Chapter 2
To Invest or Not to Invest? Assessing the Economic Viability of a Policy and Security Configuration Management Tool

Lukas Demetz and Daniel Bachlechner

Abstract The threat of information security (IS) 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 IS threats, organizations invest in IS countermeasures preventing, or, at least, reducing the probability and the impact of IS breaches. As IS budgets are constrained and the number of assets to be protected is large, IS investments need to be deliberately evaluated. Several approaches for the evaluation of IS investments are presented in the literature. In this chapter, 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 the 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 combining different elements of existing approaches.

2.1 Introduction

The perils of information security (IS) breaches are ubiquitous. In 2011, large companies were subject to attacks and IS breaches were discussed in public (e.g., [11, 12, 21]). Besides attacks, other reasons, for instance, virus and malware infections,

L. Demetz (✉) · D. Bachlechner
Department of Information Systems, School of Management, University of Innsbruck, Innsbruck, Austria
e-mail: lukas.demetz@uibk.ac.at; daniel.bachlechner@uibk.ac.at

R. Böhme (ed.), *The Economics of Information Security and Privacy*,
DOI 10.1007/978-3-642-39498-0_2, © Springer-Verlag Berlin Heidelberg 2013

lost or stolen mobile devices, human errors, and forces of nature [14, 15, 26, 43] urge organizations to invest in IS. The question today is not whether an organization will face an IS breach, but rather when a breach will occur [20]. As a result, organizations invest in countermeasures that prevent IS breaches or reduce their probability and impact.

Facing constrained budgets and an increasing number of assets to protect, organizations have to decide how much to invest in IS, and how to allocate the IS budget [2, 19]. As the probability of being exploited as well as the criticality differ from asset to asset, not all assets should receive the same level of attention [3].

Investments in IS, unlike other investments, do not generate monetary returns but result in cost savings by preventing IS breaches or by reducing the probability of their occurrence and their impact [23,32,34,37]. Analyzing the cost-benefit tradeoffs of alternative IS investments, however, is challenging [9], as not only the costs but also the benefits of IS investments with respect to known and unknown threats have to be assessed [16]. Organizations, however, need to pay attention to the economic viability of IS investments. They have to find the balance between the risks of threats on one side and the possibility to mitigate the risks and the costs thereof on the other side [8]. Mizzi [29, p. 19] defines an IS investment as economically viable if

$$E_S < L_T$$

where E_S represents security expenditures and L_T the total annual losses. That is, an IS investment is economically viable if and only if the security expenditures are smaller than the total annual losses. Mizzi [29], however, assumes that the security expenditures E_S aim to fix all vulnerabilities to assets at stake (i.e., to completely remove these vulnerabilities). Thus, security expenditures E_S, which include the costs to build IS countermeasures and the costs to fix vulnerabilities, clearly need to be lower than the sum of the losses expected from an IS breach of the vulnerabilities and the costs to repair breached assets. In the case of investments that only aim to fix a certain vulnerability (i.e., not all vulnerabilities) to an asset, the equation by Mizzi [29] does not hold. In such cases, the security expenditures need to be lower than the *reduction* of expected losses conditional the investment to fix the respective vulnerability. Similar to Mizzi, Huang et al. [23] argue that for risk-averse decision makers expenditures for IS investments increase with, however, never exceed the expected losses associated with IS threats. Gordon and Loeb [17] even argue that the optimal amount to invest in IS never exceeds 37 % of the expected losses associated with an IS breach. Willemson [44], however, shows that in some cases expenditures of nearly 100 % of the expected losses can be reasonable.

Fortunately, the literature provides a myriad of approaches (e.g., [6, 10, 20, 22]) that help decision makers in deciding whether or not to invest in a certain IS countermeasure. Among the most frequently cited approaches is the one presented by Gordon and Loeb [17] for which also several extensions have been proposed (e.g., [28, 45]).

In this chapter, we identify approaches which are suitable to assess the economic viability of a specific countermeasure, namely, 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 automating or providing decision support for critical activities related to policy and security configuration management. We describe and compare selected approaches, evaluate them with respect to their suitability for assessing the economic viability of such a tool based on a set of criteria, and discuss the approaches' advantages and disadvantages.

The remainder of this chapter is structured as follows: Sect. 2.2 introduces the policy and security configuration management tool which is the subject of the investment decision. Section 2.3 is devoted to the research methods used to collect and analyze data about approaches. We present the results of the analysis in Sect. 2.4, where we also outline the determining characteristics of the different approaches. In Sect. 2.5, we discuss the approaches with respect to their suitability for assessing the economic viability of the policy and security and configuration management tool, and highlight commonalities and differences of the approaches. Finally, Sect. 2.6 concludes this chapter and gives a short outlook on possible future work.

2.2 Policy and Security Configuration Management

Today, organizations are confronted with an increasing number of regulatory (e.g., SOX or PCI-DSS) and contractual requirements they need to comply with. As a result, they have to increase their expenditures on compliance activities [31]. This situation is particularly exacerbated for service providers offering services to clients as they are faced with a myriad of additional contractual requirements requested by their clients. Management costs, including costs for policy and security configuration management, steadily increased over recent years [25]. Currently, policy and security configuration management is mainly done manually, which often turns out to render related activities inefficient and error prone [30]. In this respect, a policy is a declarative description of an outcome. A security policy comprises rules that specify how security is established and maintained [33]. Each security policy is associated with at least one security configuration that describes imperatively how the respective goal is to be reached. While inefficiencies often lead to unnecessary high costs, a lack of trust is often the consequence of error-proneness. Disrespecting or ignoring security policies may be the causes for many IS breaches [39].

To deal with this myriad of requirements, organizations in general and service providers in particular could benefit from a tool supporting 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 of IT landscape components on the other. This end-to-end link is maintained automatically where possible, and, in case human interaction is necessary, decision support is offered. The aim of such a tool is two-fold: reducing costs (e.g., management costs and losses due to IS breaches) and increasing an organization's trustworthiness by increasing its level of security and compliance. Both goals may be achieved by partially or fully automating activities related to policy and security configuration management such as detecting misconfigurations or checking whether different security countermeasures are equivalent with respect to security level, performance and costs. Additionally, the tool would ease audits as the information necessary for audits can be provided directly by the tool.

The policy and security configuration management tool would support two different modes of operation. The first mode is a static mode, in which the end-to-end link between security and compliance requirements and configurations is planned and initially established. Additionally, the tool can be operated in a dynamic mode, in which 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 IS breaches or of problems caused by non-compliance. As the tool's functions would be tightly coupled, we assume that the tool is available only as a whole, that is, there are no modules which could be added at a later point in time.

Ideally, the tool is run not only at one organization, but also at its suppliers and clients. This way, each involved party could easily share information about requirements and configurations. As a result, each party is able to assess the fulfillment of requirements at its suppliers and to also assess whether certain requirements can be fulfilled by a supplier. Operating such a tool across several parties in a cross-organizational setting would increase the benefits of the tool for all parties involved.

Such a policy and security configuration management tool would certainly have its advantages. Nevertheless, the decision to invest in such a tool must be well justified, for instance, by applying an approach for assessing investment decisions found in the literature. Based on the policy and security configuration management tool's characteristics and its application in cross-organizational settings, we derive a set of mandatory and optional criteria a suitable approach must or should meet, respectively. The derived criteria are:

1. *The approach must be able to deal with investments made as a whole.* As we assume that the tool is only available as a whole and that there are no modules that could be added at a later point in time, a suitable approach must support decisions regarding investments made as a whole.
2. *The approach must be able to consider financial measures.* As the tool aims, among other things, at reducing the costs of policy and security configuration management, a suitable approach must support financial measures.
3. *The approach should be able to consider non-financial measures.* As the tool also aims at increasing the trustworthiness of an organization and since increased trustworthiness cannot be easily expressed in financial measures, a suitable approach should support non-financial measures.
4. *The approach must be able to support one-time costs and benefits.* As costs crucial for decision making incur immediately whenever the tool is used for planning and initially establishing the end-to-end-link between security and

compliance requirements and configurations, a suitable approach must support such one-time costs and benefits.

5. *The approach should be able to support running costs and benefits.* As the tool is also operated in a dynamic mode and since costs and benefits thus also incur over time, a suitable approach should support running costs and benefits.
6. *The approach must be applicable without explicitly considering attacks.* Some approaches rely on the provision of information on a particular attack. As the tool's primary focus is on policy and security configuration management and information on attacks is generally neither relevant nor available, a suitable approach must be applicable without considering attacks.
7. *The approach should be able to consider network effects of investments.* The more organizations are involved in a cross-organizational setting, the higher are the benefits of the tool for all parties involved. Thus, network effects should be supported by a suitable approach.

We chose a policy and security configuration management tool as the subject of the investment decision because of the tool's broad relevance for organizations in general and service providers in particular, and our insight into the unique characteristics of such a tool resulting from prior research. Assessing the economic viability of another IS investment would certainly lead to other criteria to be met by suitable approaches.

2.3 Data Collection and Analysis

In this section, we describe the methods used to collect relevant articles and to select approaches for assessing the economic viability of IS investments. Subsequently, the detailed analysis of the selected approaches is outlined.

2.3.1 Collection of Approaches

We started collecting approaches described in the literature with an unsystematic search using Google Scholar. In this step, we identified 30 relevant articles discussing IS investments. We extracted their keywords, combined them under more general terms, and ranked the terms with respect to their frequency of appearance.

Subsequently, we used the two most frequent terms – *economics of security* and *security investment* – for a systematic search, again using Google Scholar. For both terms, we looked for peer-reviewed articles with matching titles and abstracts within the first 200 search results and created a collection of articles. Since the term *security* has different connotations in other domains, and for the sake of completeness, we additionally queried Google Scholar with variations of the terms. More concretely, we replaced *security* with *information security*, *computer security* and *IT security* in both terms. Search queries using these variations, however, did not result in additional articles. Apart from that, as suggested by Webster and Watson [42], we examined the articles referenced by the already collected articles. The entire collection process resulted in 83 articles focusing on IS investments.

In the next step, we discarded articles that did not focus on approaches for supporting IS investment decision making. For instance, articles dealing with empirical analyses of IS investments (e.g., [18, 27]) were discarded. Furthermore, we excluded articles discussing approaches that help to optimally allocate a fixed budget. Additionally, articles that present an overview of several approaches (e.g., [34, 38]) were discarded. Substantial extensions to existing approaches (e.g., [28] extends [17]) were treated as individual approaches. Approaches tailored to specific countermeasures incomparable with the policy and security configuration management tool were removed. Cavusoglu et al. [10], for instance, present an approach to determine the value of intrusion detection systems and was thus not considered for detailed analysis. In case an approach was described in several articles by the same author or group of authors, newer publications were favored over older, and journal articles over articles in conference proceedings. We made sure that the newer articles did not only extend the older ones. In the case of extensions, both articles were treated separately. Eleven approaches for assessing IS investments, each described in an individual article, were finally considered for detailed analysis.

2.3.2 Analysis of Approaches

First, for each approach, the corresponding article was read carefully. While reading, information regarding the criteria introduced in Sect. 2.2 was marked and extracted. For the identification of relevant information, the descriptions of the approaches' procedures proved to be particularly valuable. For instance, 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 approaches.

2.4 Results

In the following, we present the analyzed approaches in alphabetical order. For each approach, we first give a short description of the approach and then show to what extent it meets the criteria presented in Sect. 2.2. Table 2.1 lists the analyzed approaches and the degree to which they meet the criteria. Each criterion is represented by a dedicated column. A checkmark (✓) indicates that a criterion

Table 2.1 Overview of the approaches for IS investment decisions analyzed in detail

Approach presented by	Made as a whole	Financial	Non-financial[a]	One-time costs	Running costs[a]	Attacks	Network effects[a]
Al-Humaigani and Dunn [1]	✓	✓		✓		✓	
Bodin et al. [4]	✓	✓	✓	✓	∼	✓	∼
Butler [7]	✓	✓	✓	✓		✓	
Cremonini and Martini [13]	✓	✓		✓			
Gordon and Loeb [17]	✓	✓		✓		✓	
Gordon et al. [20]	✓	✓		✓		✓	
Huang et al. [23]	✓	✓		✓		✓	
Mizzi [29]	✓	✓		✓	∼	∼	
Sonnenreich et al. [35]	✓	✓		✓		✓	
Tallau et al. [37]	✓	✓	✓	✓	∼	✓	∼
Wang et al. [40]	✓	✓		✓		✓	

✓ Criterion is met completely; ∼ Criterion is met partially

[a] Criterion is optional

is met completely, whereas a tilde (∼) indicates that a criterion is met partially. An empty cell denotes that a criterion is not met or nothing is mentioned in the respective article. In the column labeled "Attacks", a checkmark indicates that the corresponding approach does not rely on information on attacks. Columns marked with a letter "a" denote optional criteria.

In contrast to other surveys on approaches for the assessment of IS investments (e.g., [5, 36]), this chapter objective is not to present an overview of all approaches found in the literature. Rather, the objective of this chapter is to collect and analyze approaches that are suitable for determining the economic viability of a specific IS investment, namely, of a policy and security configuration management tool as presented in Sect. 2.2. As the total number of approaches presented in the literature would be too exhaustive for a detailed analysis, we reduced the number of approaches as described in Sect. 2.3. Accordingly, the approaches analyzed in detail (i.e., the results of this chapter) represent only a number of approaches found in literature. The analyzed approaches, however, are those considered most suitable for assessing the economic viability of the policy and security configuration management tool.

2.4.1 Approach of Al-Humaigani and Dunn

A rather simple approach for assessing IS investments is presented by Al-Humaigani and Dunn [1]. They argue that the maximum return of an IS investment is reached when the total costs of security, including losses due to IS breaches and costs of countermeasures, is minimal. Al-Humaigani and Dunn use measures representing expenditures for the investment and costs incurring if no investment is made.

In their approach, Al-Humaigani and Dunn calculate the return on investments based solely on financial measures. In their calculations, however, they 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:

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

where T is the threat or risk the IS investment is intended to address; C_{T1} denotes costs of procuring the 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 IS 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 and K_T the probability of the realization of the threat without the investment.

Just like all the other approaches investigated in detail, the approach proposed by Al-Humaigani and Dunn is not only able to deal with investments made as a whole but also to consider financial measures. With respect to financial measures, the approach incorporates 11 predefined costs to determine the $ROSI$. The approach is, however, not able to consider non-financial measures. While the approach supports one-time costs and benefits, it is not per se able to support running costs and benefits. However, running costs and benefits may be discounted to their present value and added to the one-time measures. The approach proposed by Al-Humaigani and Dunn is applicable without explicitly considering attacks. Like most of the other approaches, the approach is not per se able to consider network effects of investments. However, network effects may be taken into account by users of the approach when specifying the measures used. To sum up, the approach meets the four mandatory criteria but does not meet any of the optional ones.

2.4.2 Approach by Bodin et al.

Bodin et al. [4] 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 investment alternatives are compared with each other.

This approach starts with the determination of criteria and sub-criteria along with intensity levels denoting the level of fulfillment (e.g., high or very high). On the basis of these criteria and sub-criteria, IS investments are compared. Therefore, weights $C(i, j)$ for a pairwise comparison are assigned to the criteria, sub-criteria and intensity levels. The larger a weight $C(i, j)$, the more important is (sub-)criteria i over j. Then, each alternative is evaluated with respect to the criteria and sub-criteria. Simultaneously, the corresponding intensity levels are recorded. Finally, for each alternative, the weights of all criteria and sub-criteria are summed up resulting in the alternatives' total scores. The alternative yielding the highest total score is recommended.

Just as all other approaches analyzed, the approach presented by Bodin et al. is able to handle investments made as a whole. The approach allows the decision maker to choose the measures to be used for decision support. As such, the approach is able to support financial and non-financial measures as well as measures for one-time and running costs and benefits. The approach is applicable without explicitly considering attacks. Even though network effects are not proposed as measures, the approach is able to support measures for network effects of investments. To sum up, the approach meets all four mandatory criteria. Of the three optional criteria, two are met and one is partially met.

2.4.3 Approach by Butler

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

The first step of the analysis is an IS technology benefit assessment. In this step, several investment alternatives are collected and their benefits are assessed. Subsequently, each alternative is evaluated with respect to its capability to mitigate IS risks. That is, an alternative's effectiveness in reducing the probability and impact of an IS breach is assessed. These estimations are done by IS managers who rate the effectiveness based on their working experience. In the following step, an IS architecture coverage assessment is conducted. Here, each alternative is assessed with respect to the breadth of IS risks the alternative covers. In the final step, the costs of each alternative are compared with each other.

Similar to the other approaches we analyzed, the approach proposed by Butler is able to deal with investments that are made as a whole. The approach is able to support financial as well as non-financial measures. With respect to these measures, one-time costs and benefits are supported, while running costs and benefits are not per se supported. The approach is applicable without explicitly considering attacks. Just as most other approaches, the approach proposed by Butler does not per se support network effects of investments. These, however, may be considered while specifying the measures used. To sum up, the approach meets the four mandatory criteria and all but one of the optional ones.

2.4.4 Approach by Cremonini and Martini

Cremonini and Martini [13] discuss an approach to IS investment decision making which is similar to that of Sonnenreich et al. [35]. They also use a return on investment *(ROI)* based approach using the annual loss expectancy *ALE*. Additionally, they couple *ROI* with a measure referred to as return on attack *(ROA)* representing the convenience of attacks. *ROA* comprises costs faced by an attacker willing to breach a system. This allows us to compare alternatives from an attacker's point of view and to choose the alternative with the highest disadvantage for an attacker.

Cremonini and Martini define *ROI* as

$$ROI = \frac{ALE_{\text{before}S} - ALE_{\text{after}S}}{\text{costs of security measure } S},$$

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

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

The approach proposed by Cremonini and Martini is able to deal with investments made as a whole. The approach considers three financial measures to determine the *ROI*. Non-financial measures, however, are not taken into account by the approach proposed by Cremonini and Martini. While the approach is able to support one-time costs and benefits, running costs and benefits are per se not supported. Nevertheless, running costs and benefits may be discounted to their present value and considered in the determination of the *ROI*. Contrary to the other analyzed approaches, the approach proposed by Cremonini and Martini relies on information about attacks and is not easily applicable without such information. Similar to most other approaches investigated, also this approach does not account for network effects. To sum up, the approach meets three of four mandatory criteria and does not meet any of the optional ones.

2.4.5 Approach by Gordon and Loeb

Gordon and Loeb [17] present an approach for determining the optimal amount to invest to protect single assets. 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 an IS breach occurs, a threat probability t and an inherent vulnerability v denoting the probability that without additional security an attack 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 an IS 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 IS investment z $EBIS(z)$ is calculated as

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

the expected net benefit $ENBIS(z)$ reads

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

Just as all other approaches analyzed, also the approach proposed by Gordon and Loeb is able to deal with investments made as a whole as well as to consider financial measures. For determining the expected benefit of an IS investment, the approach takes two predefined costs coupled with probabilities into account. Non-financial measures, in contrast, are not considered by the approach. The approach is able to support one-time costs and benefits; running costs and benefits, however, are not per se supported. Running costs and benefits may, nevertheless, be discounted to their present value and considered within the determination of the expected benefits of the IS investment. The approach proposed by Gordon and Loeb is applicable without explicitly having information on attacks. Similar to most of the approaches analyzed, the approach does not per se consider network effects of investments. To sum up, while the approach proposed by Gordon and Loeb meets all four mandatory criteria, none of the optional ones is met.

2.4.6 Approach by Gordon et al.

Gordon et al. [20] present a wait-and-see approach based on real options. The basic idea of their approach is that in case of uncertainty regarding expected benefits, it may be better to wait for key events to occur. Often higher expected benefits can be yielded this way. Thus, before investing in IS, it may be advisable to wait for an IS breach to happen. As soon as an IS breach occurs, more information to assess the expected benefits of an IS investment is available, which makes the assessment more accurate.

Gordon et al. state that to make an investment, the net present value *(NPV)* of the investment made today must be greater than the *NPV* of the deferred investment. Determining the costs and benefits of an IS investment before an IS breach occurs is, however, uncertain. For instance, Gordon et al. [20, pp. 3–4] provide an example of an organization about to make an investment of \$1,000,000 in IS for 1 year. The benefits of this investment, are, however, uncertain. Either the benefits are \$40,000 or \$200,000 per month, both equally probable. Then, the expected value of the investment is equal to $(12 * \$40{,}000 * 0.5) + (12 * \$200{,}000 * 0.5) - \$1{,}000{,}000 =$ \$440,000. They assume that 1 month later an IS breach occurs and the benefits of the investment become known. Now, the expected value for both savings can be determined: In the 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 $EV_{high} = 11 * \$200{,}000 - \$1{,}000{,}000 = \$1{,}200{,}000$ making the investment economically viable. This example illustrates how the expected value of an IS investment increases from \$440,000 to $\$1{,}200{,}000 * 0.5 = \$600{,}000$ by deferring the decision to invest by 1 month.

Just as all other approaches analyzed, the approach proposed by Gordon et al. is able to deal with investments made as a whole as well as with financial measures. Regarding financial measures, the approach uses two predefined costs coupled with probabilities for determining the economic viability of an IS investment. The approach, is, however, not able to support non-financial measures. While one-time costs and benefits are supported by the approach, running costs and benefits are not per se considered by the approach. These, however, may be discounted and added to one-time measures. The approach proposed by Gordon et al. is applicable without explicitly considering attacks. Like most other approaches analyzed, the approach is not able to support network effects per se. They, however, may be taken into account by considering them as financial measures. To sum up, the approach meets all four mandatory criteria but none of the optional ones.

2.4.7 Approach by Huang et al.

Huang et al. [23] present an approach for determining the optimal amount to invest in IS based on the investment's expected utility. As in the approach proposed by Gordon and Loeb [17], 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 IS breach of an asset. An IS breach is associated with a probability function ρ and potential losses L including direct financial and indirect non-financial losses from, for instance, bad reputation. 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 IS countermeasures to protect the asset. That is,

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

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

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

With respect to the calculation of 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, $u = u(w)$. To determine 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 equation 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 IS breach.

The approach by Huang et al. assumes that the investment is made as a whole. Cases in which the investment is partitioned into smaller parts are not considered. As inputs for supporting investment decisions, the approach uses one-time, financial measures. Non-financial measures, and running costs and benefits, however, are neglected. For decision support, the approach by Huang et al. does not rely on information on attacks. This allows us to apply the approach without considering attacks. Information on network effects of the investment are, however, not reflected by any of the approach's input parameters. To sum up, the approach meets all four mandatory criteria, but does not meet any of the optional ones.

2.4.8 Approach by Mizzi

Mizzi [29] presents an approach for IS investment decisions based on accounting figures. In his approach, Mizzi focuses solely on financial measures comprising the annual costs F to fix a vulnerability, the one-time costs B to implement a security countermeasure, and the annual maintenance costs M. To decide about an IS investment, the costs of the total annual IS expenditures E_S and the expected total annual losses L_T of a given security vulnerability are compared. More concretely, an investment should be made, if the expenditures are lower than the expected total annual losses, that is,

$$E_S < L_T \text{ with } E_S = F + B + M.$$

In subsequent years, B does not incur. Thus, the term is dropped from the equation. 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 losses resulting from unavailability 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 as

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

in case the rebuild costs do not include man-hour costs. Alternatively, if man-hour costs are the dominant rebuild costs, R can be substituted by $R(t)$.

If the approach is used as described by Mizzi, costs and benefits that incur over the course of time discounted to the present point in time are not considered. Mizzi, however, notes that one could additionally use *NPV* or internal rate of return *(IRR)* to better account for running costs and benefits. In contrast to other approaches presented, Mizzi presents an extension to his approach in which the costs to break a security countermeasures *CTB* for an attacker can be taken into account. In all calculations, however, this approach neither takes probabilities of IS breaches nor the success rate of IS countermeasures into consideration.

Just as all other approaches analyzed, the approach proposed by Mizzi is not only able to deal with investments made as a whole but also financial measures are supported. With respect to financial measures, the approach considers eight predefined costs to determine the economic viability of an IS investment. The approach, however, does not take non-financial measures into account. While the approach is able to deal with one-time costs and benefits, running costs and benefits are not taken into account. Mizzi, however, notes that these can be discounted to their present value and added to their one-time counterparts. Contrary to most other approaches analyzed, the approach presents an optional extension in which costs seen by the attacker are considered. The approach, nevertheless, is still applicable without explicitly considering attacks. Network effects are per se not considered by the approach, but may be taken into account when specifying the measures used. To sum up, the approach meets three of the four mandatory criteria. The remaining mandatory criterion and one of the optional criteria are partially met.

2.4.9 Approach by Sonnenreich et al.

Sonnenreich et al. [35] 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 split the costs used for the calculation further into different types of costs. For supporting investment decisions, they calculate *ROSI* as

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

where

$$\text{risk exposure} = ALE = SLE \times ARO;$$

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

Just as all approaches analyzed, the approach proposed by Sonnenreich et al. is able to deal with investments made as a whole as well as with financial measures. In total, the approach considers five predefined costs to determine the *ROSI*. The approach, however, is not able to incorporate non-financial measures. For the determination of the *ROSI*, the approach incorporates one-time costs and benefits, while the approach is not per se able to take running costs and benefits into consideration. These, however, may be discounted to their present value and combined with one-time costs and benefits. Just as most other approaches, the approach presented by Sonnenreich et al. is applicable without explicitly considering attacks. Furthermore, the approach is not per se able to consider network effects of IS investments. To sum up, the approach meets all four mandatory criteria, but does not meet any of the optional ones.

2.4.10 Approach by Tallau et al.

Another approach to IS investment decision making is presented by Tallau et al. [37]. In contrast to the other approaches analyzed, Tallau et al. base their approach on the Balanced Scorecard proposed by Kaplan and Norton [24]. 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 us to view business from four different angles, thus providing a balanced view of an organization's performance.

Tallau et al. use the perspectives as were used for the original Balanced Scorecard, *financial, customer, internal processes,* and *innovation and learning*, to support IT investment decisions. 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 downtime (in hours)" as a measure in their exemplary application [37, 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 weighted degrees of fulfillment is calculated. If this approach is applied in a non-comparative way (i.e., only one investment is evaluated), 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 investments are compared with each other), the investment yielding the highest average degree is recommended.

Just as all other approaches analyzed, the approach proposed by Tallau et al. is able to deal with investments made as a whole. As the approach is based on the Balanced Scorecard, the approach is able to consider financial as well as non-financial measures. The approach allows the decision maker to freely choose the measures used for decision support. Therefore, measures for one-time and running benefits and costs, network effects and attacks can be freely chosen even though they are not predefined by the approach. To sum up, the approach meets all mandatory criteria, and partially meets the optional ones.

2.4.11 Approach by Wang et al.

Wang et al. [40] present an approach supporting IS 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 that is at risk.

VaR denotes the upper limit for daily losses L caused by an IS breach. The loss of the IS breach exceeds *VaR* with probability p. In other words, with a proper IS investment the probability that the daily losses L exceed *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 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 IS investment is in place. The approach by Wang et al. can be applied in two ways. First, in a non-comparative way (i.e., only one investment alternative is evaluated), where *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. Second, in a comparative analysis, in which *VaR* and expected daily costs are calculated and compared for each alternative IS investment. In both ways, the decision maker then chooses either of the alternatives (or the current status) based on whether he or she strives to decrease the expected daily costs or *VaR*.

Just as the other approaches analyzed, the approach proposed by Wang et al. is able to deal with investments made as a whole as well as with financial measures. With respect to financial measures, the approach considers four predefined costs for the assessment of an investment's economic viability. Non-financial measures, however, are not taken into account by the approach. The approach is able to support one-time costs and benefits, while running costs and benefits are not per se supported. Just as most of the other approaches, the approach presented by Wang et al. is applicable without explicitly considering attacks. Network effects are not per se supported by the approach. To sum up, the approach meets the four mandatory criteria but none of the optional ones.

2.5 Discussion

In this section, we discuss 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 meet the criteria derived from the tool's characteristics and its application in cross-organizational settings. Furthermore, we show commonalities and differences of the approaches.

We start with a general discussion of the approaches. Then, for each criterion the degree to which it is met by the analyzed approaches is discussed. Emphasis is put on the consequences that result from meeting or not meeting the criterion. 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 in more detail the two approaches that at least partially meet all mandatory and optional criteria.

The analyzed approaches can be divided into comparative and non-comparative approaches. The approaches by Bodin et al. [4], Butler [7], Tallau et al. [37], and Wang et al. [40] are intended for comparative analyses. In comparative analyses, several investments are compared to each other. Comparative approaches may be unsuitable 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. [37], a single investment is evaluated and compared to a certain threshold of an overall score. The investment can be made if its score exceeds the threshold. The problem, however, is to determine this threshold. As comparative approaches compare alternative investments with each other, they do not necessarily say whether an investment is economically viable. The other approaches are non-comparative. Such approaches can be used to evaluate a single investment. These approaches yield one result based on which the investment decision can be made. When comparing several investments using a non-comparative approach, the results of the approaches, for instance, the *ROSI*, are compared.

Comparing the assistance provided by the approaches, we see that the approaches by Gordon and Loeb [17], Huang et al. [23], and Wang et al. [41] help to calculate the optimal as well as the maximal amount that should be invested. The approaches, however, do not say whether one should make a certain investment. Nevertheless, if the costs of an investment are between the optimal and maximal amount to invest, the investment seems reasonable, the nearer to the optimal amount the better. Similarly, the approach by Wang et al. [40] does not say whether an investment should be made. The approach compares alternatives with respect to the investment's costs and the *VaR* of expected losses. It is up to the decision maker to choose an investment based on his or her risk appetite. The three approaches by Bodin et al. [4], Butler [7], and Tallau et al. [37] give an overview of alternative investments and indicate which investment should be favored. Again, the decision to invest remains with the decision maker. The accounting figure based approaches by Al-Humaigani and Dunn [1], Cremonini and Martini [13], and Mizzi [29] provide the expected return of the investment as the result. In case the return is positive, an investment can be made as its benefits are higher than its costs and it thus can be considered economically viable; in case the return is negative, the investment should be neglected; in case the investment equals zero, it remains with the decision maker to invest or not. The same reasoning is applied in the approach by Gordon et al. [20], except that additionally a deferment of the investment decision is taken into account.

All analyzed approaches for supporting IS investment decisions assume that the investment is made as a whole. That is, the investment is not split into smaller parts, where the decision to invest in some parts may be deferred to a later point in time. This criterion is important as the policy and security configuration management tool is provided as a whole only and cannot be split into modules.

All approaches use financial measures for costs and benefits. This is important as the decision to invest is mostly based on financial figures and as an organization's upper management is particularly interested in financial measures.

Investments, however, do not only have financial benefits. The policy and security configuration management tool aims at increasing an organization's trustworthiness, which is hardly expressible in financial measures. Three of the investigated approaches consider non-financial measures: The approach by Tallau et al. [37] considers besides the financial perspective also the customer, the internal process and the innovation and learning perspective to provide 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. [4] does not allow such a freedom in selecting measures but assesses, for instance, an investment's security architecture coverage. Finding appropriate measures for assessing investments, however, is difficult, time consuming, and depends on the person responsible for selecting the measures [37]. Allowing the decision maker to freely choose the measures used for evaluation, however, may bear some disadvantages. For instance, relationships between measures may not be obvious.

All approaches take one-time costs and benefits into account. This is important as one-time costs, for instance, for acquiring and deploying the policy and security configuration management tool, incur in any case.

Running costs and benefits, in contrast, are not per se supported by all approaches. The approach presented by Mizzi [29] gives formulas for costs incurring after the first year, however, does not discount them. As the measures can be chosen freely when applying the approaches described by Bodin et al. [4] and Tallau et al. [37], respective measures may be selected. Considering running costs is important, as the policy and configuration management tool offers a dynamic mode in which costs and benefits incur over time. Running costs and benefits may however be considered by discounting them to their present value and by adding them to the one-time costs and benefits.

Only two of the analyzed approaches directly consider attacks. First, the approach described by Mizzi [29] provides an extension that takes the attacker's cost to break a countermeasure into consideration. The approach, however, can be applied without the extension. Second, the approach described by Cremonini and Martini [13] which uses the attacker's return on an attack in the decision support.

As expected, none of the analyzed approaches considers network effects of investments per se. The approaches described by Bodin et al. [4] and Tallau et al. [37] 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 taken into consideration. This way, network effects can be taken into account. The more of an organization's suppliers and clients use the policy and security configuration management tool, the higher will be the overall benefit for all involved parties. This is because information about requirements and configurations can be easily exchanged via the tool. Taking the tool's network effects into account is important as the network effects substantially influence the benefits of the tool.

All things considered, the approach for supporting IS investment decisions presented by Cremonini and Martini [13] is the least suitable of the analyzed approaches. The approach meets three mandatory criteria (i.e., the tool is acquired as a whole, financial measures as well as one-time costs and benefits are supported); it neglects, however, important criteria such as non-financial measures, and running costs and benefits. The approaches presented by Al-Humaigani and Dunn [1], Gordon et al. [20], Gordon and Loeb [17], Huang et al. [23], Sonnenreich et al. [35], and Wang et al. [40] meet all four mandatory criteria. They are, thus partially suitable to assess the economic viability of the policy and security configuration management tool used as the subject of the investment decision. The approach described by Mizzi [29] meets three mandatory criteria (i.e., the tool is acquired as a whole, financial measures as well as one-time costs and benefits are supported) and partially fulfills two optional criteria (i.e., running costs and benefits and attackers). The approach presented by Butler [7] is a comparative approach that meets all four mandatory criteria and the optional criterion regarding non-financial measures. Only the approaches by Bodin et al. [4] and Tallau et al. [37] at least partially meet all criteria. They are, nevertheless, both not perfectly suitable to support investment decisions such as the one regarding the policy and security configuration management tool. Both approaches are intended for comparative analyses. Thus, the two approaches do not determine the investment's expected return. They also do not calculate the optimal amount to invest given the value and vulnerability of the asset to be protected. Applying one of those approaches, therefore, does not determine the economic viability, but determines which investment should be favoured over other investments. To have an evaluation with respect to financial and non-financial measures, and to determine the return of the investment or the optimal amount to invest, the approaches presented by Bodin et al. [4] and Tallau et al. [37] could be combined with one of the other approaches. For instance, the approach by Gordon and Loeb [17] or Cremonini and Martini [13] seem to be suitable for such a combination.

2.6 Conclusion

In this chapter, we presented and analyzed a set of approaches for supporting IS investment decisions. More concretely, we evaluated and compared approaches with respect to their suitability for assessing the economic viability of a policy and security configuration management tool. Such a tool helps organizations in general and service providers in particular to ensure compliance with the myriad of regulatory and contractual requirements and to reduce the risk of IS breaches. The tool aims at reducing the costs for policy and security configurations management and at increasing the trustworthiness of organizations. Derived from the tool's characteristics and its application in cross-organizational settings, we evaluated and compared the approaches with respect to whether they support investments made as a whole, consider financial and non-financial measures, are able to take one-time and running costs and benefits into account, are applicable without considering attacks, and take network effects into account.

The findings show that there is no approach which meets all criteria. There are, however, approaches, such as those presented by Bodin et al. [4] and Tallau et al. [37] that meet, at least partially, all criteria. They are, however, intended for comparative analyses and thus need to be adapted before they can be used to assess the economic viability of a single investment. It is very likely that two or more of the investigated approaches could be used in combination to assess the economic viability of the policy and security configuration management tool well. Evaluating different combinations of approaches and determining their suitability for the tool is, however, left to future work. As we focused on a specific policy and security configuration management tool in this chapter, the results are specific to the characteristics of this tool. Using another tool as the subject of the investment decision would most certainly lead to other results.

One issue to be kept in mind is that we focused on approaches that help to assess the economic viability of a certain investment. We simply presupposed that the budget to make economically viable IS investments is available. In practice, however, IS budgets are not inexhaustible. The objective then is to determine how to best spend this fixed budget.

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

References

1. Al-Humaigani, M., 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, Cairo, vols. 1–3, pp. 483–485 (2003)
2. Anderson, R., Schneier, B.: Guest editors' introduction: economics of information security. IEEE Secur. Priv. **3**(1), 12–13 (2005)
3. Bagchi, K., Udo, G.: An analysis of the growth of computer and Internet security breaches. Commun. Assoc. Inf. Syst. **12**, 684–700 (2003)
4. Bodin, L.D., Gordon, L.A., Loeb, M.P.: Evaluating information security investments using the analytic hierarchy process. Commun. ACM **48**(2), 78–83 (2005)
5. Böhme, R.: Security metrics and security investment models. In: Echizen, I., Kunihiro, N., Sasaki, R. (eds.) Security Metrics and Security Investment Models. Lecture Notes in Computer Science, vol. 6434, pp. 10–24. Springer, Berlin/Heidelberg (2010)
6. Böhme, R., 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), London (2009)
7. Butler, S.A.: Security attribute evaluation method: a cost-benefit approach. In: Proceedings of the 24th International Conference on Software Engineering, Orlando, pp. 232–240. ACM (2002)
8. Cavusoglu, H., Cavusoglu, H., Raghunathan, S.: Economics of IT security management: four improvements to current security practices. Commun. AIS **14**, 65–75 (2004)
9. Cavusoglu, H., Mishra, B., Raghunathan, S.: A model for evaluating IT security investments. Commun. ACM **47**(7), 87–92 (2004)
10. Cavusoglu, H., Mishra, B., Raghunathan, S.: The value of intrusion detection systems in information technology security architecture. Inf. Syst. Res. **16**(1), 28–46 (2005)
11. Computerworld: Honda Canada breach exposed data on 280,000 individuals. Website: http://www.computerworld.com/s/article/9217094/Update_Honda_Canada_breach_exposed_data_on_280_000_individuals (2011). Last access 1 Feb 2012
12. Computerworld: RSA warns SecurID customers after company is hacked. Website: http://www.computerworld.com/s/article/9214757/RSA_warns_SecurID_customers_after_company_is_hacked (2011). Last access 1 Feb 2012
13. Cremonini, M., 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), Cambridge (2005)
14. CSI Computer Survey: 14th Annual CSI Computer Crime and Security Survey, San Francisco (2009)
15. Deloitte: Raising the bar: 2011 TMT Global security study – key findings. http://www.deloitte.com/assets/Dcom-Global/Local%20Assets/Documents/TMT/dttl_TMT%202011%20Global%20Security%20Survey_High%20res_191111.pdf (2011)
16. Franqueira, V., Houmb, S., Daneva, M.: Using real option thinking to improve decision making in security investment. In: Meersman, R., Dillon, T., Herrero, P. (eds.) On the Move to Meaningful Internet Systems. Lecture Notes in Computer Science, vol. 6426, pp. 619–638. Springer, Berlin/Heidelberg (2010)

17. Gordon, L.A., Loeb, M.P.: The economics of information security investment. ACM Trans. Inf. Syst. Secur. **5**(4), 438–457 (2002)
18. Gordon, L.A., Loeb, M.P.: Budgeting process for information security expenditures. Commun. ACM **49**(1), 121–125 (2006)
19. Gordon, L.A., Loeb, M.P.: Economic aspects of information security: an emerging field of research. Inf. Syst. Front. **8**(5), 335–337 (2006)
20. Gordon, L.A., Loeb, M.P., Lucyshyn, W.: Information security expenditures and real options: a wait-and-see approach. Comput. Secur. J. **19**(2), 1–7 (2003)
21. Guardian, T.: Sony suffers second data breach with theft of 25 m more user details. Website: http://www.guardian.co.uk/technology/blog/2011/may/03/sony-data-breach-online-entertainment (2011). Last access 1 Feb 2012
22. Herath, H.S.B., Herath, T.C.: Investments in information security: a real options perspective with Bayesian postaudit. J. Manage. Inf. Syst. **25**(3), 337–375 (2008)
23. Huang, C.D., Hu, Q., Behara, R.S.: An economic analysis of the optimal information security investment in the case of a risk-averse firm. Int. J. Prod. Econ. **114**(2), 793–804 (2008)
24. Kaplan, R.S., Norton, D.P.: The balanced scorecard–measures that drive performance. Harv. Bus. Rev. **70**(1), 71–79 (1992)
25. Kark, K., Orlowv, L.M., Bright, S.: Forrester Research: The change and configuration management software market (2007)
26. Liginlal, D., Sim, I., Khansa, L.: How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. Comput. Secur. **28**(3–4), 215–228 (2009)
27. Liu, W., Tanaka, H., Matsuura, K.: Empirical-analysis methodology for information-security investment and its application to reliable survey of Japanese firms. Inf. Media Technol. **3**(2), 464–478 (2008)
28. 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), Hanover (2008)
29. Mizzi, A.: Return on information security investment: the viability of an anti-spam solution in a wireless environment. Int. J. Netw. Secur. **10**(1), 18–24 (2010)
30. Oehrlich, E., Lambert, N.: Forrester Research: How to manage your information security policy framework (2006). http://www.forrester.com/The+Change+And+Configuration+Management+Software+Market/fulltext/-/E-RES42580
31. Sadiq, S., Governatori, G., Namiri, K.: Modeling control objectives for business process compliance: business process management. In: Alonso, G., Dadam, P., Rosemann, M. (eds.) Business Process Management. Lecture Notes in Computer Science, vol. 4714, pp. 149–164. Springer, Berlin/Heidelberg (2007)
32. Schneier, B.: Security ROI. Website: http://www.schneier.com/blog/archives/2008/09/security_roi_1.html (2008). Last access 1 Feb 2012
33. Shirey, R.: Internet security glossary – RFC 2828. Tech. rep., The Internet Engineering Task Force – Network Working Group. http://www.ietf.org/rfc/rfc2828.txt (2000)
34. Sklavos, N., Souras, P.: Economic models and approaches in information security for computer networks. Int. J. Netw. Secur. **2**(1), 14–20 (2006)
35. Sonnenreich, W., Albanese, J., Stout, B.: Return on security investment (ROSI) – a practical quantitative modell. J. Res. Pract. Inf. Technol. **38**(1), 55–66 (2006)
36. Su, X.: An overview of economic approaches to information security management. Tech. rep., Centre for Telematics and Information Technology, University of Twente (2006)
37. Tallau, L.J., Gupta, M., Sharman, R.: Information security investment decisions: evaluating the balanced scorecard method. Int. J. Bus. Inf. Syst. **5**(1), 34–57 (2010)
38. Tsiakis, T.K., Pekos, T.: Analysing and determining return on investment for information security. In: Proceedings of the International Conference on Applied Economics (ICOAE), Chania, Crete, pp. 879–883 (2008)
39. Vroom, C., von Solms, R.: Towards information security behavioural compliance. Comput. Secur. **23**(3), 191–198 (2004)

40. Wang, J., Chaudhury, A., Rao, H.R.: A value-at-risk approach to information security investment. Inf. Syst. Res. **19**(1), 106–120 (2008)
41. Wang, S.L., Chen, J.D., Stirpe, P., Hong, T.P.: Risk-neutral evaluation of information security investment on data centers. J. Intell. Inf. Syst. **36**(3), 329–345 (2011)
42. Webster, J., Watson, R.T.: Analyzing the past to prepare for the future: writing a literature review. MIS Q **26**(2), xiii–xxiii (2002)
43. Whitman, M.E.: Enemy at the gate: threats to information security. Commun. ACM **46**(8), 91–95 (2003)
44. Willemson, J.: On the Gordon and Loeb model for information security investment. In: Proceedings of the 5th Workshop on the Economics of Information Security (WEIS), Cambridge (2006)
45. 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), Krakow, pp. 258–261 (2010)

Springer

http://www.springer.com/978-3-642-39497-3

The Economics of Information Security and Privacy
Böhme, R. (Ed.)
2013, XIII, 321 p. 57 illus., Hardcover
ISBN: 978-3-642-39497-3