Towards a Multi-objective Optimization Model to Support Information Security Investment Decision-making

Eva Weishäupl
University of Regensburg
Germany
eva.weishaeupl@wiwi.uni-regensburg.de

ABSTRACT

The protection of assets, including IT resources, intellectual property and business processes, against security attacks has become a challenging task for organizations. From an economic perspective, firms need to minimize the probability of a successful security incident or attack while staying within the boundaries of their information security budget in order to optimize their investment strategy. In this paper, an optimization model to support information security investment decision-making in organizations is proposed considering the two conflicting objectives (simultaneously minimizing the costs of countermeasures while maximizing the security level). Decision models that support the firms' decisions considering the trade-off between the security level and the investment allocation are beneficial for organizations to facilitate and justify security investment choices.

CCS CONCEPTS

• **Security and privacy → Systems security**;

KEYWORDS

Information security investment, decision-making, multi-objective optimization

ACM Reference format:
Eva Weishäupl. 2017. Towards a Multi-objective Optimization Model to Support Information Security Investment Decision-making. In *Proceedings of SHCIS'17, Neuchâtel, Switzerland, June 21-22, 2017,* 6 pages.
DOI: http://dx.doi.org/10.1145/3099012.3099013

1 INTRODUCTION

More and more organizations are highly reliant on information technology (IT) for their operative business to the extent that failure of IT systems could seriously damage the firm [34]. Additionally, security threats have become more advanced and frequent in the past years [39]. According to a global survey of Grant Thornton, one in six businesses has been targeted by a cyber-attack in the past year [24]. This led to a blow up of the costs caused by security incidents: In 2015, cybercrime is estimated to have caused $315 billion in damages worldwide [24]. To avoid these damages, organizations need to protect systems, data and processes by reducing vulnerabilities and by improving their monitoring capabilities [18]. Specifically, they invest into various security technologies to prevent, or, at least, reduce the probability and the impact of breaches. These security countermeasures protect systems, data and processes against technical failure, damage or attacks such as data loss prevention, spy-ware detection, removal applications and cryptographic techniques [18, 20]. Information security investments surpassed $75.4 billion worldwide in 2016 and are expected to grow further [13, 19].

When it comes to information security investments, key tasks for organizations are (1) to determine the optimal amount to invest, (2) to decide which technical, managerial and organizational security countermeasures lead to a sufficient level of protection and (3) to decide how much should be spent on which countermeasure in the presence of budget constraints [2, 12, 23]. All in all, deciding on investments considering the trade-off between investment costs and the increase in information security that is brought by the investment is a challenging task for information security managers: a variety of security controls is available and recommended but optimal decisions need to be made in the presence of trade-offs between the two conflicting objectives. In practice, these decisions are frequently made based on the personal perception and experience of the decision maker who is usually unfamiliar with certain system characteristics, vulnerabilities and threats [51]. Academic researchers approached this problem with quantitative and qualitative methods neglecting the crucial factor of practical applicability [51]. To address this issue, we pose the following research question:

> How do firms need to allocate their information security budget in order to maximize the security level (i.e. to minimize the risk of a successful attack) while minimizing their information security expenses?

To answer this research question, we provide a multi-objective optimization model that can be used as a decision support system by organizations to determine the security controls to invest in for an optimal result regarding the maximization of security and minimization of investments, in order to optimize their investment strategy. Multi-objective optimization is a decision-theoretic approach to find solutions for multiple objective problems, i.e. optimization problems involving more than one objective function which have to be optimized simultaneously.

This paper is structured as follows: In the next section, we give a short overview on the literature on decision-making in the context of information security investments. Afterwards, we present the multi-objective optimization model and discuss approaches to

SHCIS'17, Neuchâtel, Switzerland

DOI: http://dx.doi.org/10.1145/3099012.3099013

finding solutions. Finally, we conclude the paper and give possible directions for future research.

2 RELATED WORK

According to Huang et al. [29], academic research streams in the field of information security investments address the following three main questions: (1) what is the optimal amount of information security investment, (2) in what security controls to invest, and (3) how to make the investment effective. The first question is mainly approached with traditional decision analysis including utility theory or value-at-risk approaches [29], e.g., in [21], [1] or [30]. The third question regarding the effectiveness of the information security investment has been addressed in literature with game theory [29], e.g., in [10, 16, 17] or [41]. The first and third question will not be addressed in this paper.

We focus on the second question regarding the allocation of the prior determined budget to security controls. In academic literature, this allocation problem has been addressed with traditional management tools like cost-benefit analysis or financial analysis [29] but is still not sufficiently solved [44]. Cost-benefit analysis methods have been applied to compare alternative security designs with the firms current implementation of security countermeasures to check if a more efficient selection is available [8].

In financial analysis approaches metrics such as return on security investment (ROSI), net present value (NPV) or internal rate of return (IRR) are used as decision-support to select appropriate investments [22, 25, 32, 33, 40, 47, 49]. Furthermore, analytic hierarchical process (AHP) has been applied to determine the optimal allocation of the information security budget [6]. In the AHP model qualitative concerns and quantitative (financial) measures in information security are combined [6].

In addition, optimization models have been used for the allocation of countermeasures: In [52] a multi-objective decision-making framework is used to meet the conflict between cost and benefit. The opportunity costs and the direct costs including procurement, training and implementation of security controls are minimized with regard to several economic constraints.
The multi-objective approach presented in [46] takes the decision-maker's risk-preferences into account and supports him in selecting portfolios of security controls in order to reduce the risk of security incidents. Three objective functions (minimizing the costs, minimizing residual risk and maximizing the number of measures in a portfolio) are considered [46]. Sawik [43] also considers the decision-makers cost/risk preferences and his preferred confidence level. Furthermore, Viduto et al. [51] provide a model to select security countermeasures regarding financial costs and residual risks. While considering the relationship between system vulnerabilities, threats and countermeasures, a risk assessment and optimization model (RAOM) was proposed [51].

While extant research has contributed useful insights in the domain of information security investment allocation, a decision-support model for investment allocation considering the classic components of risk analysis namely assets, controls, vulnerabilities and threats and their interdependencies is still missing [27]. In order to close this gap, we propose a multi-objective optimization model to support information security investment decision making which will be described in the following.

3 MULTI-OBJECTIVE OPTIMIZATION-MODEL

In this paper the terms asset, threat, vulnerability and control are defined as follows:

An *asset* a_i, $i = 1, ..., n$ is a tangible or intangible resource including people, property and information which has value for the firm and needs protection [5], for example hardware, software, data, network infrastructure, company reputation, knowledge or skills.

A *threat* t_j, $j = 1, ..., m$ is defined as any circumstance, entity or event that can exploit a vulnerability, intentionally or accidentally, and access, damage, or destroy an asset [4, 36]. Threats include natural disaster (e.g., lightning, hurricane) and internal or external cyber threats (malicious former or current employees, competitors, terrorists or hackers) [7].

A *vulnerability* v_k, $k = 1, ..., p$ is a technical or organizational weakness or gap in a firm's protection efforts which can be exploited by threats and result in security incidents [5]. Examples are software and hardware bugs or backdoors, insufficient policies for employees or ineffective controls.

Controls c_l, $l = 1, ..., q$ are countermeasures which reduce the ability for a threat to exploit existing vulnerabilities by preventing, detecting, counteracting or mitigating security risks [5]. These controls can be classified into three categories [45]: technical controls including firewalls, antivirus software and encryption techniques, operational controls including physical access controls and backup capabilities and management controls including policies and employee training [3, 45].

Methods and procedures for the identification of assets, threats, vulnerabilities and controls in organizations can be found in [32], [15], [9] or [35]. To identify a firm's assets, a framework provided by the National Institute of Standards and Technology (NIST) can be applied which uniquely identifies assets using known information [54]. For the identification of threats, archival records of attacks in log files or threat modelling techniques (e.g., attack graphs, attack trees or onion skin models) can be used [37]. Vulnerabilities can be identified through automated vulnerability scanning tools or penetration tests with the aid of databases such as the National Vulnerability Database (NVD) which publicly provides information on reported vulnerabilities [51, 55]. Moreover, a comprehensive list of 114 security controls in 14 groups can be found in the information security standard ISO/IEC 27001:2013 [31]. From this list, the organization can identify those security controls which are already applied.

Once this information has been gathered, the decision maker is facing the problem of choosing the most effective and efficient security controls to implement.

The relationship between the constructs is depicted in Figure 1 adopted from [50]: controls protect the assets from harm through threats. Thus implementing a control aims to close, or at least reduce, a vulnerability. To be more precise, assets are affected by vulnerabilities and threads exploit these vulnerabilities, if they are

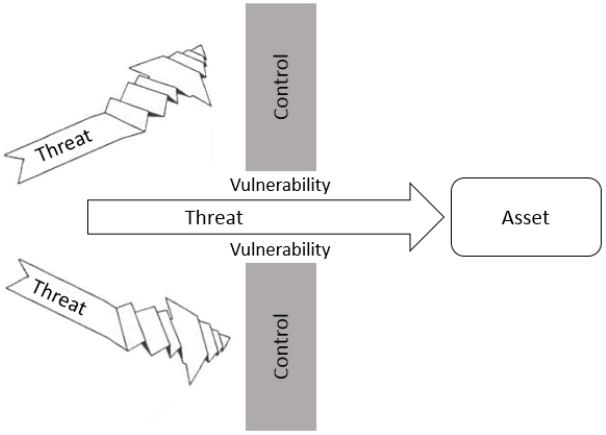

Figure 1: Interrelationship between assets, threats, vulnerabilities and controls [50]

not protected by a corresponding control. For example, the asset *data* can be affected by the vulnerability *lack of training* and the threat *employee* can exploit this vulnerability. The associated control is a *security workshop to train employees*.

Therefore, we assume the relations

$$R := \big\{(a_i, v_k), (t_j, v_k), (c_l, v_k) \mid i = 1, ..., n; j = 1, ..., m; k = 1, ..., p; l = 1, ..., q\big\}.$$

In the following, $(a_i, v_k) \in R$ indicates that the asset a_i is affected by the vulnerability v_k. Analogously, $(t_j, v_k) \in R$ indicates that the threat t_j exploits the vulnerability v_k. In consequence, the set of all threats exploiting the vulnerability v_k can be expressed as

$$\{t_j \mid j = 1, ..., m \text{ and } (t_j, v_k) \in R\}. \tag{1}$$

Furthermore, let w_{a_i} be the importance value of the asset a_i as described in [15]. This importance value indicates the comprehensive impact on the firm if the asset should not be available and can be calculated from the importance values of the business processes which require this asset [15]. Additionally, $P(t_j)$ be the probability of the threat t_j occurring. It can be calculated as described in the threat probability determination phase in [15]. The quality of a control c_l is defined as g_{c_l} as described in [15]. The quality g_{c_l} of a control c_l indicates the probability of a control protecting a vulnerability. Additionally, s_{v_k} is the severity of the vulnerability v_k which indicates the overall impact on the organization should the vulnerability be exploited by a threat.

For the multi-objective optimization model two objective functions are considered with the primary objective being the maximization of the security level and the secondary objective being the minimization of the investment amount in information security controls and costs in case of security incidents. These two objective functions are optimized with respect to the implementation of controls (decision variables) in the presence of constraints on the variables, i.e. a solution is computed which gives the values of the objective functions acceptable for the decision maker.

Note that the threats are modelled as uncontrollable variables, i.e. they are not under the control of the decision makers.

Due to the duality principle, i.e. converting a maximization to a minimization problem by multiplying the objective function by -1, the multi-objective optimization model has the general form

$$\min\,(f_1(x), f_2(x))$$
$$\text{s.t. } x \in X$$

with x being a vector of decision variables and X being a feasible set for x defined by constraint functions.

In the following, we will develop the two objective functions (security function and cost function) and the constraints. Afterwards we discuss approaches to solving the multi-objective optimization model.

3.1 Security Function

To calculate the security level, we assume that the total security level is computed from the security levels per asset weighted by the assets' importance value w_{a_i}, i.e.

$$\text{security level} = \sum_{a_i} \text{security level}\,(a_i) \cdot w_{a_i}. \tag{2}$$

Hereby, the security level of an asset a_i is calculated by

$$\text{security level}\,(a_i) = 1 - \min\big(1, \sum_{\substack{v_k \\ (a_i, v_k) \in R}} s(v_k)\big) \tag{3}$$

which means that the security level of a_i is diminished by the severities of each vulnerability a_i is affected by. To ensure a consistent interpretation of the security level of a_i, negative values are prohibited (by applying the minimum function).

The severity s_{v_k} of a vulnerability v_k is computed from the corresponding threats and controls [53].

The probabilities of occurrence of the treats are regarded as independent events. Hence, the probability of occurrence for a set of threads threatening a vulnerability v_k is computed as follows:

$$1 - \Big(\prod_{\substack{t_j \\ (t_j, v_k) \in R}} 1 - P(t_j) \Big) = P(t_1 \vee t_2 \vee ... \vee t_m) \text{ for } (t_j, v_k) \in R. \tag{4}$$

The probability that v_k is not protected by the corresponding controls (the gap as depicted in Figure 1) is

$$\prod_{\substack{c_l \\ (c_l, v_k) \in R}} (1 - g_{c_l}) \tag{5}$$

and therefore we set

$$s(v_k) = \prod_{\substack{c_l \\ (c_l, v_k) \in R}} (1 - g_{c_l}) \cdot \big(1 - \prod_{\substack{t_j \\ (t_j, v_k) \in R}} (1 - P(t_j))\big). \tag{6}$$

All in all, the security function is

$$\sum_i w_{a_i} \cdot \Bigg(1 - \min\Bigg(1, \sum_{\substack{v_k \\ (a_i, v_k) \in R}} \Big(\big(\prod_{\substack{c_l \\ (c_l, v_k) \in R}} (1 - g_{c_k})\big) \cdot \Big(1 - \prod_{\substack{t_j \\ (t_j, v_k) \in R}} (1 - P(t_j))\Big)\Big)\Bigg)\Bigg). \tag{7}$$

In the security function, the set of assets, threats and vulnerabilities is fixed whereas the set of controls is variable.

3.2 Cost Function

According to [26, 48], the cost function consists of

- configuration-specific costs including software costs (with license fees), hardware costs and one-time IT labor costs for setup,
- operating costs including annual fixed operating costs (e.g., annual license fees, updates) and annual variable operating costs (e.g., employee workshops or training),
- costs in case of security incidents including immediate economic impact (e.g., disruption of business processes, damage in system requiring repair), short-term economic impact (e.g., negative impact on reputation of firm) and long-term economic impact (e.g., decline in stock price).

We define a security incident as follows: A threat t_j successfully exploits a vulnerability v_k and accesses, damages or destroys an asset a_i resulting in economic losses. The set of all security incidents is denoted by SI. The cost of such a security incident are reduced by the controls c_l which affect the vulnerability v_k, i.e. $C(v_k) := \{c_l \mid l = 1, ..., q \text{ and } (c_l, v_k) \in R\}$.

Accordingly,

$$\begin{aligned}\text{cost function} := &\sum_{c_l} \text{configuration-specific costs } (c_l) \\ &+ \sum_{c_l} \text{operating costs } (c_l) \\ &+ \sum_{(a_i, t_j, v_k) \in \text{SI}} \text{costs in case of security incidents}(a_i, t_j, v_k, C(v_k)).\end{aligned} \tag{8}$$

Hereby the configuration-specific costs regarding all controls are

$$\sum_{c_l} \big(\text{software costs}(c_l) + \text{hardware costs}(c_l) + \text{IT labor costs}(c_l)\big). \tag{9}$$

For already implemented controls configuration-specific costs are negligible or significantly lower than for newly purchased ones.

The operating costs regarding all controls are

$$\sum_{c_l} \sum_{t=0}^{T} \frac{\text{fixed operating costs}(c_l) + \text{variable operating costs}(c_l, t)}{(1+k)^t} \tag{10}$$

with $t = 0, ..., T$ being the time horizon and k the interest rate. Scaling may be necessary for configuration-specific and operating costs since one-time or annual license fees for certain controls (e.g., anti-virus software) may apply to the whole organization or specific entities (e.g., each computer requires its own license).

The costs in case of a security incident $(a_i, t_j, v_k) \in SI$ are computed through

$$\begin{aligned}&\text{immediate impact } (a_i, t_j, v_k, C(v_k)) \\ &+ \text{short-term impact } (a_i, t_j, v_k, C(v_k)) \\ &+ \text{long-term impact } (a_i, t_j, v_k, C(v_k)).\end{aligned} \tag{11}$$

For the computation of the immediate, short-term and long-term impacts as functions of a_i, t_j, v_k and $C(v_k)$, valuation scores for intangible damages caused by security incidents which range from 1 to 10 as developed in [14] can be used. These valuation scores are mapped to financial losses. For instance, a major stock price impact has the valuation score 10 and the associated financial loss of \$25 M to \$30 M for a specific firm [14].

3.3 Constraints

For the multi-objective optimization model we maximize the security level and minimize the costs subject to the following constraints.

3.3.1 Budget Constraint. Since most organizations have a budget for information security which can be spent on security controls [42], a budget constraint is required. Therefore, we add the inequality constraint

$$\text{costs} \leq \text{budget}. \tag{12}$$

This budget should be determined by the decision maker in advance. It can be obtained from a variety of methods ranging from personal opinion to formal theoretical development (e.g., [21]).

3.3.2 Non-negativity and Integrality Conditions. The following conditions on the data parameters should be met:

$$g_{c_l} \in [0, 1] \; \forall \, l = 1, ..., q, \tag{13}$$

$$P(t_j) \in [0, 1] \; \forall \, j = 1, ..., m, \tag{14}$$

$$w_{a_i} \in [0, 1] \; \forall \, i = 1, ..., n, \tag{15}$$

$$\sum_{i=1}^{n} w_{a_i} = 1. \tag{16}$$

Note that constraints for the severity s_{v_k} arise from the constraints on g_{c_l} and $P(t_j)$ and that the security level as defined through the security function (7) has a value between 0 and 1 and thus is normalized and ratio-scaled, improving the interpretability.

In our model, the non-negativity and integrality conditions are hard constraints, i.e. they are required to be satisfied. The budget constraint is a soft constraint which has some variable values that are penalized in the objective function if the conditions on the variables are not satisfied.

4 SOLVING THE MULTI-OBJECTIVE OPTIMIZATION-MODEL

Since the security level increases with high investments because those investments are said to reduce vulnerabilities and expected losses, the two objective functions as defined above are conflicting. Therefore, there does not exist one single solution that simultaneously optimizes each objective but a (perhaps infinite) set of pareto optimal solutions[1]. In practice, however, the decision maker only needs one solution and has to choose one of the optimal solutions. He has to include additional information, namely his preferences among the two competing objectives. In our case, the decision

[1] A solution is *pareto optimal* if none of the objectives can be improved without impairing at least one of the others [11].

maker needs to weight the objectives depending on whether he considers the minimization of investments or the maximization of the security level as more important.

For the consideration of the decision maker's preferences three different approaches are available [38]. These approaches can be distinguished from each other based on the role played by the decision maker [46]: (1) When using the *a priori approach*, the decision maker specifies his preferences before the optimization is conducted. (2) In an *a posteriori approach* the decision maker chooses one solution out of a representative set of pareto optimal solutions according to his preferences after the optimization is conducted. The a posteriori approach is the most common approach [28]. (3) In an *interactive approach* the decision maker provides information on his preferences at various times during the optimization. This information is taken into account when generating new pareto optimal solutions which can be assessed by the decision maker in the next iteration [38]. Therefore, the interactive approach allows the decision maker to guide the search for the optimal solution.

The drawback for the a priori approach is that it may be difficult for the decision maker to define his preferences before the optimization starts because he may not yet have gathered enough information on the alternatives and their strengths and weaknesses [46]. In the a posteriori approach, however, the choosing among a large number of solutions may be challenging. Both problems are eliminated in the interactive approach. Moreover, the computational costs are low for interactive methods [38].

All in all, the interactive approach for finding the optimal solution to our multi-objective optimization model is recommended.

5 CONCLUSION

We developed a multi-objective optimization model which can be used in organizations to determine the optimal allocation of the security expenses to specific security controls. It is taken into account that firms simultaneously aim to reduce their spending on information security and to attain a certain level of security. These goals are modelled as objective functions which are optimized with respect to the implementation of security controls in the presence of hard constraints on the variables. To develop the two objective functions, we consider an interrelationship between the constructs assets, vulnerabilities, threats and security controls. Finally, we identify the interactive approach as the most appropriate one for solving the proposed model.

The model can be utilized in organizations as a decision support system to determine the security controls to invest in for an optimal result regarding costs and security. The decision maker is provided with quantitative results to justify the decision he ultimately makes against his supervisor.

In the future, we would like to evaluate the presented model with conducting a case study to test the model's real world applicability and to discuss the benefits of adopting quantitative decision support techniques in comparison with qualitative ones.

Furthermore we will extend the model so that risk-preferences of the firm are taken into account, i.e. whether the organization or the decision maker has a risk-averse, risk-neutral or risk-seeking attitude to information security.

Also we would like to consider the different important values of assets for different departments or stakeholders. For example, a specific software may be essential to one department's business but irrelevant to another's business.

Moreover, the compatibility of security controls to each other is crucial: security controls might be mutually exclusive or reduce each other's effectiveness when implemented simultaneously. Such interdependencies need to be modelled as constraints.

Additionally, the model should consider that the implementation of security controls can cause further hidden costs. For instance, encryption on mobile computing devices may slow down the boot process which reduces the employees' productivity or impedes business processes.

ACKNOWLEDGEMENT

The research leading to these results was supported by the 'Bavarian State Ministry of Education, Science and Arts', as part of the FORSEC research association.

REFERENCES

[1] Tobias Ackermann, Thomas Widjaja, and Peter Buxmann. 2013. Towards the Optimal Security Level: Quantification of Risks in Service-Based Information Systems. In *System Sciences (HICSS), 2013 46th Hawaii International Conference on System Sciences*. IEEE, 3038–3047.

[2] Ross Anderson and Bruce Schneier. 2005. Guest Editors' Introduction: Economics of Information Security. *IEEE Security & Privacy* 3, 1 (2005), 12–13.

[3] Wade H Baker and Linda Wallace. 2007. Is Information Security under Control?: Investigating Quality in Information Security Management. *IEEE Security & Privacy* 5, 1 (2007).

[4] France Belanger, Janine S Hiller, and Wanda J Smith. 2002. Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes. *The journal of strategic Information Systems* 11, 3 (2002), 245–270.

[5] Stefano Bistarelli, Fabio Fioravanti, and Pamela Peretti. 2006. Defense Trees for Economic Evaluation of Security Investments. In *First International Conference on Availability, Reliability and Security (ARES'06)*. IEEE, 8–pp.

[6] Lawrence D Bodin, Lawrence A Gordon, and Martin P Loeb. 2005. Evaluating Information Security Investments Using the Analytic Hierarchy Process. *Commun. ACM* 48, 2 (2005), 78–83.

[7] Jakub Breier and Ladislav Hudec. 2013. On Selecting Critical Security Controls. In *Availability, Reliability and Security (ARES), 2013 Eighth International Conference on*. IEEE, 582–588.

[8] Shawn A Butler. 2002. Security Attribute Evaluation Method: A Cost-benefit Approach. In *Proceedings of the 24th international conference on Software engineering*. ACM, 232–240.

[9] Koen Buyens, Bart De Win, and Wouter Joosen. 2007. Empirical and Statistical Analysis of Risk Analysis-driven Techniques for Threat Management. In *Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on*. IEEE, 1034–1041.

[10] Huseyin Cavusoglu, Birendra Mishra, and Srinivasan Raghunathan. 2005. The Value of Intrusion Detection Systems in Information Technology Security Architecture. *Information Systems Research* 16, 1 (2005), 28–46.

[11] Kalyanmoy Deb, Karthik Sindhya, and Jussi Hakanen. 2016. Multi-objective Optimization. In *Decision Sciences: Theory and Practice*. CRC Press, 145–184.

[12] Lukas Demetz and Daniel Bachlechner. 2013. To Invest or Not to Invest? Assessing the Economic Viability of a Policy and Security Configuration Management Tool. In *The Economics of Information Security and Privacy*. Springer, 25–47.

[13] eWeek. 2016. Spending on Information Security Expected to Rise in 2016. Article. (January 2016). http://www.eweek.com/it-management/spending-on-information-security-expected-to-rise-in-2016.html.

[14] Fariborz Farahmand, Shamkant B Navathe, Philip H Enslow, and Gunter P Sharp. 2003. Managing Vulnerabilities of Information Systems to Security Incidents. In *Proceedings of the 5th international conference on Electronic commerce*. ACM, 348–354.

[15] Stefan Fenz, Andreas Ekelhart, and Thomas Neubauer. 2011. Information Security Risk Management: In which Security Solutions is it worth investing. *Communications of the Association for Information Systems* 28, 1 (2011), 329–356.

[16] Xing Gao, Weijun Zhong, and Shue Mei. 2013. A Differential Game Approach to Information Security Investment under Hackers Knowledge Dissemination. *Operations Research Letters* 41, 5 (2013), 421–425.

[17] Xing Gao, Weijun Zhong, and Shue Mei. 2013. A Game-Theoretic Analysis of Information Sharing and Security Investment for Complementary Firms. *Journal of the Operational Research Society* 65, 11 (2013), 1682–1691.

[18] Gartner. 2011. Gartner Highlights Strategies for Dealing with the Increase in Advanced Targeted Threats. Press Release. (August 2011). http://www.gartner.com/newsroom/id/1774514 http://www.gartner.com/newsroom/id/1774514.

[19] Gartner. 2015. Gartner Says Worldwide Information Security Spending Will Grow Almost 4.7 Percent to Reach 75.4 Billion in 2015. Press Release. (September 2015). http://www.gartner.com/newsroom/id/3135617 http://www.gartner.com/newsroom/id/3135617.

[20] Gartner. 2016. Magic Quadrant for Enterprise Data Loss Prevention. Article. (January 2016). https://www.gartner.com/doc/reprints?id=1-2X96R6A&ct=160128&st=sb https://www.gartner.com/doc/reprints?id=1-2X96R6A&ct=160128&st=sb.

[21] Lawrence A Gordon and Martin P Loeb. 2002. The Economics of Information Security Investment. *ACM Transactions on Information and System Security* 5, 4 (2002), 438–457.

[22] Lawrence A Gordon and Martin P Loeb. 2002. Return on Information Security Investments: Myths vs. Realities. *Strategic finance* 84, 5 (2002), 26–31.

[23] Lawrence A Gordon and Martin P Loeb. 2006. Economic Aspects of Information Security: An Emerging Field of Research. *Information Systems Frontiers* 8, 5 (2006), 335–337.

[24] Grant Thornton. 2015. Cyber Attacks Cost Global Business over 300bn. Press Release. (September 2015). http://www.grantthornton.global/insights/articles/cyber-attacks-cost-global-business-over-300bn-a-year/

[25] Manish Gupta, Shamik Banerjee, Manish Agrawal, and H Raghav Rao. 2008. Security Analysis of Internet Technology Components enabling Globally Distributed WorkplacesâĂŤA Framework. *ACM Transactions on Internet Technology (TOIT)* 8, 4 (2008), 17.

[26] Hemantha SB Herath and Tejaswini C Herath. 2008. Investments in Information Security: A real options Perspective with Bayesian Postaudit. *Journal of Management Information Systems* 25, 3 (2008), 337–375.

[27] Almut Herzog, Nahid Shahmehri, and Claudiu Duma. 2007. An Ontology of Information Security. *International Journal of Information Security and Privacy (IJISP)* 1, 4 (2007), 1–23.

[28] Jan Hettenhausen, Andrew Lewis, Marcus Randall, and Timoleon Kipouros. 2013. Interactive Multi-objective Particle Swarm Optimisation using Decision Space Interaction. In *Evolutionary Computation (CEC), 2013 IEEE Congress on*. IEEE, 3411–3418.

[29] C Derrick Huang, Ravi S Behara, and Jahyun Goo. 2014. Optimal Information Security Investment in a Healthcare Information Exchange: An Economic Analysis. *Decision Support Systems* 61 (2014), 1–11.

[30] C Derrick Huang, Qing Hu, and Ravi S Behara. 2006. Economics of Information Security Investment in the Case of Simultaneous Attacks. (2006).

[31] International Standard ISO/IEC 27001: 2013. 2005. Information Technology–Security Techniques–Information Security Management Systems–Requirements. (2005).

[32] Borka Jerman-Blažič and others. 2008. An economic modelling approach to information security risk management. *International Journal of Information Management* 28, 5 (2008), 413–422.

[33] Borka Jerman-Blažič and others. 2008. Towards a Standard Approach for Quantifying an ICT Security Investment. *Computer Standards & Interfaces* 30, 4 (2008), 216–222.

[34] Grover S Kearns and Albert L Lederer. 2004. The Impact of Industry Contextual Factors on IT focus and the use of IT for Competitive Advantage. *Information & Management* 41, 7 (2004), 899–919.

[35] Man Li, Xinxi Feng, and Jiaoping Chen. 2009. Research of Threat Identification based on Bayesian Networks. In *Wireless Communications, Networking and Mobile Computing, 2009. WiCom'09. 5th International Conference on*. IEEE, 1–3.

[36] Martin Ljungdahl and Michael Nordström. 2016. Security Analysis of Machine Monitoring Sensor Communication. (2016).

[37] Carsten Maple and Valentina Viduto. 2010. A Visualisation Technique for the Identification of Security Threats in Networked Systems. In *Information Visualisation (IV), 2010 14th International Conference*. IEEE, 551–556.

[38] Kaisa Miettinen, Francisco Ruiz, and Andrzej P Wierzbicki. 2008. Introduction to multiobjective optimization: interactive approaches. In *Multiobjective Optimization*. Springer, 27–57.

[39] Ponemon Institute. 2015. *2015 Cost of Data Breach Study: Global Analysis*. Technical Report. Ponemon Institute.

[40] Steve Purser. 2004. *A Practical Guide to Managing Information Security*. Artech House.

[41] Genserik Reniers and Karel Soudan. 2010. A Game-Theoretical Approach for Reciprocal Security-Related Prevention Investment Decisions. *Reliability Engineering & System Safety* 95, 1 (2010), 1–9.

[42] Robert Richardson and CSI Director. 2008. CSI Computer Crime and Security Survey. (2008).

[43] Tadeusz Sawik. 2013. Selection of Optimal Countermeasure Portfolio in IT Security Planning. *Decision Support Systems* 55, 1 (2013), 156–164.

[44] Andreas Schilling and Brigitte Werners. 2015. Optimal Information Security Expenditures Considering Budget Constraints.. In *PACIS*. 251.

[45] Gary Stoneburner, Alice Y Goguen, and Alexis Feringa. 2002. Sp 800-30. Risk Management Guide for Information Technology Systems. (2002).

[46] Christine Strauss and Christian Stummer. 2002. Multiobjective Decision Support in IT-Risk Management. *International Journal of Information Technology & Decision Making* 1, 02 (2002), 251–268.

[47] Xiaomeng Su. 2006. An Overview of Economic Approaches to Information Security Management. (2006).

[48] Hanna Toivanen. 2015. Case Study of Why Information Security Investment Fail? (2015).

[49] Theodosios Tsiakis and George Stephanides. 2005. The Economic Approach of Information Security. *Computers & security* 24, 2 (2005), 105–108.

[50] Assurance User and Audit Planning. 1995. An Introduction to Computer Security: The NIST Handbook. (1995).

[51] Valentina Viduto, Carsten Maple, Wei Huang, and David López-Peréz. 2012. A Novel Risk Assessment and Optimisation Model for a Multi-objective Network Security Countermeasure Selection Problem. *Decision Support Systems* 53, 3 (2012), 599–610.

[52] Zikai Wang and Haitao Song. 2008. Towards an optimal information security investment strategy. In *Networking, Sensing and Control, 2008. ICNSC 2008. IEEE International Conference on*. IEEE, 756–761.

[53] Michael E Whitman. 2003. Enemy at the Gate: Threats to Information Security. *Commun. ACM* 46, 8 (2003), 91–95.

[54] John Wunder, Adam Halbardier, and David Waltermire. 2011. *Specification for Asset Identification 1.1*. US Department of Commerce, National Institute of Standards and Technology.

[55] Su Zhang, Doina Caragea, and Xinming Ou. 2011. An Empirical Study on Using the National Vulnerability Database to Predict Software Vulnerabilities. In *International Conference on Database and Expert Systems Applications*. Springer, 217–231.