To invest or not to invest?

Assessing the economic viability of a policy and security configuration management tool

Lukas Demetz and Daniel Bachlechner
Department of Information Systems
School of Management
University of Innsbruck, Austria
{firstname.lastname}@uibk.ac.at

Abstract. The threat of information security breaches is omnipresent. Large organizations such as Sony or Lockheed Martin were recently attacked and lost confidential customer information. Besides targeted attacks, virus and malware infections, lost or stolen laptops and mobile devices, or the abuse of the organizational IT through employees, to name but a few, also put the security of assets in jeopardy. To defend against information security threats, organizations invest in security countermeasures preventing, or, at least, reducing the probability and the impact of information security breaches. As information security budgets are constrained and the number of assets to be protected is large, information security investments need to be deliberately evaluated. Several approaches for the evaluation of information security investments are presented in literature. In this article, we identify, compare, and evaluate such approaches using the example of a policy and security configuration management tool. Such a tool is expected to reduce costs of organizational policy and security configuration management and to increase the trustworthiness of organizations. It was found that none of the analyzed approaches can be used without reservation for the assessment of the economic viability of the policy and security configuration management tool used as an example. We see, however, considerable potential for new approaches for the evaluation of information security investments in combining different elements of existing approaches.

Keywords: economics of information security, information security investments, policy and security configuration management

1 Introduction

The perils of information security breaches are ubiquitous. In 2011, large companies were subject to attacks and information security breaches were discussed in public: Personal data including credit card information of 25 million Sony users were compromised [24]; Citigroup and Honda Canada suffered breaches exposing information of 200,000 [24] and 280,000 customers [11], respectively; RSA's SecureID authentication was at risk after an attack [12] leading to breaches, for instance, at Lockheed Martin [39], to name but a few. Besides attacks, there are also other sources of information security breaches. Other reasons that urge organizations to invest in information security include, among others, virus and malware infections, unavailability of critical systems, lost or stolen laptops and mobile devices, and abuse of IT systems by employees, human errors, and forces of nature [14, 29, 44]. Deloitte's 2011 global security study [15] reveals that the majority of 138 large technology, media and telecommunications organizations from around the world experienced at least one information security breach in 2010. The question thus is not whether an organization will face a breach, but rather when the next breach will incur and which assets will be compromised [21]. Therefore, organizations invest in security countermeasures that prevent, or, at least, reduce the probability and the impact of breaches.

In times of constrained information security budgets and an increasing number of assets to be protected, organizations have to decide how much they should invest in information security in general, and how the information security budget should be allocated to specific security countermeasures [2, 20]. Each asset is associated with an information system that provides the asset or the asset is part of. An information system, in turn, usually has an inherent vulnerability which can be a flaw or weakness in the system that could be exploited, for instance, by an attacker. A vulnerability, however, may also be exploited by technical defects of natural disasters. An attack is a deliberate assault on the security of a system. For each vulnerability, there exists a threat represented as the probability that the vulnerability is exploited. The expected losses expressed as the probability times the impact of a security breach is referred to as risk. To mitigate risks, an organization can deploy countermeasures [35]. As each threat is associated with a certain risk, not all threats should receive the same level of attention [3].

Information security investments, unlike other investments such as buildings or machines, do not generate monetary returns. Instead, their benefits result from cost savings by preventing or by reducing the probability or impact of security

breaches [e.g., 26, 34, 36, 38]. As all other investments, information security investments should be managed by analyzing the cost-benefit tradeoffs [8]. This is, however, aggravated as the benefits of an information security investment in its capability of safeguarding against identified and, more common, unknown threats have to be assessed [18]. As a result, assessing the benefits of information security investments is a challenging task [9]. Besides cost-benefits, information security investments can alternatively be managed with respect to their cost-effectiveness.

Organizations need to find a balance between the probabilities and impacts of information security threats and the possibilities to mitigate the risks through security investments [8]. Furthermore, the expenditures to secure an asset should correspond to the asset's value and the expected losses resulting from security breaches [21]. For instance, spending \$100 on a lock securing a certain asset worth \$50 would not be economically viable. Mizzi [32, pp. 19] defines the economic viability of an information security investment as

$$E_S < L_T \text{ or } (F + B + M) < (L_T + A(t) + r(t))$$

where E_S represents security expenditures, L_T total annual losses, F annual costs to fix the vulnerability by applying system patches and updates, B one-time costs to implement security countermeasures, M annual maintenance costs, L_I instantaneous losses, $A(t)$ availability losses, and $r(t)$ a function describing the annual costs to rebuild lost assets. That is, an information security investment is economically viable if and only if the security expenditures are smaller than the total annual losses. Accordingly, Huang et al. [26] argue that for a risk-averse decision maker expenditures for information security investments increase with, however, never exceed the expected losses associated with information security threats. Furthermore, they argue that the optimal investment is zero as long as the expected losses resulting from an information security breach are under a certain threshold. Gordon and Loeb [22] argue that the optimal amount to invest in information security should never exceed 37% of the expected losses of an information security breach. Willemson [45], however, shows that by relaxing some of Gordon and Loeb's [22] requirements, expenditures of nearly 100% of the expected losses can be reasonable. The maximum amount to invest in information security is where there is no difference in costs upfront and the expected losses of an information security threat [26].

For deciding whether to invest in a specific information security countermeasure, literature provides a myriad of approaches that support such decisions. Albeit having the same objectives, these approaches differ with respect to their foundation. For instance, there are approaches based on real options [e.g., 21, 25], game theory [e.g., 4, 10], or accounting figures such as return on investment [e.g., 6, 28]. Among the most frequently cited approaches is the one presented by Gordon and Loeb [22] for which also some extensions have been proposed [e.g., 31, 46]. The approaches, however, do not only differ in their foundation, they also have different assumptions. For instance, risk neutral decision makers [e.g., 10, 42], risk averse decision makers [e.g., 26], single threats to assets [22], or breaches resulting in predictable outcomes and variances [7].

The aim of this article is to identify approaches presented in literature that support decision making with respect to information security investments. More concretely, we identify approaches suitable for assessing the economic viability of a policy and security configuration management tool. Such a tool, helps, first, to reduce the costs associated with policy and security configuration management and, second, to increase the trustworthiness of an organization by establishing a transparent link between business policies and technical configurations. We compare selected approaches and evaluate them with respect to their suitability for assessing the economic viability of such a tool, and discuss their advantages and disadvantages for such a decision.

The remainder of this article is structured as follows: Section 2 describes the policy and security configuration management tool which will be the subject of the investment decision. Based on the tool's characteristics, we derive requirements for suitable approaches supporting information security investment decision making. Section 3 is devoted to the research methods used to collect and analyze suitable approaches. We present the results of our analysis in section 4, where we describe the identified approaches. In section 5, we discuss the approaches with respect to their suitability for assessing the economic viability of a tool supporting policy and security and configuration management and highlight commonalities and differences of the approaches. Finally, section 6 concludes this article and gives a short outlook on possible future work.

2 Policy and Security Configuration Management

Today, organizations are confronted with an increasing number of regulatory and contractual requirements, they need to comply with. As a result, they have

to increase their expenditures on activities ensuring compliance [19, 33]. Depending on their industry sector, different regulations and laws are posed on organizations, for instance, Basel II and Sarbanes-Oxley in the finance sector, or the Health Insurance Portability and Accountability Act for health-related organizations in the US.

This situation is particularly exacerbated in the case of service providers offering services to customers. As most service providers serve multiple customers, they face a myriad of contractual requirements they have to comply with. Currently, policy and security configuration management is mainly done manually, which is often inefficient, usually cost-intensive, and generally error prone [16]. Management costs, including costs for policy and security configuration management, were steadily rising over the last years [17].

For dealing with this myriad of regulatory and contractual requirements, organizations in general and service providers in particular need a tool that supports them in policy and security configuration management. Such a tool establishes and maintains a consistent and transparent link between high-level security and compliance requirements at one end and low-level technical configurations on the other. This end-to-end link is maintained automatically, where possible, and, in case human interaction is necessary, the tool offers decision support. As a result, the tool achieves two distinct goals: reducing costs (e.g., management costs and losses due to information security breaches) and increasing an organization's trustworthiness by increasing its security and compliance. Both goals are achieved by partially of fully automatizing processes, such as detecting misconfigurations or checking whether two security controls are equivalent with respect to the provided security level, performance and costs. Additionally, the end-to-end link between security and compliance requirements and configurations eases audit processes as the information necessary for audits can be provided automatically by the tool. Thus, audits can be performed in shorter time which, in turn, allows auditors to increase the scope of an audit or the sample size.

The policy and security configuration management tool offers two different modes of operation. The first is a static mode which is run in a plan and build phase. Here, the tool is used to initially establish the end-to-end link between security and compliance requirements and configurations. Put simply, the tool checks if all requirements are met by the current configuration of the IT landscape. The second mode is a dynamic one. In this mode, configurations are

constantly monitored for deviations from the ideal configuration. Such an automated monitoring allows organizations to detect misconfigurations quicker and thus to reduce the risk of information security breaches or of problems caused by non-compliance. As the tool's functions are tightly coupled, we assume that the tool is shipped as a whole, that is, there is no functionality which can be bought at a later point in time.

Ideally, the tool is run not only at one organization, but also at its suppliers and customers. This way, each involved party can easily and efficiently share information about requirements and configurations via the tool. This way, each party is able to assess the fulfillment of requirements at its suppliers and to also assess whether customer requirements can be fulfilled. Operating this policy and security configuration management tool across several parties increases the tool's benefits for all parties involved in such organizational networks. Additionally, auditors also benefit if an organization's suppliers use the tool, as they can access necessary information more easily.

Such a policy and security configuration management tool certainly has its advantages - it saves time and costs and, at the same time, increases trustworthiness. Simply investing in such a tool without deliberately assessing its economic viability would, however, be quite naïve. Therefore, a decision to invest must be well supported, for instance, by applying an appropriate investment approach. As stated above, literature provides a myriad of investment approaches, all based on different foundations and assumptions. Based on the policy and security configuration management tool's characteristics and its application in cross-organizational settings, we can derive a set of requirements an approach supporting investment decision making should cover. While some requirements are mandatory, others are optional but desirable. The requirements are:

- *The approach must support investment decisions regarding security products bought as a whole.* The policy and security configuration management tool is bought as a whole; there are no features of the tool that can be bought at a later point in time. That is, the decision to buy the policy and security configuration management tool is a one time decision made at a certain point in time without deferment options.
- *The approach must consider financial measures.* The tool aims at reducing costs for policy and security configuration management. Therefore, financial measures must be considered. Financial measures are particularly important

for an organization's upper management as they are predominantly interested in financial measures when making decisions.

- *The approach should consider non-financial measures.* Besides reduced costs, the policy and security configuration management tool aims to increase trustworthiness of an organization measured in terms of the level of security and compliance. Neither increased trustworthiness nor the level of security and compliance can be easily expressed in financial measures. Nevertheless, they should be considered for supporting decision making.
- *The approach must support one-time costs and benefits.* The policy and security configuration management tool is applied in a plan and build phase. Here, costs (e.g., costs of setting up the tool or a new project) incur immediately and play a crucial role in the decision making.
- *The approach should support running costs and benefits.* The policy and security configuration management tool is additionally operated in a running mode. In this mode, costs (e.g., maintenance or monitoring costs) and benefits (e.g., reduced costs to identify misconfigurations) incur over time and should be taken into consideration.
- *The approach must be applicable without explicitly considering attacks.* Some approaches rely on the provision of information on a particular attack. Even though attacks are a major cause of information security breaches, the tool's primary focus is on policy and security configuration management and thus assuring compliance with various requirements. Thus, attacks are not the primary concern and approaches should be applicable without considering information on attacks.
- *The approach should consider network effects of the investment.* Organizations, possibly service providers themselves, consume services from their suppliers. The more of an organization's suppliers use the policy and security configuration management tool, the higher will be the tool's benefit for each involved party as information can be shared more easily between them.

We chose the policy and security configuration management tool because of the tool's broad relevance for organizations in general and service providers in particular, our insight into the unique characteristics resulting from prior research, and the usefulness of the results for the funding research project. Assessing the economic viability of another tool would certainly lead to other requirements to be fulfilled by investment approaches and in consequence to other suitable approaches.

3 Method

The analysis of investment approaches is based on a set of scientific articles. We collected articles describing approaches supporting decision making regarding information security investments. In this section, we describe the methods used to collect relevant articles and to select suitable approaches for a detailed analysis. Afterwards, the method used for the detailed analysis of the selected approaches is outlined.

3.1 Collection of approaches

We collected approaches to be included in the analysis in a three-step process consisting of, first, an unsystematic search to identify appropriate keywords, second, a systematic keyword using the set of keywords, and, third, a filtering based on the requirements presented in the previous section. In the following, each of the steps will be explained in more detail.

We started collecting approaches with an unsystematic search using Google Scholar. In this step, we identified 30 relevant articles discussing information security investments. We extracted the describing keywords, unified them to more general terms, grouped and ranked them with respect to their frequency of appearance.

Subsequently, we used the two most frequent keywords - *economics of security* and *security investment* - for a systematic search, again using Google Scholar. For both keywords, we looked for peer reviewed articles with matching title and abstract in the first 200 search results and added them to the collection of articles. Since the term *security* has different connotations in other domains (for instance, in finance, a security is a tradable document showing ownership of stocks, bonds, and other investments) and for the sake of completeness, we additionally queried Google Scholar with variations of the term. More concretely, we replaced the term *security* with *information security, computer security* and *IT security* in the two keywords *economics of security* and *security investment*. Search queries using these variations, however, did not result in any further articles. Additionally, as suggested by [43], we examined the references in the articles. If found, we added relevant articles to our collection. The entire collection process resulted in 83 articles dealing with information security investments.

In the next step, we discarded those articles that do not focus on approaches for supporting information security investment decision making. For instance,

articles dealing with empiric analyses of information security investments [e.g., 23, 30] were discarded. Furthermore, we excluded articles presenting approaches to determine the cost-effectiveness of investments, that is, approaches that help to optimally allocate a fixed budget. Additionally, the approaches have to offer decision support whether to invest in a certain information security product. Articles that present an overview of several approaches [e.g., 36, 40] were discarded. Instead, the articles originally presenting the approach were added to our collection, if not yet present. Extensions to existing approaches (e.g., [31] extends [22]) were treated as individual approaches. Investment approaches tailored to a specific technology incomparable to the policy and security configuration management tool were not considered. Cavusoglu et al. [10], for instance, present an approach dedicated to determine the value of intrusion detection systems and was thus not considered for a detailed analysis. In case an approach was described in several articles by the same author(s), newer publications were favored over older and journal articles over conference articles. Here, we made sure that the newer articles did not extend the older ones. In case of extensions, both articles were treated separately. After this filtering, 11 approaches, each described in an individual article, were considered for a detailed analysis. Table 1 gives an overview of the approaches analyzed in detail.

3.2 Analysis of approaches

The 11 articles we collected and filtered according to the above approach were then analyzed in detail. For each approach, the respective article was read carefully. While reading, information regarding the requirements presented in section 2 was marked and extracted. To identify relevant information, we particularly looked at the descriptions of the approaches' procedures of supporting investment decisions. The requirement whether the investment is made as a whole was assessed by looking for hints in the approach's description whether the investment can be split into smaller investments. For information regarding financial and non-financial measures, we looked primarily at the approaches' input and output parameters. There, we analyzed whether they solely represent financial measures, or also non-financial ones. We proceeded similarly to determine whether one time and running costs and benefits are considered in the approach. Additionally, we looked at the calculations and analyzed whether running costs and benefits are present and accounted for. We are fully aware that running costs and benefits can be treated as one-time costs and benefits, for in-

stance, by discounting them using the net present value (NPV) method. For this requirement, however, we looked whether an approach directly takes running costs and benefits into account. This would render the approach more flexible with respect to running costs and benefits. Additionally, this way, running costs and benefits could be accounted for more precisely. For determining whether the approach can be applied without considering information on attacks and whether network effects of the investment are considered, we once again looked at the approaches' procedures in the respective articles.

4 Results

In the following, we present the analyzed approaches. For each approach, we first present a short description of the approach and then show its fulfillment of the requirements. Table 1 lists the analyzed approaches and the degree to which they fulfill the requirements presented in section 2. Each requirement is represented by a dedicated column. For the degree of fulfillment, a checkmark (✓) indicates that a requirement is met completely, whereas a tilde (∼) indicates that a requirement is met partially. An empty cell denotes that a requirement is not met or nothing is mentioned in the respective article. In the column labelled "Attacks", a ✓indicates that an approach does not rely on information on attacks.

All articles presenting the approaches were published after 2000, the oldest being published in 2002 and the latest in 2011. With respect to publication outlets, no peculiarities could be identified. Seven approaches were presented in journal articles including general information systems journals (e.g., Information Systems Research to journals) as well as journals with an information security focus (e.g., ACM Transactions on Information and Systems Security). The remaining four approaches were published in conference proceedings. Even though some approaches are proposed by the same authors [e.g., 21, 22], all analyzed approaches are completely independent of each other.

In the following, we present the 11 approaches collected using the procedure described in section 3.1. For each article, we first present a general description and then describe its suitability to support information security investment decision making with respect to the policy and security configuration management tool.

Table 1. Overview of analyzed approaches for information security investment decisions

Approach presented in	**Bought as a whole**	**Financial**	**Non-financial**	**one-time costs**	**Running costs**	**Attacks**	**Network effects**
Gordon and Loeb [22]	✓	✓		✓		✓	
Mizzi [32]	✓	✓		✓	∼	∼	
Al-Humaigani and Dunn [1]	✓	✓		✓		✓	
Sonnenreich et al. [37]	✓	✓		✓		✓	
Cremonini and Martini [13]	✓	✓		✓			
Huang et al. [26]	✓	✓		✓		✓	
Tallau et al. [38]	✓	✓	✓	✓	∼	✓	∼
Wang et al. [41]	✓	✓		✓		✓	
Gordon et al. [21]	✓	✓		✓		✓	
Bodin et al. [5]	✓	✓	✓	✓	∼	✓	∼
Butler [7]	✓	✓	✓	✓		✓	

4.1 Approach by Gordon and Loeb

In Gordon and Loeb [22] the authors present an approach for determining the optimal amount to invest to protect a single asset. For this, the authors assume a risk-neutral decision maker and a one-period model (i.e., all decisions and outcomes occur instantaneously). Each asset is associated with monetary losses λ in case a breach occurs, a threat probability t and an inherent vulnerability v denoting the probability that without additional security, a realized threat is successful. The expected losses L associated with an asset represent the product of the threat probability t and the monetary losses λ and are calculated as $L = t \times \lambda$. To reduce the vulnerability v of an asset, an organization invests $z > 0$ monetary units. In this respect, $S(z, v)$ represents a security breach probability function denoting the probability that the asset with vulnerability v is compromised given the investment z to secure the asset.

The expected benefit from an investment z in information security $EBIS(z)$ is calculated as

$$EBIS(z) = [v - S(z, v)]L;$$

the expected net benefit $ENBIS(z)$ reads

$$ENBIS(z) = [v - S(z, v)]L - z.$$

Gordon and Loeb argue that an investment z should not exceed the point where the marginal benefits equal marginal costs, thus determining an upper bound for investments. The optimal amount z^* to invest in information security is reached if the difference between marginal benefits and costs is maximized. This optimal amount is, however, at most 38% of the expected losses without the investment, and is in most cases considerably smaller.

To assess the approach's suitability for supporting information security investment decisions regarding the policy and security configuration management tool, we focus on the set of requirements derived from the tool's characteristics and use. Gordon and Loeb consider a one-period model. This means, among others, that all decisions occur instantaneously. Thus, the investment is cannot split into several smaller investments and is made as a whole. This fulfills the respective requirement. For supporting investment decisions, the approach focuses on financial measures and probabilities of threats, yet leaving out non-financial measures. As a consequence of the assumed one-period model, outcomes incur also instantaneously. Thus, time value of money is not considered. Because of this, the considered financial measures are one-time costs and benefits; running

costs and benefits cannot be taken into account. As the approach bases the decision support on monetary losses, the vulnerability of an asset and the probability a threat is realized, the approach is applicable without taking the information on attacks into account. Network effects are not taken into consideration.

To sum up, the approach presented by Gordon and Loeb is suitable for investments made as a whole, considers financial measures and probabilities as inputs, and does not rely on information on an attack or an attacker. The approach does not consider non-financial measures, running costs and benefits, and network effects.

4.2 Approach by Mizzi

Mizzi [32] presents an approach for information security investment decisions based on accounting figures. In his approach, Mizzi focuses solely on financial measures including the annual costs F to fix a vulnerability, the one-time costs B to implement a security countermeasure, and the annual maintenance costs M. The decision to invest in an information security countermeasure is simply a matter of comparing the costs of the total annual information security expenditures E_S with the expected total annual losses L_T of a given security vulnerability. More concretely, an investment should be made, if the expenditures are lower than the expected total annual losses, that is,

$$E_S < L_T,$$

where E_S is calculated as

$$E_S = F + B + M$$

in the first year and as

$$E_S = F + M$$

in subsequent years. L_T can be calculated in several ways: One way is to account for the instantaneous losses L_I and the losses of asset I over t days of unavailability, that is

$$L_T = L_I + I * t/365;$$

the availability losses over t days may also be modeled as a function $A(t)$ making the total annual losses equal to

$$L_T = L_I + A(t);$$

additionally, the costs R to rebuild a compromised asset can also be taken into consideration, either as

$$L_T = L_I + A(t) + R$$

in case the rebuild costs do not include man-hour costs, or as

$$L_T = L_I + A(t) + R(t)$$

if man-hour costs are the dominant rebuild costs.

If the approach is used as described by Mizzi, it does not consider costs and benefits that incur over the course of time discounted to the present point in time. Mizzi, however, notes that one could additionally use NPV or IRR to better account for running costs. In contrast to other approaches presented, Mizzi additionally presents an extension to his approach in which the costs to break a security countermeasures CTB for an attacker can be considered. This way, the efforts needed by an attacker to break a security countermeasure can be taken into account. In all calculations, however, this approach does neither take probabilities of information security breaches nor the success rate of information security countermeasures into consideration.

When assessing the approach's suitability to support information security investment decisions, we note that the investment is treated as one single investment. The decision making is supported based on financial measures, however, not including non-financial ones. The approach considers both one-time costs as well as running costs. Running costs incurring in latter periods, are, however, not discounted. Mizzi notes that for considering running costs, NPV or IRR may be used. In the approach's extension, an attacker's costs are taken into consideration. The approach, however, is applicable without this extension. Network effects of the investment are not taken into account.

To sum up, the approach presented by Mizzi meets the requirements with respect to investments made as a whole, financial measures and one-time costs and benefits. It partially fulfills the requirements regarding running costs and attacks. The approach neither considers non-financial measures nor network effects.

4.3 Approach by Al-Humaigani and Dunn

A rather simple approach to information security investment is presented by Al-Humaigani and Dunn [1]. They argue that the maximum return of an information security investment is reached when the total costs of security, including

losses due to information security breaches and costs of information security countermeasures, is minimal. For this, Al-Humaigani and Dunn use measures representing costs to invest and costs incurring if not invested in information security.

In their approach, Al-Humaigani and Dunn calculate the return on security investment based solely on financial measures. In their calculations, they, however, use financial measures for non-financial aspects, for instance, losses in reputation and goodwill. Al-Humaigani and Dunn determine the return on security investment (ROSI) using the following equation:

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

where T is the threat or risk the security investment is intended for; C_{T1} denotes costs of procuring the security countermeasures, C_{T2} costs of additional hardware and facilities, C_{T3} costs of training, C_{T4} losses due to limitations placed on business, C_{T5} costs of adopting a secured-by-design strategy, C_{T6} costs to recover from an information security breach, C_{T7} losses due to business interruption, C_{T8} losses in human casualties, C_{T9} losses in data from business and legal aspects, C_{T10} losses in reputation and goodwill, C_{T11} the amount paid by the insurance, K_T the probability of the realization of the security threat without the information security investment.

To determine the approach's suitability to assess the economic viability of the policy and security configuration management tool, we again look at the requirements derived in section 2. The approach by Al-Humaigani and Dunn treats the investment as a single investment, not considering cases in which the investment is split up. Thus, the approach meets the first requirements. The decision support is solely based on financial measures. Financial measures are important as an organization's management is mostly interested in such measures. Non-financial measures (e.g., an organization's trustworthiness), however, also provide useful information about the investment and should thus not be left out of consideration. The financial measures consist of one-time costs only, which incur as soon as the investment is made. The policy and configuration management tool, however, is also operated in a dynamic mode in which running costs and benefits incur over time. By not taking running costs and benefits into account, the approach does not meet the respective requirement and neglects important information about the investment. Furthermore, the approach does not rely on information on attacks, thus it meets the respective requirement.

Network effects are not considered in the approach. As the tool is applied in a network of organizations, the tool's network effects increase the benefits for all parties within the network.

To sum up, the approach presented by Al-Humaigani and Dunn is suitable for investments made as a whole, considers financial measures that incur once, and does not rely on information on attacks. The approach, however, does not take non-financial measures, network effects, and running costs and benefits into account.

4.4 Approach by Sonnenreich et al.

Sonnenreich et al. [37] propose an approach similar to the traditional accounting figure return on investment (ROI) termed return on security investment $ROSI$. In contrast to other approaches, Sonnenreich et al. do not divide the costs used for the calculation further into different types of costs. For supporting investment decisions, they calculate $ROSI$ as

$$ROSI = \frac{(risk\ exposure * risk\ mitigated) - solution\ costs}{solution\ costs},$$

where

$$risk\ exposure = ALE = SLE \times ARO;$$

ALE denotes the annual loss exposure, that is, the single loss expose SLE times the annual rate of occurrence ARO of an information security breach that the security investment should mitigate.

Looking at the requirements to assess the approach's suitability for supporting information security investment decisions, the approach by Sonnenreich et al. regards the investment as a whole that cannot be split into smaller investments. For supporting investment decisions, however, only financial measures are taken into consideration; non-financial ones are left out. Thus, the requirement regarding financial measures met, the one regarding non-financial measures is not met. The costs and benefits incur once. Even though Sonnenreich et al. mention NPV and IRR for discounting running costs incurring at a later point in time, they are not taken into account. As the approach does not rely on information on attacks, the approach is applicable without considering attacks and thus meets the respective requirement. Finally, network effect are not used for supporting investment decisions. As a consequence, useful information about the investment is neglected and the respective requirement is not met.

To sum up, the approach presented by Sonnenreich et al. is suitable for investments made as a whole, and meets the requirements with respect to financial measures and one-time costs and benefits. Furthermore, it does not rely on information on attacks and is thus applicable without considering attacks. The approach cannot be used to take non-financial measures or running costs into consideration, and it disregards network effects of the investment.

4.5 Approach by Cremonini and Martini

Cremonini and Martini [13] discuss an approach to information security investment decision making similar to the one of Sonnenreich et al. They also use a ROI based approach using the annual loss expectancy ALE. Additionally, they couple the ROI with a measure representing the convenience of attacks termed return on attack ROA. This allows to compare alternatives from an attacker's point of view and to choose the alternative with the highest disadvantage from an attacker's point of view.

Cremonini and Martini define the ROI as

$$ROI = \frac{ALE_{beforeS} - ALE_{afterS}}{costs\ of\ security\ measure\ S},$$

where $ALE_{beforeS}$ and ALE_{afterS}, respectively, denote the annual costs related to all information security incidents that security countermeasure S is destined to mitigate, before and after S was implemented. The ROA, on the other hand, is equal to

$$ROA = \frac{gain\ from\ successful\ attack}{costs\ before\ S + losses\ caused\ by\ S}.$$

The costs associated with ROA are the costs faced by an attacker willing to breach a system. Again, as with other approaches, no qualitative measures are taken into account.

Looking at the requirements derived from the tool's characteristics, we can determine the approach's suitability to assess the tool's economic viability. The approach by Cremonini and Martini assumes that the investment is made as a whole that has no additional features to be purchased later on. This way, the approach clearly meets the respective requirement. Looking at the requirements of financial and non-financial measures, the approach only considers the former, and leaves out the latter. As a consequence, the approach neglects useful information that may be helpful for making investment decisions. The costs and losses in the calculations incur only once, meeting the respective requirement;

the requirement regarding running costs and benefits that incur in the tool's dynamic mode of operation over time is not met. The approach strongly relies on information on attacks. If such information is not available, the approach is hardly applicable. Thus, the respective requirement is not met. Network effects of the investment are neglected, again not meeting the respective requirement.

To sum up, the approach presented by Cremonini and Martini is suitable for investments made as a whole. Additionally, the approach takes financial measures incurring once as inputs. However, it relies on information on attacks. The approach does not account for non-financial measures, running costs and benefits, and network effects.

4.6 Approach by Huang et al.

Huang et al. [26] present an approach for determining the optimal amount to invest in information security based on the investment's expected utility. As in the approach presented by Gordon and Loeb [22], in this approach, the level of investment also depends on the asset to be protected, its vulnerability, and the associated potential losses. In their approach, Huang et al. assume a single-event, single-period security breach of an asset. A breach is associated probability function ρ and potential losses L including direct monetary and indirect losses resulting from, for instance, bad reputation or liability. ρ is a function of the threat probability t external to the organization and determined by the attractiveness of the asset; the vulnerability v of the asset is determined by the configuration of the information system providing the asset; and the investment S in information security countermeasures to protect the asset. That is,

$$\rho = \rho(S, v, t).$$

The expected losses due to an information security breach is denoted by X with

$$X = \begin{cases} L, \rho, \\ 0, (1 - \rho) \end{cases}$$

For calculating the optimal amount to invest, Huang et al. assume that with increasing investment S the breach probability ρ decreases, and that the marginal improvement on security decreases with a higher investment S. They further assume a risk-averse decision maker, whose aim is to maximize the expected utility u, determined by the organization's wealth w. That is, $u = u(w)$. For

determining the optimal amount to invest, the expected utility of the investment, written as

$$E[u(w - S - X)] = \rho u(w - S - L) + (1 - \rho)u(w - S)$$

needs to be maximized. To do so, the equitation needs to be differentiated with respect to S and set equal to zero. Besides determining the optimal amount to invest, the approach by Huang et al. can also be used to calculate the upper bound of investments (i.e., the maximum amount to invest). Even for a risk-averse decision maker, the maximum amount to invest should never exceed the expected losses of a potential information security breach.

For assessing the approach's suitability for supporting information security investment decisions based on the example of the policy and security configuration management tool, we note that the approach by Huang et al. assumes that the investment is made as a whole, not considering cases in which it is partitioned into smaller parts. This way, the approach meets the respective requirement. For supporting investment decisions, the approach uses financial measures, which are especially important for an organization's management. Non-financial measures, however, are left out of consideration. The financial measures consider one-time costs, thus meeting the respective requirement. Running costs and benefits that incur in the tool's dynamic mode of operation are neglected. As a consequence, the approach does not fulfill the respective requirement. The approach by Huang et al. does not rely on information on attacks. This allows to apply the approach without considering attacks, which is a requirement the approach should meet. Network effects of the investment are not taken into account by the approach, thus not meeting the respective requirement.

To sum up, the approach presented by Huang et al. is suitable for investments made as a whole, considers one time financial measures as inputs, and does not rely on information on attacks. The approach does not meet the requirements regarding non-financial measures, running costs and benefits, and network effects.

4.7 Approach by Tallau et al.

Another approach to information security investment decision making is presented by Tallau et al. [38]. In contrast to the other analyzed approaches, Tallau et al. base their approach on the Balanced Scorecard proposed by Kaplan and Norton [27]. In general, the Balanced Scorecard is a performance measurement

system that does not only consider financial measures, but also non-financial ones related to internal processes, customers, and innovation and learning. The Balanced Scorecard allows to view business from four different angles, thus providing a balanced view of an organization's performance.

As in the original Balanced Scorecard, Tallau et al. use the four perspectives *financial, customer, internal processes,* and *innovation and learning* for deciding whether to invest. For each perspective, goals and measures for the investment are established. For instance, the authors use "Reduce hacks/intrusions in past year by 90%" as a goal and "Server down time (in hours)" as a measure in their exemplary application [38, p. 47]. Additionally, each goal is weighted indicating the importance relative to the other goals. Next, the degree to which each goal is fulfilled is determined, the goals are weighted and the average of all weigthed degrees of fulfillment is calculated. If this approach is applied in a non-comparative way (i.e., only one investment is evaluted), a minimum average degree of fullfilment of the goals can be set. If the investment's average degree is above the threshold, an investment is considered to be economically viable. If the approach by Tallau et al. is used in a comparative analysis (i.e., several investements are compared with each other), the investment yielding the highest average degree is recommended.

For assessing the approach's suitability to assess the policy and security configuration management tool's economic viability, we use the requirements presented in section 2. The approach by Tallau et al. assumes investments as a whole, thus meeting the respective requirement. The decision support is based on both financial and non-financial measures, such as customer satisfaction or increased trustworthiness. This way, the approach presents a balanced view of the investment. Both respective requirements are fulfilled. As measures used within the decision support can be chosen freely by the decision maker, one-time costs as well as running costs may be taken into account. The same holds true for measures regarding attacks and network effects. That is, the approach can be applied without considering attacks and measures with respect to network effects can be chosen.

To sum up, the approach presented by Tallau et al. is suitable for investments made as a whole. It completely meets the requirements with respect to financial and non-financial measures, and one-time costs. Additionally, it partially fulfills the requirements regarding running costs and network effects and does not rely on information on attacks.

4.8 Approach by Wang et al.

Wang et al. [41] present an approach supporting information security investment decisions based on value-at-risk (VaR), a tool originally developed for the assessment of the risk associated with financial assets. With their approach, Wang et al. are able to measure the risk of daily losses and, by using extreme value analysis, to assess the value at risk.

VaR denotes the upper limit for daily losses L caused by an information security breach. The information security breach exceeds VaR with probability p. In other words, with a proper information security investment the probability that the daily losses L exceeds VaR is p. That is,

$$p = Pr[L \geq VaR] = 1 - Pr[L \leq VaR].$$

The daily losses L at a given investment level I is

$$L = \sum_{j=1}^{T} n_j C_j(I),$$

where j is the type of information security incident, n_j is the number of occurrences of incident type j, and C_j denotes the costs caused by an incident of type j. Both n_j and C_j assume that the information security investment is in place. In case the approach by Wang et al. [41] is applied in a non-comparative way (i.e., only one investment alternative is evaluated), VaR and the expected daily costs of the investment, consisting of the average daily losses and daily solution costs, are compared with the current situation. In case the approach is applied in a comparative analysis, for each alternative, VaR and expected daily costs are calculated. Then, the decision maker can choose either of the alternatives (or the current status) based on his level of risk aversion. That is, the decision maker chooses an alternatives based on whether he or she strives to decrease the expected daily costs or VaR.

For assessing the approach's suitability for information security investment decisions regarding the policy and security configuration management tool, we note that the VaR based approach by Wang et al. [41] assumes information security investments to be made as a whole, neglecting cases in which the investment is split into smaller parts. This way, the approach meets the respective requirement. For supporting investment decisions, the approach uses financial measures and thus fulfills the requirement accordingly. Non-financial measures, however, are not considered in the approach. Thus, the respective requirement

is not met and useful information of the investment is left out of consideration. The financial measures incur once, therefore meeting the requirement with respect to one-time costs and benefits. Running costs and benefits incurring over time in the tool's dynamic mode of operation, however, are not taken into consideration. The approach does not rely on information on attacks and is thus applicable without considering attacks. This way, the approach meets the respective requirement. In contrast, the requirement regarding network effects is not met, as the approach uses no measures associated with the tool's network effects.

To sum up, the approach presented by Wang et al. is suitable for investments made as a whole, and takes one time financial measures into consideration. It does, however, not take non-financial, running costs and benefits, and network effects of the investment into account. The approach can be applied without having information on attacks.

4.9 Approach by Gordon et al.

Gordon et al. [21] present a wait-and-see approach based on real options. The basic idea of their approach is that in case of uncertainty with respect to expected benefits, it may be better to wait for key events to occur as often higher expected benefits can be yielded this way. Thus, before investing in information security, it may be advisable to wait for an information security breach to happen. As soon as a breach occurs, more information to assess the expected benefits of an information security investment is available, thus making the assessment more accurate. They argue that because of this deferment option, several information security breaches can be explained.

Gordon et al. state that in order to make the investment, the NPV of the investment made today must be greater than the NPV of the deferred investment. Determining the costs and benefits of an information security investment before a breach occurs is, however, uncertain. For instance, Gordon et al. [21, pp. 3-4] provide an example of an organization about to make an investment of \$1.000.000 in information security for one year. The benefits of this investment, are, however, uncertain. Either, the benefits are \$40.000 or \$200.000 per month, both being equally probable. Then, the expected value of this investment is equal to $(\$12 * 40.000 * 0.5) + (12 * \$200.000 * 0.5) - \$1.000.000 = \$440.000$. They assume that one month later an information security breach occurs and the benefits of the investment become known. Now, we are able to determine the expected

value for both savings: In case of the lower benefits, the expected value of the investment is $EV_{low} = 11 * \$40.000 - \$1.000.000 = -\$560.000$, which is negative and the investment should not be made. When looking at the higher benefits, the expected value yields $EV_{high} = 11 * \$200.000 - \$1.000.000 = \$1.200.000$ and should be taken. This example illustrates, how the expected value of an information security investment increases from \$440.000 to $\$1.200.000 * 0.5 = \$600.000$ by deferring the decision to invest by one month.

When assessing the approach's suitability to assess the economic viability of the policy and security configuration management tool, we note that even though the approach by Gordon et al. considers that the decision to invest can be deferred, the authors assumes that the investment is made as a whole meeting the respective requirement. The decision making is supported by taking financial measures into account. This way, the approach meets the requirement regarding financial measures. Non-financial measures, which provide useful information on the investment, are, however, neglected. one-time costs are taken into account by the approach; running costs and benefits that incur in the tool's dynamic mode are, in contrast, left out of consideration, not meeting the respective requirement. For supporting information security investment decisions, the approach does not rely on information about attacks making it possible to apply the approach without considering attacks. The approach thereby meets the respective requirement. Network effects are left out of consideration by the approach, thus not fulfilling the requirement regarding network effects.

To sum up, the approach presented by Gordon et al. is suitable for investments made as a whole, considers one time financial measures as inputs, and does not rely on information on attacks. The approach leaves out non-financial measures and network effects; running costs and benefits cannot be taken into account.

4.10 Approach by Bodin et al.

Bodin et al. [5] present an approach based on the analytic hierarchy process (AHP). The AHP uses besides financial measures also non-financial measures for analyzing multi-criteria decision problems. The approach by Bodin et al. is predominantly used in comparative analyses, where several alternatives are compared with each other.

The first step of this approach is to determine criteria and sub-criteria, along with intensity levels denoting the level of fulfillment (e.g., high or very high) for

each of them. According to these criteria and sub-criteria, information security investments will be evaluated and compared. Following, weights $C(i, j)$ for a pairwise comparison are assigned to the criteria, sub-criteria and intensity levels. The larger a weight $C(i, j)$ is, the more preferred is element i over j. In the next step, each alternative is evaluated with respect to the criteria and sub-criteria and the respective intensity levels are recorded. Finally, for each alternative, the weights of all criteria and sub-criteria are added up resulting in the alternative's total score. This can then be compared and the alternative yielding the highest total score is recommended.

Looking at the requirements to assess the approach's suitability to assess the policy and security configuration management tool's economic viability, the approach assumes the investment to be made as a whole, meeting the requirement accordingly. For supporting information security investment decisions, the approach takes financial as well as non-financial measures, which can both be chosen freely by the decision maker, into consideration. This way, the approach fulfills both respective requirements. As the measures for evaluation can be chosen freely, measures for one-time costs and running costs can be selected. In the same way, measures with respect to network effects can be chosen for the decision support.

To sum up, the approach presented by Bodin et al. is suitable for investments made as a whole. It fully meets the requirements with respect to financial and non-financial measures, and one-time costs. Additionally, it partially takes running costs and benefits and network effects into account and does not rely on information on attacks.

4.11 Approach by Butler

The last approach analyzed is a comparative approach described by Butler [7] called Security Attribute Evaluation Method (SAEM). This approach is a quantitative cost-benefit analysis for information security investment decisions involving four steps. For the initial data collection, structured interviews with IT and security managers are conducted.

The first step of the analysis is a security technology benefit assessment. In this step, several investment alternatives are collected and their benefits are assessed. A benefit can be either achieved by preventing a breach or by reducing a breach's consequences. Subsequently, each alternative is evaluated with respect to its capability to mitigate information security risks. This means that

an alternative's effectiveness in reducing the probability and/or the impact of an information security breach is assessed. These estimations are done by security managers who rate the effectiveness based on their working experience. In the following step, a security architecture coverage assessment is conducted. Here, each alternative is assessed with respect to the breadth of security risks the alternative covers. In the final step, the costs of each alternative are compared with each other. To save time in decision making, the alternatives providing the highest benefit are compared first.

For assessing the approach's suitability for supporting information security investments, we use the requirements derived from the tool's characteristics. We note that in the approach presented by Butler the investment is treated as an undividable investment, which cannot be partitioned into smaller parts. Thus, the approach meets the respective requirement. Information security investment decisions are supported by the use of financial as well as non-financial measures meeting this way the two respective requirements. The costs in the approach are regarded as one-time costs. Running costs are not considered. This way, important information on the investment is not taken into account and the approach does not meet the respective requirement. As the approach does not rely on information on attacks, the approach can be applied without considering attacks and thus fulfills the respective requirement. Network effects of the investment are not accounted for in the approach, therefore the approach does not meet the requirement regarding network effects.

To sum up, the approach presented by Butler is suitable for investments made as a whole. It considers one time financial measures and non-financial measures. However, it leaves out running costs and benefits as well as network effects. For supporting investment decisions, the approach does not rely on information on attacks.

5 Discussion

In this section, we discuss the results of the analysis of approaches supporting investment decisions with respect to the policy and security configuration management tool. More concretely, we highlight the degree to which the analyzed approaches fulfill the requirements we derived from the tool's characteristics and its application in cross-organizational settings. Furthermore, we highlight commonalities and differences of the approaches and discuss their suitability to support the assessment of the tool's economic viability.

In the following, we start with a general discussion of the approaches. Then, for each requirement the degree to which it is fulfilled by the analyzed approaches is discussed in a dedicated paragraph. Additionally, we present the consequences that result from the fulfillment or non-fulfillment of the requirement. At the end of this section, we summarize the suitability of each approach to support investment decisions with respect to the policy and security configuration management tool. Finally, we address the two approaches that at least partially fulfill all requirements in more detail.

The analyzed approaches can be divided into comparative and non-comparative approaches. The approaches by Bodin et al. [5], Butler [7], Tallau et al. [38], and Wang et al. [41] are intended for comparative analyses. In comparative analyses several alternative investments are compared to each other with respect to financial and non-financial measures. Comparative approaches may become problematic in case only one investment needs to be evaluated. In such cases, the investment can be compared to the current situation without the investment being made. Alternatively, as, for instance, proposed by Tallau et al. [38], the approach is applied to evaluate only the single investment. For being economically viable, the investment must reach a certain threshold, say 80%, of an overall score. The problem in this case, however, is to determine this threshold. Compartive approaches compare alternative investments and help to determine which alternative should be favored. The problem, however, is that they do not necessarily say whether an investment is economically viable. For instance, the approaches say that investment A should be favored over investment B, but they do not say whether, for instance, a positive return can be expected from the investment. The seven other approaches are non-comparative approaches. Such approaches can be used to evaluate a single investment. That is, these approaches yield one result based on which the investment decision can be made. When comparing several alternative investments using a non-comparative approach, only the results of the approach, for instance, the $ROSI$ of each alternative, is compared.

When we compare the type of assistance provided by the approaches, we see that the approaches by Gordon and Loeb [22], Huang et al. [26], and Wang et al. [42] help to calculate the optimal amount a risk-neutral and risk-averse decision maker, respectively, should invest. Furthermore, they can be used to determine the maximal amount to invest. Gordon and Loeb [22], for instance, state that one should not invest more than 37% of the expected losses. The ap-

proaches, however, do not say whether one should make a certain investment. Nevertheless, we can assume that if the costs of an investment are between the optimal and maximal expenditure, the investment should be made, the nearer to the optimal amount the better. Similarly, the approach by Wang et al. [41] does not say whether an investment should be made. The approach compares alternatives with respect to the investments' costs and the VaR of expected losses. It is then up to the decision maker to choose an investment based on his or her risk preference, which may be either to take a higher risk regarding the VaR and lower investment costs, or vice versa. The three approaches by Bodin et al. [5], Butler [7], and Tallau et al. [38] give an overview of alternative investments and show which investment should be favored over the alternative investments. The decision to make an investment depends again on the decision maker. The approaches by Al-Humaigani and Dunn [1], Cremonini and Martini [13], and Mizzi [32], based on accounting figures, provide as the result the return to be expected from the investment. In case the return is positive, an investment can be made as its benefits are higher than its costs and is thus economically viable; in case the return is negative, the investment should be neglected, because the investment costs are higher than the expected benefits; in case the investment equals zero, it is up to the decision maker to make the investment or not. The same thinking applies to the approach by Gordon et al. [21], except that the approach additonally takes a deferrement of the investment decision into account.

All analyzed approaches for supporting information security investment decisions assume that the investment is made as a whole. That is, the investment is not split into smaller parts (e.g., based on functionality), where the decision to invest in some parts may be deferred and made at a later point in time. This requirement is important as the policy and security configuration management tool is provided as a whole and not split into several smaller parts with functionality to be bought at a later point in time.

For supporting investment decisions, all identified approaches use financial measures. This is important as an organization's upper management is especially interested in financial measures such as the return to be expected from an investment.

Investments, however, do not only have financial benefits. The policy and security configuration management tool, for instance, aims at increasing an organization's trustworthiness, which can hardly be expressed in financial mea-

sures. Therefore, non-financial measure should not be neglected as they provide additional important information about an investment. Three of the identified approaches support non-financial measures: The approach by Tallau et al. [38] provides, based on the Balanced Scorecard, besides a financial perspective, three other perspectives (i.e., customer, internal processes, and innovation and learning) that are considered for the decision support. The approach by Butler [7] allows the decision maker to freely choose the measures that will be used to evaluate the investment. The approach by Bodin et al. [5] does not allow such a freedom in selecting measures, but assesses, for instance, an investment's security architecture coverage. Tallau et al. [38] state, however, that finding appropriate measures for evaluating investments is difficult and time consuming and depends on the one responsible for selecting the measures. Allowing the decision maker to freely chose the measures that will be used in the decision support, however, may bear some disadvantages. For instance, relationships between measures may hardly be described. Furthermore, it may also be difficult to formalize the measures so that they can be used for the evaluation of investments.

All approaches take one-time costs and benefits into account. This is important as one-time costs, for instance, for buying and deploying the policy and security configuration management tool, incur in any case. Therefore they need to be taken into account.

Running costs and benefits, in contrast, are not directly considered by any approach. The approach presented by Mizzi [32] gives formulas for costs incurring after the first year, however, does not discount them. Because in the approaches described by Bodin et al. [5] and Tallau et al. [38] the measures can be chosen freely, respective measures may be selected. Considering running costs is important, as the policy and configuration management tool is operated in a dynamic mode. In this mode, costs and benefits do not incur immediately, but over time. Therefore, running costs and benefits should not be neglected.

Only two of the analyzed approaches directly consider attacks; the other nine do not consider attacks directly. The first one is the approach described by Mizzi [32] in which an extension considering attacks is presented. The extension takes the attacker's cost to break a countermeasure into consideration. The approach, however, can be applied without the extension. The second one is the approach described by Cremonini and Martini [13] which uses the attacker's return on an attack in the decision support. The policy and security configuration management tool's primary purpose is to manage policies and security configurations,

that is, to ensure that an organization is compliant with all applicable laws and regulations. Considering attacks and an attacker's costs for breaching a system is thus not necessary and can therefore be neglected. It is thus important that the approach can be applied without considering attacks.

As expected, none of the analyzed approaches directly considers network effects of investments. The approaches by Bodin et al. [5] and Tallau et al. [38] allow the decision maker to freely choose measures to be used in the approach. Therefore, measures focusing on the investment's network effects may be selected and thus taken into consideration. This way, network effects can be taken into account. The more of an organization's service providers also use the policy and security configuration management tool, the higher will be the overall benefit for all involved parties. This is because information about compliance and security requirements can be easily exchanged between the involved parties via the tool. Thus, taking the tool's network effects into account is important as the network effects substantially influence the benefits of the tool.

In summary, the approach for supporting information security investment decisions presented by Cremonini and Martini [13] is the least suitable of the analyzed approaches. The approach fulfills three requirements (i.e., the tool is bought as a whole, financial measures and one-time costs and benefits) neglecting, however, important requirements such as non-financial measures and running costs and benefits. The approaches presented by Al-Humaigani and Dunn [1], Gordon et al. [21], Gordon and Loeb [22], Huang et al. [26], Sonnenreich et al. [37], and Wang et al. [41] fulfill only four of the requirements (i.e., the tool is bought as a whole, financial measures, one-time costs and benefits, and applicability without considering attacks). They are, thus only partially suitable to assess the economic viability of the policy and security configuration management tool, as useful information on the investment is not considered for the investment decision support. The approach described by Mizzi [32] meets three requirements (i.e., the investment is made as a whole, financial measures, and one-time costs and benefits), and partially fulfills two requirement with respect to running costs and benefits and, attacks. The approach presented by Butler [7] is a comparative approach that meets five out of the seven requirements but not the requirements with respect to running costs and network effects. Only the approaches by Bodin et al. [5] and Tallau et al. [38] at least partially fulfill all requirements. They are, nevertheless, both not completely suitable for supporting investment decisions regarding the example of the policy and security

configuration management tool. Both approaches are used in comparative analyses where several investment alternatives are evaluated and compared to each other. Furthermore, the two approaches do neither determine the return to be expected from the investment nor the optimal amount to invest given the asset's value and vulnerability. To do so, the approaches presented by Bodin et al. [5] and the one presented by Tallau et al. [38] could be combined with one of the other approaches to have on the one hand an evaluation with respect to financial and non-financial measures, and on the other hand to determine the return of the investment or the optimal amount to invest.

6 Conclusion

In this article, we identified, analyzed and presented a set of approaches for supporting information security investment decisions. Additionally, we evaluated and compared them with respect to their suitability for assessing the economic viability of a policy and configuration management tool. This tool helps organizations in general and service providers in particular to deal with the myriad of regulatory and contractual requirements they need to comply with. The tool aims at reducing the costs for the management of policies and security configurations and at increasing the level of security and compliance of organizations. For evaluating and comparing the approaches' suitability to support investment decisions regarding the tool, we derived from the tools functionality and usage in cross-organizational settings several requirements. The approaches should allow that the investment is made as a whole, consider financial and non-financial measures, take one time and running costs and benefits into consideration, be applicable without considering attacks, take network effects of the investment into account.

The findings show that there is no approach that is completely suitable. There are approaches, such as the ones presented by Bodin et al. [5] and Tallau et al. [38], respectively, that fulfill most of the requirements. They, however, are intended for comparative analyses and cannot be easily used to assess the economic viability of a single investment. It may be that a combination of two or more approaches that complement each other can be used together. Finding compatible approaches and determining their fit is, however, left to future work. As we focused in this article on a policy and security configuration management tool, the results are specific to the characteristics of this tool. Using another tool as an example would most certainly have led to other results.

One limitation of this article is that we focused on investment approaches that help to assess the economic viability of a certain investment. This means that it is assumes that sufficient money is available to make the investment. In practice, however, security budgets are not inexhaustible. The objective then is to determine how to best spend this budget with respect to well-defined objectives and thus to determine the cost-effectiveness of investments.

Acknowledgments

The research leading to these results was partially funded by the European Union 7th Framework Programme (FP7) through the PoSecCo project (project no. 257129).

References

[1] Al-Humaigani M. and Dunn D. B. A model of return on investment for information systems security. In *Proceedings of the 46th IEEE International Midwest Symposium on Circuits & Systems, Vols 1-3*, pp. 483–485, 2003.

[2] Anderson R. and Schneier B. Guest Editors' Introduction: Economics of Information Security. *IEEE Security & Privacy*, 3(1):12–13, 2005. doi: 10.1109/MSP.2005.14.

[3] Bagchi K. and Udo G. An analysis of the growth of computer and Internet security breaches. *Communications of the Association for Information Systems*, 12:684–700, 2003. URL: `http://aisel.aisnet.org/cais/vol12/iss1/46/`.

[4] Böhme R. and Moore T. The Iterated Weakest Link - A Model of Adaptive Security Investment. In *Proceedings of the 8th Workshop on the Economics of Information Security (WEIS 2009)*, London, England, 2009.

[5] Bodin L. D., Gordon L. A., and Loeb M. P. Evaluating information security investments using the analytic hierarchy process. *Communications of the ACM*, 48(2):78–83, 2005. doi: 10.1145/1042091.1042094.

[6] Bojanc R. and Jerman-Blažič B. Towards a standard approach for quantifying an ICT security investment. *Computer Standards & Interfaces*, 30 (4):216–222, 2008. doi: 10.1016/j.csi.2007.10.013.

[7] Butler S. A. Security attribute evaluation method: a cost-benefit approach. In *Proceedings of the 24th International Conference on Software Engineering*, pp. 232–240, Orlando, Florida, 2002. ACM. doi: 10.1145/581339.581370.

[8] Cavusoglu H., Cavusoglu H., and Raghunathan S. Economics of IT security management: Four improvements to current security practices. *Communications of the AIS*, 14:65–75, 2004.

[9] Cavusoglu H., Mishra B., and Raghunathan S. A model for evaluating IT security investments. *Communications of the ACM*, 47(7):87–92, 2004. doi: 10.1145/1005817.1005828.

[10] Cavusoglu H., Mishra B., and Raghunathan S. The Value of Intrusion Detection Systems in Information Technology Security Architecture. *Information Systems Research*, 16(1):28–46, Mar. 2005. URL: `http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=17004376&site=ehost-live`.

[11] Computerworld . Honda Canada breach exposed data on 280,000 individuals. Website, 2011. URL: `http://www.computerworld.com/s/article/9217094/Update_Honda_Canada_breach_exposed_data_on_280_000_individuals`. Last access: Februrary, 1st 2012.

[12] Computerworld . RSA warns SecurID customers after company is hacked. Website, 2011. URL: `http://www.computerworld.com/s/article/9214757/RSA_warns_SecurID_customers_after_company_is_hacked`. Last access: February, 1st 2012.

[13] Cremonini M. and Martini P. Evaluating Information Security Investments from Attackers Perspective: the Return-On-Attack (ROA). In *Proceedings of the 4th Workshop on the Economics of Information Security (WEIS 2005)*, 2005.

[14] CSI Computer Survey . 14th Annual CSI Computer Crime and Security Survey, 2009.

[15] Deloitte . Raising the Bar 2011 TMT Global Security Study – Key Findings, 2011. URL: `http://www.deloitte.com/assets/Dcom-Global/Local%20Assets/Documents/TMT/dttl_TMT%202011%20Global%20Security%20Survey_High%20res_191111.pdf`.

[16] Forrester Research . How To Manage Your Information Security Policy Framework, 2006.

[17] Forrester Research . The Change And Configuration Management Software Market, 2007.

[18] Franqueira V., Houmb S., and Daneva M. Using Real Option Thinking to Improve Decision Making in Security Investment. In Meersman R., Dillon T., and Herrero P., editors, *On the Move to Meaningful Internet Systems*, volume 6426 of *Lecture Notes in Computer Science*, pp. 619–638.

Springer Berlin / Heidelberg, 2010. URL: http://dx.doi.org/10.1007/978-3-642-16934-2_46.

[19] Ghose A. and Koliadis G. Auditing Business Process Compliance: Service-Oriented Computing – ICSOC 2007. In Krämer B., Lin K.-J., and Narasimhan P., editors, *Lecture Notes in Computer Science*, volume 4749, pp. 169–180. Springer Berlin / Heidelberg, 2007. URL: http://dx.doi.org/10.1007/978-3-540-74974-5_14.

[20] Gordon L. and Loeb M. Economic aspects of information security: An emerging field of research. *Information Systems Frontiers*, 8(5):335–337, 2006. URL: http://dx.doi.org/10.1007/s10796-006-9010-7.

[21] Gordon L., Loeb M., and Lucyshyn W. Information security expenditures and real options: A wait-and-see approach. *Computer Security Journal*, 19 (2):1–7, 2003.

[22] Gordon L. A. and Loeb M. P. The economics of information security investment. *ACM Transactions on Information and System Security*, 5(4): 438–457, 2002. doi: 10.1145/581271.581274.

[23] Gordon L. A. and Loeb M. P. Budgeting Process for INFORMATION SECURITY EXPENDITURES. *Communications of the ACM*, 49(1):121–125, Jan. 2006. URL: http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=19349580&site=ehost-live.

[24] Guardian T. Sony suffers second data breach with theft of 25m more user details. Website, 2011. URL: http://www.guardian.co.uk/technology/blog/2011/may/03/sony-data-breach-online-entertainment. Last access: February, 1st, 2012.

[25] Herath H. S. B. and Herath T. C. Investments in Information Security: A Real Options Perspective with Bayesian Postaudit. *Journal of Management Information Systems*, 25(3):337–375, 2008. doi: 10.2753/MIS0742-1222250310.

[26] Huang C. D., Hu Q., and Behara R. S. An economic analysis of the optimal information security investment in the case of a risk-averse firm. *International Journal of Production Economics*, 114(2):793–804, 2008. doi: 10.1016/j.ijpe.2008.04.002.

[27] Kaplan R. S. and Norton D. P. The Balanced Scorecard–Measures That Drive Performance. *Harvard Business Review*, 70(1):71–79, Jan. 1992. URL: http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=9205181862&site=ehost-live.

[28] Kim S. and Lee H. Cost-Benefit Analysis of Security Investments: Methodology and Case Study. In Gervasi O., Gavrilova M., Kumar V., Laganà A., Lee H., Mun Y., Taniar D., and Tan C., editors, *Proceedings of the International Conference on Computational Science and Its Applications (ICCSA 2005)*, volume 3482 of *Lecture Notes in Computer Science*, pp. 305–315, Berlin / Heidelberg, 2005. Springer. URL: `http://dx.doi.org/10.1007/11424857_132`.

[29] Liginlal D., Sim I., and Khansa L. How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *Computers & Security*, 28(3–4):215–228, 2009. doi: 10.1016/j.cose.2008.11.003. URL: `http://www.sciencedirect.com/science/article/pii/S0167404808001181`.

[30] Liu W., Tanaka H., and Matsuura K. Empirical-analysis methodology for information-security investment and its application to reliable survey of Japanese firms. *Information and Media Technologies*, 3(2):464–478, 2008.

[31] Matsuura K. Productivity Space of Information Security in an Extension of the Gordon-Loeb's Investment Model. In *Proceedings of the 7th Workshop on the Economics of Information Security (WEIS 2008)*, 2008.

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

[33] Sadiq S., Governatori G., and Namiri K. Modeling Control Objectives for Business Process Compliance: Business Process Management. In Alonso G., Dadam P., and Rosemann M., editors, *Lecture Notes in Computer Science*, volume 4714, pp. 149–164. Springer Berlin / Heidelberg, 2007. URL: `http://dx.doi.org/10.1007/978-3-540-75183-0_12`.

[34] Schneier B. Security ROI. Website, 2008. URL: `http://www.schneier.com/blog/archives/2008/09/security_roi_1.html`. Last access: Februray 1st, 2012.

[35] Shirey R. Internet Security Glossary - RFC 2828. The Internet Engineering Task Force - Network Working Group, 2000. URL: `http://www.ietf.org/rfc/rfc2828.txt`.

[36] Sklavos N. and Souras P. Economic models and approaches in information security for computer networks. *International Journal of Network Security*, 2(1):14–20, 2006. URL: `http://ijns.femto.com.tw/download_paper.jsp?PaperID=IJNS-2005-07-08-1&PaperName=ijns-v2-n1/ijns-2006-v2-n1-p14-20.pdf`.

[37] Sonnenreich W., Albanese J., and Stout B. Return On Security Investment (ROSI) – A Practical Quantitative Modell. *Journal of Research and Practice in Information Technology*, 38(1):55–66, 2006. URL: http://www.jrpit.acs.org.au/jrpit/JRPITVolumes/JRPIT38/JRPIT38.1.45.pdf.

[38] Tallau L. J., Gupta M., and Sharman R. Information security investment decisions: evaluating the Balanced Scorecard method. *International Journal of Business Information Systems*, 5(1):34–57, Jan. 2010. doi: http://dx.doi.org/10.1504/IJBIS.2010.029479. URL: http://inderscience.metapress.com/content/v2t235805210k143/fulltext.pdf.

[39] The Wall Street Journal . Lockheed Martin Hit By Security Breach. Website, 2011. URL: http://online.wsj.com/article/SB10001424052702303654804576350083016866022.html. Last access: February, 1st 2012.

[40] Tsiakis T. K. and Pekos T. Analysing and determining Return on Investment for Information Security. In *Proceedings of the International Conference on Applied Economics (ICOAE)*, p. 879, 2008. URL: http://kastoria.teikoz.gr/icoae2/wordpress/wp-content/uploads/articles/2011/10/103-2008.pdf.

[41] Wang J., Chaudhury A., and Rao H. R. A value-at-risk approach to information security investment. *Information Systems Research*, 19(1):106–120, Mar. 2008. doi: 10.1287/isre.1070.0143.

[42] Wang S.-L., Chen J.-D., Stirpe P., and Hong T.-P. Risk-neutral evaluation of information security investment on data centers. *Journal of Intelligent Information Systems*, 36(3):329–345, 2011. URL: http://dx.doi.org/10.1007/s10844-009-0109-4.

[43] Webster J. and Watson R. T. Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*, 26(2):xiii–xxiii, June 2002. URL: http://www.jstor.org/stable/4132319.

[44] Whitman M. E. Enemy at the gate: threats to information security. *Communications of the ACM*, 46(8):91–95, 2003. doi: 10.1145/859670.859675.

[45] Willemson J. On the Gordon & Loeb Model for Information Security Investment. In *Proceedings of the 5th Workshop on the Economics of Information Security (WEIS 2006)*, 2006.

[46] Willemson J. Extending the Gordon and Loeb Model for Information Security Investment. In *Proceedings of the 5th International Conference on the Availability, Reliability, and Security (ARES '10)*, pp. 258–261, 2010. doi: 10.1109/ARES.2010.37.