving the ROI of the security management process. – Computers & Security, 23, 542-546.

109. Radulescu, M. C. (2016). Considerations on the selection and prioritization of information security solutions. – Audit Financiar, Vol, XIV, No. 5(137), 564-574.

110. Richardson, R. (2010/2011). CSI Computer Crime and Security Survey, CSI Computer Security Institute. https://cours.etsmtl.ca/gti619/documents/divers/CSIsurvey2010.pdf (09.09.2017)

111. Rowe, B. R. (2007). Will Outsourcing IT Security Lead to a Higher Social Level of Security. – WEIS 2007.

112. Ryan, J. J. C. H., Mazzuchi, T. A., Ryan D. J., Lopez de la Cruz, J., Cooke, R. (2012). Quantifying information security risks using expert judgment elicitation. – Computers & Operations Research 39, 774-784.

113. Saaty, R. W. (1987). The analytic hierarchy process – what it is and how it is used. – Mathematical Modelling, Volume 9, Issues 3–5, 161-176.

114. Sawik, T, (2013). Selection of optimal countermeasure portfolio in IT security planning. – Decision Support Systems 55, 156-164.

115. Schechter, S. E. (2004). Computer Security Strength & Risk: A Quantitative Approach. – A dissertation, Harvard University.

116. Schilling, A., Werners, B. (2015). Optimal Information Security Expenditures Considering Budget Constraint. – Pacific Asia Conference on Information Systems (PACIS) Proceedings, Paper 251. http://aisel.aisnet.org/pacis2015/251 (14.01.2017)

117. Schneier B. (2008). Security ROI: Fact or Fiction? – CSO Magazine, September 2, 2008.

118. Shameli-Sendi, A., Aghababaei-Barzegar, R., Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). – Computers & Security 57, 14-30.

119. Sklavos, N., Souras, P. (2006). Economic Models and Approaches in Information Security for Computer Networks. – International Journal of Network Security, Vol.2, No.1, 14-20.

120. Sonnenreich, W., Albanese, J., Stout, B. (2006). Return on Security Investment (ROSI) - A Practical Quantitative Model. – Journal of Research and Practice in Information Technology, Vol. 38, No. 1, February, 1-15.

121. Soo Hoo, K. J. (2000). How Much Is Enough? A Risk-Management Approach to Computer Security. – Consortium for Research on Information Security and Policy (CRISP), June. http://cisac.fsi.stanford.edu/publications/how_much_is_enough__a_riskmanagement_approach_to_computer_security (10.12.2016)

122. Su, X. (2006). An overview of economic Approaches to Information security Management. – Technical Report TR-CTIT-06-30, University of Twente. http://doc.utwente.nl/66172/1/00000177.pdf (4.11.2016).

123. Tallau, L. J., Gupta, M., Sharman, R. (2010). Information security investment decisions: evaluating the balanced scorecard method. International Journal of Business Information Systems 5(1), 34–57.

124. Tatsumi, K., Goto, M. (2010). Optimal Timing of Information Security Investment: A Real Options Approach. – Economics of Information Security and Privacy, Moore, T., Pym, D., Ioannidis, C. (Ed), 211-228.

125. Toivanen, H. (2015). Case Study of Why Information Security Investment Decision Fail? – Jyväskylän Yliopisto, Tietojenkäsittelytieteiden Laitos, 2015

126. Tsiakis, T. (2010). Information Security Expenditures: a Techno-Economic Analysis. – IJCSNS International Journal of Computer Science and Network Security, Vol. 10, No. 4, April, 7-11.

127. Tsiakis, T. K., Pekos, G. D. (2008). Analysing and determining Return on Investment for Information Security. – International Conference on Applied Economics – ICOAE. http://kastoria.teikoz.gr/icoae2/wordpress/wp-content/uploads/articles/2011/10/103-2008.pdf (3.3.2016)

128. Varian, Hal R. (2004). System Reliability and Free Riding. – Economics of Information Security, Vol. 12 of the series Advances in Information Security, 1-15.

129. vom Brocke, J., Strauch, G., Buddendick, C. (2007). Return on Security Investments – Towards a Methodological Foundation of Measurement Systems. – Paper presented at the 13th Americas Conference on Information Systems (AMCIS 2007), Keystone, CO, USA. (VHB: D).

130. Wang, Q., Zhu, J. (2016). Optimal Information Security Investment Analyses with the Consideration of the Benefits of Investment and Using Evolutionary and Using Evolutionary Game Theory. – Information Management (ICIM), 2016 2nd International Conference.

131. Wei, H., Frinke, D., Carter, O., Ritter, C. (2001). Cost-benefit analysis for network intrusion detection systems. – CSI 28th Annual Computer Security Conference; October 29-31, Washington, D.C.

132. Willemson, J. (2006). On the Gordon & Loeb Model for Information Security Investment. – WEIS 2006.

133. Willemson, J. (2010). Extending the Gordon & Loeb Model for Information Security Investment. – 2010 International Conference on Availability, Reliability and Security, IEEE.

134. Wood, C. C., Parker, D. B. (2004). Why ROI and similar financial tools are not advisable for evaluating the merits of security projects. – Computer Fraud & Security, Volume 2004, Issue 5, May, 8-10.

135. Zhuo, Y., Solak, S. (2014). Measuring and Optimizing Cybersecurity Investments: A Quantitative Portfolio Approach. – Proceedings of the 2014 Industrial and Systems Engineering Research Conference, Guan, Y., Liao, H. Eds.

Appendix 1 – The Summary of Information Security Investment Approaches

Chapter		Approach	Rather theoretical or practical approach	Relevance of the investment problem for the small firms	Applicable by the small firms
3.2.1.	1.	Gordon, Loeb (2002b)	Theoretical	Not relevant	No
	2.	Gordon *et al.* (2016)	Theoretical	Not relevant	No
	3.	Huang *et al.* (2008)	Theoretical	Not relevant	No
	4.	Huang *et al* .(2006)	Theoretical	Not relevant	No
	5.	Wang, Zhu (2016)	Theoretical	Not relevant	No
	6.	Huang, Behara (2016)	Theoretical	Not relevant	No
3.2.2.	7.	Bodin *et al.* (2005)	Practical	Not relevant	No
	8.	Kanungo (2006)	Practical	Not relevant	No
	9.	Ojamaa *et al.* (2008)	Practical	Not relevant	No
	10.	Kirt, Kivimaa (2008)	Practical	Not relevant	No
	11.	Dlamini (2011)	Theoretical	Not relevant	No
	12.	Dewri *et al.* (2012)	Theoretical	Not relevant	No
	13.	Khouzani *et al.* (2016)	Theoretical	Not relevant	No
	14.	Panaousis *et al.* (2014)	Theoretical	Not relevant	No
	15.	Zhuo, Zolak (2014)	Theoretical	Not relevant	No
3.2.3.	16.	Butler (2002)	Practical	Partially	No
	17.	Buldas *et al.* (2006)	Practical	Not relevant	No
	18.	Bistarelli *et al.* (2007)	Practical	Not relevant	No
	19.	Kumar *et al.* (2008)	Theoretical	Not relevant	No
3.2.4.	20.	Soo Hoo (2000)	Practical	Relevant	Partially
	21.	Pfleeger, Pfleeger (2003)	Practical	Relevant	Partially
	22.	Al-Humaigani, Dunn (2004)	Theoretical	Relevant	No
	23.	Purser (2004)	Theoretical	Relevant	No
	24.	Dimopoulos, Furnell (2005)	Practical	Not relevant	No
	25.	Sonnenreich *et al.* (2006)	Practical	Relevant	Yes
	26.	ENISA (2012)	Practical	Relevant	Yes
	27.	Bojanc *et al.* (2012); Bojanc, Jerman-Blažic (2013)	Theoretical	Relevant	No
	28.	Gonzalez-Granadillo *et al.* (2012a, 2012b, 2014a, 2014b)	Practical	Relevant	No
3.2.5.	29.	Gordon et al.(2003a)	Practical	Relevant	No
	30.	Herath, Herath (2008-2009)	Practical	Relevant	No
	31.	Böhme, Moore (2009)	Theoretical	Not relevant	No
	32.	Barth *et al.* (2010)	Theoretical	Not relevant	No
	33.	Tatsumi, Goto (2010)	Theoretical	Not relevant	No
	34.	Tallau *et al.* (2010); Kong *et al.* (2012)	Practical	Not relevant	No

Appendix 2/5 – The Results of mARO, mSLE, mALE and ROSI with Different Security Risk Treatment Options Calculated Separately for Each Risk

Alternative		**Control**	**Risk 1**		**Control**	**Risk 2**		**Control**	**Risk 3**		**Control**	**Risk 4**
	ARO		0,40			0,30			0,50			0,20
	SLE		22 710,00			134 210,00			68 960,00			133 730,00
	ALE		9 084,00			40 263,00			34 480,00			26 746,00
Mit 1	mARO	A	0,40	**Mit16**	B	0,20	**Mit31**	B	0,35	**Mit 38**	D	0,05
	mSLE		10 710,00			134 210,00			68 960,00			133 730,00
	mALE		4 284,00			26 842,00			24 136,00			6 686,50
	Cost		835,00			835,00			857,00			956,00
	ROSI		**4,75**			**15,07**			**11,07**			**19,98**
Mit2	mARO	B	0,30	**Mit17**	D	0,15	**Mit32**	D	0,30	**Mit 39**	G	0,05
	mSLE		22 710,00			134 210,00			68 960,00			133 730,00
	mALE		6 813,00			20 131,50			20 688,00			6 686,50
	Cost		857,00			956,00			956,00			1 076,00
	ROSI		**1,65**			**20,06**			**13,43**			**17,64**
Mit3	mARO	D	0,30	**Mit18**	F	0,28	**Mit33**	F	0,40	**Mit 40**	I	0,20
	mSLE		22 710,00			134 210,00			68 960,00			117 000,00
	mALE		6 813,00			37 578,80			27 584,00			23 400,00
	Cost		956,00			300,00			300,00			2 300,00
	ROSI		**1,38**			**7,95**			**21,99**			**0,45**

Appendix 3/5 – The Results of mARO, mSLE, mALE and ROSI with Different Security Risk Treatment Options Calculated Separately for Each Risk

Alternative		**Control**	**Risk 1**		**Control**	**Risk 2**		**Control**	**Risk 3**		**Control**	**Risk 4**
Mit4	mARO	F	0,35	**Mit19**	I	0,30	**Mit34**	B,D	0,14	**Mit 41**	D,I	0,05
	mSLE		22 710,00			117 960,00			68 960,00			117 000,00
	mALE		7 948,50			35 388,00			9 654,40			5 850,00
	Cost		300,00			2 300,00			1 453,00			3 256,00
	ROSI		**2,79**			**1,12**			**16,09**			**5,42**
Mit5	mARO	A,B	0,30	**Mit20**	B,F	0,18	**Mit35**	B,F	0,18	**Mit 42**	G,I	0,05
	mSLE		10 710,00			134 210,00			68 960,00			117 000,00
	mALE		3 213,00			24 157,80			12 412,80			5 850,00
	Cost		1 332,00			1 157,00			1 157,00			3 376,00
	ROSI		**3,41**			**12,92**			**18,07**			**5,19**
Mit6	mARO	A,D	0,30	**Mit21**	B,I	0,20	**Mit36**	G	0,10			
	mSLE		10 710,00			117 960,00			68 960,00			
	mALE		3 213,00			23 592,00			6 896,00			
	Cost		1 431,00			3 157,00			1 076,00			
	ROSI		**3,10**			**4,28**			**24,64**			
Mit7	mARO	A,F	0,35	**Mit22**	D,I	0,15	**Mit37**	B, G	0,10			
	mSLE		10 710,00			117 960,00			68 960,00			
	mALE		3 748,50			17 694,00			6 896,00			
	Cost		1 135,00			3 256,00			1 573,00			
	ROSI		**3,70**			**5,93**			**16,54**			

Appendix 4/5 – The Results of mARO, mSLE, mALE and ROSI with Different Security Risk Treatment Options Calculated Separately for Each Risk

Alternative		**Control**	**Risk 1**		**Control**	**Risk 2**		**Control**	**Risk 3**		**Control**	**Risk 4**
Mit8	mARO	A,B,D	0,20	**Mit23**	B,D,I	0,10						
	mSLE		10 710,00			117 960,00						
	mALE		2 142,00			11 796,00						
	Cost		2 168,00			3 753,00						
	ROSI		**2,20**			**6,59**						
Mit9	mARO	A,B,F	0,25	**Mit24**	B,F,I	0,18						
	mSLE		22 710,00			117 960,00						
	mALE		5 677,50			21 232,80						
	Cost		1 872,00			3 457,00						
	ROSI		**0,82**			**4,50**						
Mit 10	mARO	G	0,10	**Mit25**	G	0,05						
	mSLE		22 710,00			134 210,00						
	mALE		2 271,00			6 710,50						
	Cost		1 076,00			1 076,00						
	ROSI		**5,33**			**30,18**						
Mit 11	mARO	A,G	0,10	**Mit26**	B,D	0,10						
	mSLE		10 710,00			134 210,00						
	mALE		1 071,00			13 421,00						
	Cost		1 551,00			1 453,00						
	ROSI		**4,17**			**17,47**						

Appendix 5/5 – The Results of mARO, mSLE, mALE and ROSI with Different Security Risk Treatment Options Calculated Separately for Each Risk

Alternative		Control	Risk 1		Control	Risk 2	Control	Risk 3	Control	Risk 4
Mit 12	mARO	A, B, G	0,10	**Mit27**	B,G	0,05				
	mSLE		10 710,00			134 210,00				
	mALE		1 071,00			6 710,50				
	Cost		2 288,00			1 573,00				
	ROSI		**2,50**			**20,33**				
Mit 13	mARO	B, D	0,20	**Mit28**	F,I	0,28				
	mSLE		22 710,00			117 960,00				
	mALE		4 542,00			33 028,80				
	Cost		1 453,00			2 600,00				
	ROSI		**2,13**			**1,78**				
Mit 14	mARO	B, F	0,25	**Mit29**	G,I	0,05				
	mSLE		22 710,00			117 960,00				
	mALE		5 677,50			5 898,00				
	Cost		1 157,00			3 376,00				
	ROSI		**1,94**			**9,18**				
Mit 15	mARO	B,G	0,10	**Mit30**	B, G, I	0,05				
	mSLE		22 710,00			117 960,00				
	mALE		2 271,00			5 898,00				
	Cost		1 573,00			3 873,00				
	ROSI		**3,33**			**7,87**				

Appendix 6/7 – The Results of mARO, mSLE, mALE and RORPI

Risk:	**1**	**2**	**3**	**4**	**ALE Total**		
ARO	0,40	0,30	0,50	0,20			
SLE	22 710,00	134 210,00	68 960,00	133 730,00			
ALE	9 084,00	40 263,00	34 480,00	26 746,00	**110 573,00**		

Mit Alt.	**Controls**		**Risk1**	**Risk2**	**Risk3**	**Risk4**	**mALE Total**	**Cost**	**RORPI**
1	D	mARO	0,30	0,15	0,30	0,05			
		mSLE	22 710,00	134 210,00	68 960,00	133 730,00			
		mALE	6 813,00	20 131,50	20 688,00	6 686,50	**54 319,00**	956,00	**57,84**
2	G	mARO	0,10	0,05	0,10	0,05			
		mSLE	22 710,00	134 210,00	68 960,00	133 730,00			
		mALE	2 271,00	6 710,50	6 896,00	6 686,50	**22 564,00**	1 076,00	**80,79**
3	A	mARO	0,30	0,15	0,30	0,05			
	D	mSLE	10 710,00	134 210,00	68 960,00	133 730,00			
		mALE	3 213,00	20 131,50	20 688,00	6 686,50	**50 719,00**	1 431,00	**40,83**
4	A	mARO	0,10	0,05	0,10	0,05			
	G	mSLE	10 710,00	134 210,00	68 960,00	133 730,00			
		mALE	1 071,00	6 710,50	6 896,00	6 686,50	**21 364,00**	1 551,00	**56,52**
5	B	mARO	0,20	0,10	0,14	0,05			
	D	mSLE	22 710,00	134 210,00	68 960,00	133 730,00			
		mALE	4 542,00	13 421,00	9 654,40	6 686,50	**34 303,90**	1 453,00	**51,49**
6	B	mARO	0,10	0,05	0,10	0,05			
	G	mSLE	22 710,00	134 210,00	68 960,00	133 730,00			
		mALE	2 271,00	6 710,50	6 896,00	6 686,50	**22 564,00**	1 573,00	**54,95**
7	B	mARO	0,30	0,20	0,35	0,20			
	I	mSLE	22 710,00	134 210,00	68 960,00	117 000,00			
		mALE	6 813,00	26 842,00	24 136,00	23 400,00	**81 191,00**	3 157,00	**8,31**
8	D	mARO	0,30	0,15	0,30	0,05			
	I	mSLE	22 710,00	117 960,00	68 960,00	117 000,00			
		mALE	6 813,00	17 694,00	20 688,00	5 850,00	**51 045,00**	3 256,00	**17,28**
9	F	mARO	0,35	0,28	0,40	0,20			
	I	mSLE	22 710,00	117 960,00	68 960,00	117 000,00			
		mALE	7 948,50	33 028,80	27 584,00	23 400,00	**91 961,30**	2 600,00	**6,16**

Appendix 7/7 – The Results of mARO, mSLE, mALE and RORPI

Mit Alt.	Controls		Risk1	Risk2	Risk3	Risk4	mALE Total	Cost	RORPI
10	G	mARO	0,10	0,05	0,10	0,05			
	I	mSLE	22 710,00	117 960,00	68 960,00	117 000,00			
		mALE	2 271,00	5 898,00	6 896,00	5 850,00	**20 915,00**	3 376,00	**25,56**
11	A	mARO	0,20	0,10	0,14	0,05			
	B	mSLE	10 710,00	134 210,00	68 960,00	133 730,00			
	D	mALE	2 142,00	13 421,00	9 654,40	6 686,50	**31 903,90**	1 928,00	**39,80**
12	A	mARO	0,10	0,05	0,10	0,05			
	B	mSLE	10 710,00	134 210,00	68 960,00	133 730,00			
	G	mALE	1 071,00	6 710,50	6 896,00	6 686,50	**21 364,00**	2 288,00	**37,99**
13	A	mARO	0,35	0,28	0,40	0,20			
	F	mSLE	10 710,00	117 960,00	68 960,00	117 000,00			
	I	mALE	3 748,50	33 028,80	27 584,00	23 400,00	**87 761,30**	3 435,00	**5,64**
14	A	mARO	0,10	0,05	0,10	0,05			
	G	mSLE	10 710,00	117 960,00	68 960,00	117 000,00			
	I	mALE	1 071,00	5 898,00	6 896,00	5 850,00	**19 715,00**	3 851,00	**22,59**
15	B	mARO	0,20	0,10	0,14	0,05			
	D	mSLE	22 710,00	117 960,00	68 960,00	117 000,00			
	I	mALE	4 542,00	11 796,00	9 654,40	5 850,00	**31 842,40**	3 753,00	**19,98**
16	B	mARO	0,25	0,18	0,18	0,20			
	F	mSLE	22 710,00	117 960,00	68 960,00	117 000,00			
	I	mALE	5 677,50	21 232,80	12 412,80	23 400,00	**62 723,10**	3 457,00	**12,84**
17	B	mARO	0,10	0,05	0,10	0,05			
	G	mSLE	22 710,00	117 960,00	68 960,00	117 000,00			
	I	mALE	2 271,00	5 898,00	6 896,00	5 850,00	**20 915,00**	3 873,00	**22,15**
18	A	mARO	0,20	0,10	0,14	0,05			
	B	mSLE	10 710,00	117 960,00	68 960,00	117 000,00			
	D	mALE	2 142,00	11 796,00	9 654,40	5 850,00	**29 442,40**	4 668,00	**16,38**
	I								
19	A	mARO	0,25	0,10	0,14	0,05			
	B	mSLE	22 710,00	117 960,00	68 960,00	117 000,00			
	F	mALE	5 677,50	11 796,00	9 654,40	5 850,00	**32 977,90**	4 372,00	**16,75**
	I								
20	A	mARO	0,10	0,05	0,10	0,05			
	B	mSLE	10 710,00	117 960,00	68 960,00	117 000,00			
	G	mALE	1 071,00	5 898,00	6 896,00	5 850,00	**19 715,00**	4 788,00	**17,98**
	I								