Optimizing Information Systems Security Design Based on Existing Security Knowledge

Andreas Schilling(✉) and Brigitte Werners

Faculty of Management and Economics, Ruhr University Bochum,
Universitätsstraße 150, 44780 Bochum, Germany
{andreas.schilling,or}@rub.de
http://www.rub.de/or

Abstract. Information systems and the information enclosed are of significant value and it is indispensable for organizations to ensure their protection. To achieve high security, existing knowledge is available and provides recommendations and guidelines to follow. Due to the large amount of data and the complex dependencies within their structure, it is often challenging to make informed design decisions. This paper proposes a quantitative model that is tailored to the optimal selection of security safeguards from an existing security knowledge base. The input data are extracted from the extensive IT baseline protection catalogues of the German Federal Office for Information Security (BSI). The total amount of data include more than 500 threats and 1200 safeguard options. In an application example, we illustrate that an optimal decision can reduce the number of required safeguards substantially while still maintaining a high security level.

Keywords: Information security · System security design · Decision support model · Combinatorial optimization

1 Introduction

Information technology (IT) has become a critical factor for organizations and continuously spreads into more and more areas. The loss, manipulation, disclosure, or simply the unavailability of information may lead to expenses, missed profits, or even legal consequences. If security is weak, attackers will eventually find a weak spot and cause damage. One approach to deal with information security design is to follow common information security practices and guidelines which are available from various sources including, but not limited to, the International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), and German Federal Office for Information Security (BSI). These practices can help organizations by guiding them on how to establish an effective basis for security. The information is mostly available in form of standards that have to be followed more or less strictly.

For our analysis, we chose on the IT baseline protection catalogues (or IT-Grundschutz catalogues) [4] which are part of a standard provided by the BSI.

A. Persson and J. Stirna (Eds.): CAiSE 2015 Workshops, LNBIP 215, pp. 447–458, 2015.
DOI: 10.1007/978-3-319-19243-7_41

The catalogues are publicly available, free of charge, and offer an extensive repository of technical, organisational, personnel, and infrastructural information security knowledge to protect information systems (IS). The catalogues are also in line with the ISO 27000 series which makes them internationally applicable. Organizations trying to improve security face the challenge of selecting appropriate safeguards from the given catalogues. There is, however, no practical solution available to optimally select safeguards that result in a desired security level. Since most companies have no specialized information security knowledge, this decision process has to be outsourced to a specialized service provider (e.g., a consulting company) which causes additional costs.

This paper presents an approach to optimize information security design by using large amounts of available information. For this purpose, we propose a combinatorial optimization model which makes use of the entire IT baseline protection catalogues. Our model is also applicable to an arbitrary subset of components which makes it usable for any use case covered by the knowledge base of the catalogues. The presented model can help to automate the decision process or at the very least support security design decisions.

The remainder of the paper is organized as follows: Sect. 2 outlines literature related to decision making in IT security. Section 3 discusses the general security investment problem and introduces the source of data which we used as basis for our analysis. Section 4 presents a mathematical model and shows how available data are utilized to support decision making in information security. In Sect. 5, we conceive a realistic case study to demonstrate the application of our model and discuss respective results. Section 6 concludes the paper.

2 Related Work

In recent years, the interest in quantitative models for information security investment decisions has increased significantly. This trend is driven by the fact that system complexity continuously increases and a growing amount of data is available to support decision making. There are several research streams which basically try to solve the security investment problem from different angles. In this analysis, we focus on the selection problem, i.e., what security safeguards should be selected for implementation?

Most approaches addressing this question apply management tools and financial analysis based on measures like annual loss expectancy, return on investment, internal rate of return, net present value, etc. [2,10,11,13]. Other approaches use real options analysis where dynamic aspects of investments are considered and the flexibility of decision making is utilized [6,12,14]. An optimization driven approach to select security safeguards is proposed by Sawik [9] which produces optimal safeguard portfolios. In their study, they used a bi-objective model to minimize expected and worst case losses applying the value-at-risk. Viduto et al. [15] proposed a multi-objective model that also factors in financial costs in addition to losses. Rakes et al. [8] argue that, in addition to expected losses, sparse events that might result in high-impact losses should be considered, too. They propose

a model which considers the trade-off between expected and worst-case losses. If it is not sufficient or possible to deploy safeguards to achieve sufficient security, cyber insurance is also an option [1,7].

These approaches either use a small set of very generic data or require the decision maker to collect most of it before the optimization can be conducted. Our model builds on the foundation and ideas established in previous work but requires less information input which makes it more applicable to practical use cases. Using an existing knowledge base significantly reduces workload during a risk assessment and ensures that the data meet a certain quality threshold. To the best of our knowledge, no model exists to support concrete investment decisions of security safeguards which incorporates large amount of data of an existing knowledge base and is still practically applicable in terms of information requirements and computational time.

3 Problem Description

An organization usually runs several business processes and operates a number of information systems. The continuous operation of these systems and the security of processed information is considered to be of high priority for every organization. For this reason, organizations try to achieve high security of such systems by deploying security safeguards. In order to adequately protect IS, organizations can make use of existing information security knowledge. In the following, we use the IT baseline protection catalogues which consist of components (or modules) that comprise all relevant parts of the processes, applications, and systems of an organization. The IT baseline protection catalogues define 80 components which are grouped into 5 categories: general aspects, infrastructure, information systems, networks, and applications. Each component contains a description of the subject, a list of threats, and a set of applicable safeguard options. In total, the IT baseline protection catalogues contain 518 threats and 1244 safeguards.

The catalogues specify that the security of each component is endangered by a number of threats. Depending on the nature of the threat, it is possible that it applies to more than one component. Each threat has a particular criticality, that can be obtained in an automatic manner from the existing knowledge base. To counteract threats, the organization can deploy various safeguards which reduce the criticality of a specific subset of threats according to the safeguards effectiveness. To use this information, we extracted the information from the catalogues and generated an SQLite database serving as a knowledge base for our evaluation.

If an organization intends to obtain a valid ISO or BSI certificate, there are predefined selections available to achieve different security levels. An entry level certificate requires the implementation of 46 % of the safeguards and the ISO 27001 certificate requires 79 % of all safeguards to be implemented. If a certificate is not required, a smaller subset may be sufficient to achieve a desired security level. The model presented in this paper can be used to obtain an initial selection of safeguards that may be further customized according to additional requirements.

4 Model Formulation

In this section, we consider a single-stage combinatorial optimization model which is set up as a mixed integer linear programming (MILP) problem. The goal is to select a feasible subset of safeguards that maximizes security and meets a number of linear constraints. We first establish a nonlinear formulation in Sect. 4.1 and then use the natural logarithm to linearize it in Sect. 4.2. Table 1 lists parameters and decision variables which are used in the following.

Table 1. Parameters and decision variables.

Indices and sets	
$\mathcal{P}$	Index set of components (indexed by p)
$\mathcal{I}$	Index set of threats (indexed by i)
$\mathcal{K}$	Index set of safeguards (indexed by k)
Parameters	
σ_k	Effectiveness coefficient of a safeguard
γ_i	Criticality coefficient of a threat
$C_{i,p}$	Connection between component and threat, $C_{i,p} \in \{0,1\}$
$T_{k,i}$	Connection between threat and safeguard, $T_{k,i} \in \{0,1\}$
$\overline{N}$	Maximum number of safeguards
Decision variables	
s_k	Selection of safeguards, $s_k \in \{0,1\}$
t_i	Threat criticality index (TCI)
c_p	Component criticality index (CCI)

Let $p \in \mathcal{P}$ denote a component of the system in question and let $i \in \mathcal{I}$ denote a threat. Matrix $C_{i,p} \in \{0,1\}$ denotes whether threat i endangers component p ($C_{i,p} = 1$) or not ($C_{i,p} = 0$) and is given in an extension to the IT baseline protection catalogues. Each threat has a preset criticality coefficient $\gamma_i \geq 0$ and a variable criticality index $t_i \geq 0$. The criticality coefficient of a threat is an input to the model and expresses how severe a threat is without investing in security. The criticality index, on the other hand, is variable and determined during optimization. It is reduced if safeguards are deployed which are applicable to the threat in question. The criticality coefficient is not directly provided by the catalogues and we use a generated value based on available data (see Sect. 5.2).

To determine the criticality of a component, we use variable c_p which is called component criticality index (CCI). Due to the fact that the highest threat is the most critical indicator of security, c_p is defined as the maximum of all criticality indexes of threats associated with the component in question, i.e.,

$$c_p = \max_{i \in \mathcal{I}} \{t_i | C_{i,p} = 1\} \quad \forall p \in \mathcal{P}. \tag{1}$$

Whether threat i is associated with component p is defined by the corresponding value of matrix $C_{i,p}$ and can be obtained from the IT baseline protection catalogues. The definition of c_p is based on the assumption that the security of a component depends on the most critical of its threats, i.e., the weakest link in the security chain. Therefore, to reduce the criticality of a component, the criticality index of its most critical threat has to be reduced first.

By deploying safeguards, the criticality index of a threat is reduced. If no safeguards are deployed for a particular threat, we have $t_i = \gamma_i$. A safeguard only reduces the criticality of a threat if it is associated with this threat ($T_{k,i} = 1$) and if it is implemented ($s_k = 1$). In case an applicable safeguard ($T_{k,i} = 1$ and $s_k = 1 \Leftrightarrow T_{k,i} \cdot s_k = 1$) is deployed, the criticality index of an associated threat is reduced from γ_i to $\gamma_i \cdot \sigma_k$, where $\sigma_k \in [0, 1]$ is the effectiveness coefficient of the deployed safeguard. To generalize this expression for multiple safeguards, we multiply γ_i by

$$ {\sigma_k}^{s_k \cdot T_{k,i}} = \begin{cases} \sigma_k & \text{if } s_k = 1 \text{ and } T_{k,i} = 1 \\ 1 & \text{if } s_k = 0 \text{ or } T_{k,i} = 0 \end{cases} \quad \forall\, k \in \mathcal{K}, \tag{2} $$

which only takes value σ_k if both $s_k = 1$ and $T_{k,i} = 1$ and defaults to 1 otherwise. In case the expression takes value 1, the criticality index of a threat is not reduced. Considering all safeguards at once we get the following equation to calculate the remaining criticality index of threat i:

$$ t_i = \gamma_i \cdot \prod_{k \in \mathcal{K}} {\sigma_k}^{s_k \cdot T_{k,i}} \quad \forall\, i \in \mathcal{I}. \tag{3} $$

4.1 Nonlinear Model for Determining an Optimal Selection of Safeguards

Based on these definitions, we establish the optimization model as follows:

$$ \min \quad \left[\max_{p \in \mathcal{P}} c_p \right] \tag{4} $$

$$ \text{s.t.} \quad c_p = \max_{i \in \mathcal{I}} \{ t_i | C_{i,p} = 1 \} \qquad \forall\, p \in \mathcal{P} \tag{5} $$

$$ t_i = \gamma_i \cdot \prod_{k \in \mathcal{K}} {\sigma_k}^{s_k \cdot T_{k,i}} \qquad \forall\, i \in \mathcal{I} \tag{6} $$

$$ \sum_{k \in \mathcal{K}} s_k \leq \overline{N} \tag{7} $$

$$ s_k \in \{0, 1\} \qquad \forall\, k \in \mathcal{K} \tag{8} $$

$$ t_i \geq 0 \qquad \forall\, i \in \mathcal{I}\,. \tag{9} $$

The objective function (4) minimizes the maximum of all CCIs. This formulation assumes that all components are equally important for the overall security of the system. If this is not the case, it would be possible to weight components

differently by multiplying their indexes with an additional weighting factor. The objective value characterizes the overall security of the system in question and is called the system security index (SSI). Constraint (5) defines CCI c_p as the maximum of associated threat criticality indexes (TCIs). The total number of safeguards is limited to $\overline{N}$ in constraint (7). Finally, the decision regarding the selection of safeguards is binary (8) and all threat criticality indexes have to be nonnegative (9).

4.2 Linearization Using the Natural Logarithm

The established formulation of the problem has some drawbacks regarding its solvability due to its nonlinearity in constraint (6). Nonlinear problems are substantially more difficult to solve than linear problems. We will show in the following how to obtain a MILP formulation of the problem. Constraint (6) is the only nonlinear equation where the product of multiple decision variables is calculated. To reformulate this constraint, we take the natural logarithm of t_i and thus eliminate the multiplication of decision variables:

$$t_i = \gamma_i \cdot \prod_{k \in \mathcal{K}} {\sigma_k}^{s_k \cdot T_{k,i}} \tag{10}$$

$$\Leftrightarrow \qquad \ln(t_i) = \ln(\gamma_i) + \sum_{k \in \mathcal{K}} s_k \cdot T_{k,i} \cdot \ln(\sigma_k) \tag{11}$$

To replace constraint (6) with (10), we have to precompute $\ln(\gamma_i)$ and $\ln(\sigma_k)$ which can be done before starting the optimization. Since ln(.) is a strictly monotonic function, it is order-preserving which means it is still possible to differentiate between t_i values.

The resulting MILP problem is a lot easier to solve with respect to computational complexity. There are several solvers available which can solve large instances within a reasonable solution time. The following version of the problem can be implemented as a linear model and is written as

$$\min \quad \left[\max_{p \in \mathcal{P}} \ln(c_p)\right] \tag{12}$$

$$\text{s.t.} \quad \ln(c_p) = \max_{i \in \mathcal{I}} \{\ln(t_i) | C_{i,p} = 1\} \qquad \forall\, p \in \mathcal{P} \tag{13}$$

$$\ln(t_i) = \ln(\gamma_i) + \sum_{k \in \mathcal{K}} s_k \cdot T_{k,i} \cdot \ln(\sigma_k) \qquad \forall\, i \in \mathcal{I} \tag{14}$$

$$\text{and} \quad (7, 8)\,.$$

Constraint (14) now defines the logarithmic TCI and $\ln(c_p)$ is defined accordingly in constraint (13). The objective function (12) has also been adjusted and now minimizes the maximum logarithmic CCI.

5 Application Scenario

In this section, we give an illustrative example to show some details of the presented model and its application. For this purpose, we use a system which

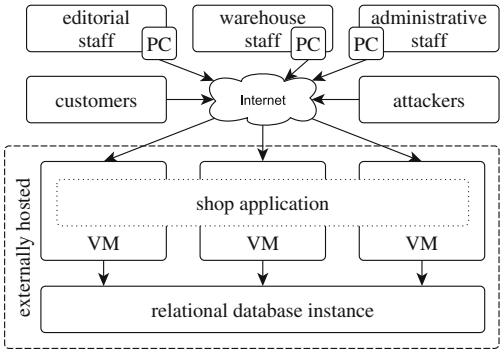

Fig. 1. Externally hosted exemplary e-commerce IS with components and actors.

represents a typical setup for providing a cloud-based e-commerce service. The setup includes a relational database, a shop application running on multiple virtual computing instances (i.e., virtual machines (VMs)), and 5 categories of users. It is visualized in Fig. 1. The computing instances process user requests and access a dedicated database instance to access persistent data. The system is maintained by editorial staff, warehouse staff, and administrative staff. In addition to normal customers which are using the system in the intended way, attackers are threatening the security of the system and data.

The model was implemented in Xpress-Mosel, a modeling and programming language that is part of the FICO® Xpress Optimization Suite [5]. We used the 64 bit version of FICO® Xpress Optimization Suite 7.6 with default settings. Additional data processing, including data extraction and solver input generation was implemented in Python 2.7.

5.1 Data

For our analysis, we extracted 16 components (7 non-technical and 9 technical ones) from the IT baseline protection catalogues which are directly applicable to the system in question. From these components, a list of threats per component and potential safeguards per threat was compiled. All components including the number of threats and safeguards per component are listed in Table 2. For a detailed description of components and a list of corresponding threats, we refer the reader to [4].

To extract information on the connection of threats and safeguards, we used cross-reference tables which are available as an extension to the IT baseline protection catalogues [3]. Since threats may be connected to more than one component and safeguards may be connected to more than one threat, the total number of 190 threats and the total number of 337 safeguards are less than the sum of the columns in Table 2. As a result, the size of matrix $C_{i,p}$ is 16×190 and 190×337 for matrix $T_{k,i}$.

Table 2. System components.

No.	Component	# Threats	# Safeguards
Non-technical			
1	Security management	4	14
2	Organisation	18	17
3	Personnel	21	15
4	Handling security incidents	3	24
5	Outsourcing	26	17
6	Patch and change management	22	18
7	Internet use	23	16
Technical			
8	Data protection	13	16
9	Protection against malware	16	13
10	General server	33	33
11	Servers under Unix	7	26
12	Internet PCs	20	17
13	Client under Windows 7	32	45
14	Web servers	27	27
15	Databases	23	32
16	Web applications	39	38

5.2 Generation of Additional Parameters

The catalogues do not provide an effectiveness coefficient σ_k in the form required for our model. However, each safeguard is assigned a qualification level (A, B, C, Z, W) indicating for which certification it is required (with A being the highest level). For the purpose of our example, we assume that the effectiveness of safeguards is correlated to its qualification level, i.e. a higher qualification level indicates a higher effectiveness. Thus, σ_k is defined as

$$\sigma_k = \begin{cases} 0.5 & \text{if qualification level} = A \\ 0.6 & \text{if qualification level} = B \\ 0.7 & \text{if qualification level} = C \\ 0.8 & \text{if qualification level} = Z \\ 0.9 & \text{if qualification level} = W \end{cases} \quad \forall\, k \in \mathcal{K} \tag{15}$$

where, for example, $\sigma_k = 0.7$ indicates that a safeguard reduces a threat's criticality index t_i by $1 - 0.7 = 30\,\%$ if deployed, hence $t_i = \gamma_i \cdot \sigma_k = \gamma_i \cdot 0.7$.

The second required parameter is the criticality coefficient γ_i of a threat. Since it is also not directly provided by the official standard, we generate it based on the available information. For this purpose, we assume that the criticality of a threat is determined by the number and qualification of safeguards

associated with it. This means if a threat has more and higher qualified safeguards associated with it, it is assumed to be more critical. We use the following calculation to generate γ_i:

$$\gamma_i = \sum_{k \in \mathcal{K}} T_{k,i} \cdot g(\sigma_k) \text{ with } g(x) = \sqrt{x} \quad \forall\, i \in \mathcal{I}\,. \tag{16}$$

Equation (16) states that the threat criticality coefficient γ_i is the sum of associated $g(\sigma_k)$ values where $g(.)$ returns a numeric value for each value of σ_k. Threat i is associated with safeguard k if $T_{k,i} = 1$. For this example, we chose a concave square root function. As a result, safeguards with higher qualification levels influence the criticality index of associated threats at a diminishing rate.

5.3 Results

To evaluate the model, we compare its results with official BSI and ISO certificates. The BSI entry level certificate requires all A level safeguards to be implemented and for an ISO 27001 certificate, all A, B, and C level safeguards are required. In our example, this would require implementing 177 safeguards for an entry level certificate. To fulfill the conditions of an ISO 27001 certificate, 270 safeguards have to be implemented.

To establish a baseline, Fig. 2 shows the component criticality indexes (CCIs) of an unprotected system compared with the entry level and ISO 27001 certifications. In case of an unprotected system, no safeguards are implemented ($s_k = 0, \forall k \in \mathcal{K}$). To obtain the results for the entry level and ISO 27001 certificates, we fixed the values of s_k to 1 if safeguard k is required by the corresponding certificate (and to 0 otherwise). Note that, although we compute these values using the introduced model, no optimization is carried out at this point, since all decision variables are preset by fixating s_k.

Figure 2 shows that both certifications increase security by reducing the criticality of all system components. The components are displayed on the x-axis

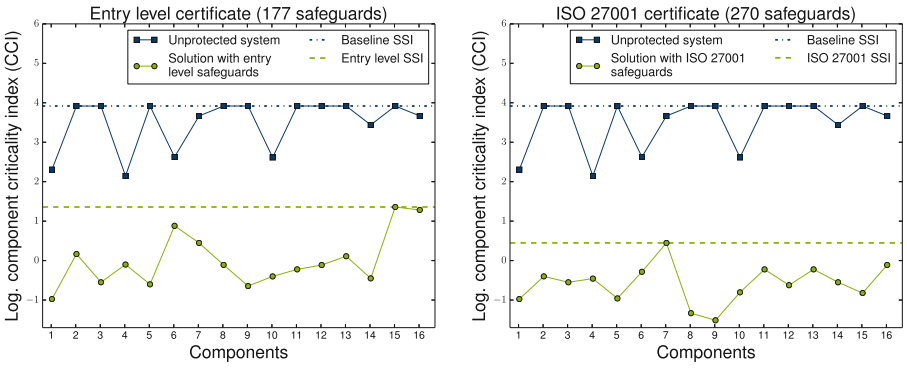

Fig. 2. Logarithmic component criticality indexes (CCIs) of an unprotected system compared with solutions corresponding to entry level and ISO 27001 certifications.

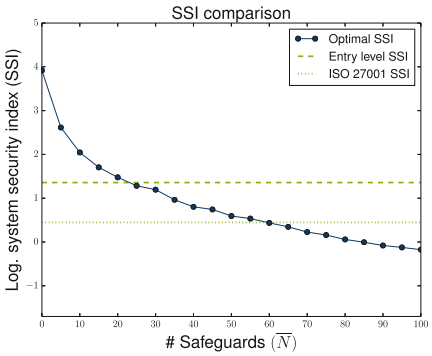

Fig. 3. SSIs of multiple optimal solutions compared with entry level and ISO 27001 certifications.

and the logarithmic CCI is measured on the y-axis. We use logarithmic values to improve readability. In each subplot, the square dots indicate the logarithmic CCIs of an unprotected system and the round dots represent the reduced logarithmic indexes. The dotted line is the objective value of the model, which is the maximum of all component criticality indexes (1). Since the most critical component is the weakest link in the security chain of the system, we call this value the system security index (SSI). We use this value to compare alternative solutions and find that by implementing all entry level safeguards, the logarithmic SSI is reduced by 65.3 % from 3.92 to 1.36 and in case of the ISO 27001 certification by 88.6 % to 0.45. When compared to the actual SSI values, this corresponds to a reduction of 92.3 % and 96.9 % respectively.

Now we are trying to find a smaller selection of safeguards than defined by the standards but one that offers a comparable security level. The questions for an organization trying to do this are: is it possible to achieve a similar security level (i.e., a similar SSI value) by implementing less safeguards? And if so, how many safeguards are necessary for a similar level of security? To answer these questions, we compute several optimal solutions and relax the safeguard limitation (7) in the process. Figure 3 shows the SSIs of 20 optimal solutions where each solution corresponds to an optimal selection of safeguards with a fixed maximum $\overline{N}$ of implemented safeguards. To improve readability, the figure again visualizes the logarithmic SSI values. The dashed and dotted lines mark the SSI of the entry level and ISO 27001 certificates respectively.

As can be seen in Fig. 3, by implementing an optimal solution with a maximum of between 20 and 25 safeguards, it is possible to realize an SSI value similar to the one of the entry level certification. In other words, it is possible to achieve a similar security level with approximately 86 % to 89 % less safeguards. In comparison to the ISO 27001 certificate, the implementation of around 60 safeguards is sufficient for a similar security level which cuts the number of required safeguards by nearly 78 %. These numbers show that an optimal decision with respect to the assumptions outlined can make a significant difference.

However, it should be noted that we do not expect an organization to follow a given solution strictly. Any solution may be used as a starting point for further analyses and design decisions.

6 Conclusion

The security design of information systems is a difficult task due to high system complexity and large amounts of relevant data. To address this problem, a considerable amount of research has been done to determine how to invest based on risk and financial measures. The problem is that existing approaches require the decision maker to provide a lot of exact input data like exact threat and vulnerability probabilities, asset valuations, and other fine-grained parameters. However, these values are very difficult to obtain in practice and, in addition, are critical to the solution. Approaches that require less information often remain vague in their results and require the decision maker to fill in the gaps himself.

The approach presented in this paper is designed to give very concrete decision support and at the same time does not require the decision maker to provide extensive input data. We established a knowledge base with data from the IT baseline protection catalogues of the BSI and developed a combinatorial optimization model to determine an optimal selection of safeguards. The decision maker only has to define the system in question by specifying relevant components. By choosing the maximum number of safeguards, the decision maker can influence the security level of the system according to his risk-preference. We applied our model to an exemplary information system and were able to demonstrate that security levels similar to the ones defined by the BSI and ISO 27001 certificates can be obtained with less safeguards. Using these results as a starting point for further analyses reduces workload and strengthens security.

Future research may include extending the scope of the model by taking additional factors into account. An interesting extension would be a multi-stage model to take into consideration that a system is operated over time. An adaptive multi-stage model could be used during the entire operation of a system to add, exchange, or remove safeguards and thereby adapt to a changing threat environment. To improve the quality of solutions, it is possible to introduce uncertainty of some of the input parameters. In doing so, more robust solutions can be obtained that also yield good security if some input parameters were determined inaccurately.

Acknowledgment. This work was partially supported by the Horst Görtz Foundation.

References

1. Baer, W.S., Parkinson, A.: Cyberinsurance in IT security management. IEEE Secur. Priv. **5**(3), 50–56 (2007)
2. Bojanc, R., Jerman-Blažič, B.: Quantitative model for economic analyses of information security investment in an enterprise information system. Organizacija **45**(6), 276–288 (2012)

3. Federal Office for Information Security: 13. EL: Cross-reference tables of the IT-Grundschutz catalogues: 13th version (2013). https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/hilfmi/checklisten/checklisten.html
4. Federal Office for Information Security: IT-Grundschutz-Catalogues: 13th version (2013)
5. FICO: Xpress-SLP: Program Reference Manual (2008)
6. 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)
7. Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., Sadhukhan, S.K.: Cyber-risk decision models: to insure IT or not? Decis. Support Syst. **56**, 11–26 (2013)
8. Rakes, T.R., Deane, J.K.: Paul Rees, L.: IT security planning under uncertainty for high-impact events. Omega **40**(1), 79–88 (2012)
9. Sawik, T.: Selection of optimal countermeasure portfolio in IT security planning. Decis. Support Syst. **55**(1), 156–164 (2013)
10. Schilling, A., Werners, B.: A quantitative threat modeling approach to maximize the return on security investment in cloud computing. In: Endicott-Popovsky, B. (ed.) Proceedings of the International Conference on Cloud Security Management. Academic Conferences and Publishing International, Reading (2013)
11. Sonnenreich, W., Albanese, J., Stout, B.: Return on security investment (ROSI) - a practical quantitative model. J. Res. Pract. Inf. Technol. **38**(1), 45–56 (2006)
12. Tatsumi, K., Goto, M.: Optimal timing of information security investment: a real options approach. In: Moore, T., Pym, D., Ioannidis, C. (eds.) Economics of Information Security and Privacy, pp. 211–228. Springer, US (2010)
13. Tsiakis, T.: Information security expenditures: a techno-economic analysis. Int. J. Comput. Sci. Netw. Secur. **10**(4), 7–11 (2010)
14. Ullrich, C.: Valuation of IT investments using real options theory. Bus. Inf. Syst. Eng. **5**(5), 331–341 (2013)
15. Viduto, V., Maple, C., Huang, W., López-Peréz, D.: A novel risk assessment and optimisation model for a multi-objective network security countermeasure selection problem. Decis. Support Syst. **53**(3), 599–610 (2012)