TRENDY EKONOMIKY A MANAGEMENTU
TRENDS ECONOMICS AND MANAGEMENT
ISSN 1802-8527 (Print) / ISSN 2336-6508 (Online)

2022 39(1): 25–34
DOI: http://dx.doi.org/10.13164/trends.2022.39.25

Comparison of the Most Important Models of Investments in Cyber and Information Security

Lukáš Podešva, Miloš Koch

Abstract

Purpose of the article: Cyber security has become a key factor in determining the success or failure of companies that rely on information systems. However, this entails considerable investment. Typical investments in information technology aim to create value, while investments in cyber security aim to minimise losses caused by cyber-attacks. In the case of investment in cyber and information security, therefore, we must evaluate the amount of loss that will never actually occur. This is a complicated problem, and several approaches have been proposed over the years to estimate the cost-benefit balance of security investments.
Methodology/methods: This paper is based on previous research (Podešva *et al.*, 2021), where two most used methods of the ROI / ROSI (Bojanc, 2008) and Gordon-Loe model (Gordon, Loeb, 2002) were identified in the field of investments in cyber and information security. Both methods are described and the advantages and limitations for further research are identified.
Scientific aim: The main goal is to select the most suitable method for further research in the field of investment in cyber and information security.
Findings: ROI / ROSI does not seem suitable for further research because it only tells us what percentage of return on in-vestment will be provided during a given period. The separate use of this method (ROI / ROSI) provides us with very limited results and it is necessary to combine it with other methods. On the other hand, the Gordon-Loeb model is much more complex despite several limitations, especially for coefficients *ʎ* and *t*. Further research will therefore focus on the constant *t* (probability of attack on a given information set) and its value will be modelled based on the SIR epidemic model on network with standard incidents (Podešva, Koch 2019).
Conclusions: At present, there is no standardised approach to decision-making and the size of investments in cyber and in-formation security. This is a very complex issue, and it is very difficult to find one universal model. Nevertheless, there are several models that help in this decision-making process, and as the most appropriate method for further research is Gordon-Loe model.

Keywords: Return on investment, Return on security investment, ROI, ROSI, Gordon – Loeb Model, Investment, Information security, Cyber security

JEL Classification: M15, M21

Introduction

The development of information and communication technologies in recent years has changed our society into an information society. Information acquires a new meaning and knowledge about the environment, its state, and the processes of gaining in it. Information thus becomes a very valuable commodity that needs to be protected. With the expansion of using computers and the Internet in everyday life, the risk of their misuse increases.

The number of cyber-attacks creates a need for organisations to prioritise certain ways of defending them-selves. Each organisation must consider the threats to which they are most at risk and act to reduce vulnerability across many relevant vulnerabilities. This is a particularly difficult task that many key information security personnel are unable to perform effectively. According to Chronopoulos *et al.* (2018), the main reasons are: (a) lack of budget; (b) uncertainty about the cost of cyber-attacks and the availability of cyber security controls; and (c) non-refundability of expenditure.

Cybersecurity has become a key factor in determining the success or failure of companies that rely on information systems. However, this entails considerable investment. No action is free, and each such investment brings its own return on loss prevention. Typical investments in information technology aim to create value, while investments in cybersecurity aim to minimise the losses caused by cyber-attacks. In the case of investments in cyber and information security, therefore, we must evaluate the amount of loss that will never actually occur. To address information security issues, businesses are forced to invest more in information security. However, previous studies have shown that higher investment in cyber security does not necessarily lead to better outcomes (Cavusoglu *et al.*, 2005; Dor, Elovici, 2016; Feng *et al.*, 2014; Qian *et al.*, 2017).

This is a complicated issue, and several approaches have been proposed over the years to estimate the cost-benefit balance of security investments. The most important and proven models include the return on investment (ROI), respectively. Return on security investment (ROSI) (Bojanc, 2008) and a model proposed by Gordon and Loeb in 2002 (Gordon, Loeb, 2002). Later, the Gordon and Loeb model (Gordon, Loeb, 2002) was extended in several directions; for example, Hausken (2007) used the game theory to simulate the benefits of companies working together to defend against cyber-attacks. Although both approaches are very general, they provide a means of considering whether a security investment is appropriate (worth its price) and help to find the optimal level of security investment.

This article is based on a systematic literature search (Podešva *et al.*, 2021) and will serve as a basis for further research in the field of investment in cyber and information security. First, it explains the principles of both models (ROI / ROSI and Gordon-Loeb model). Then the methods will be compared according to several criteria. Finally, one method is selected, and the direction of further research is described.

1. Literature review

Cybersecurity economics is an area focusing on whether organisations make sufficient investments in security of their assets and whether the budget allocated to security is invested in the right things. Although there has been a significant increase in research in cybersecurity economics, thorough understanding of the safety level, investments in security control and improvements of new controls need to be investigated further since cyber-crime and economic espionage present ever growing problems to businesses.

Return on investment (ROI) is a standard method in the processes of budgeting and evaluating corporate investments and can be quickly applied to the justification of cyber security without the need to modify ROI patterns. In their article, Summer Fowler, Chen (2017) stated that in recent years, more and more Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) have experienced difficulties in justifying cyber and information security investments or expenditures through standard return on investment (ROI) methods. This has led some researchers to design specialised ROI formulas designed to take into account the unique features of cyber security. For example, Markovic-Petrovic, Stojanovic (2014) proposed an improved method for assessing security risks in the event of attacks on the SCADA information and communication infrastructure. Schilling, Werners (2013) have developed a stochastic cloud security risk model to maximise the return on security investment (ROSI). Da Silva, Geus (2015) presented another qualitative and quantitative approach to the calculation of ROSI with regard to tangible and intangible benefits. Although these formulas have their own advantages, they still have difficulties inherited from general ROI concepts.

However, the most important study is Gordon, Loeb (2002), where the authors found the upper limit of investment by a risk neutral company should be 1 / e (36.79%) of the potential loss amount. Another interesting finding is that with increasing vulnerability (as long as certain assumptions about the relationship between company susceptibility and marginal yield from security investments are maintained), the optimum investment in cybersecurity may either increase substantially, or first increase and then decrease. The support for these findings in literature is mixed. However, Hausken (2007) demonstrates that the optimum investment must not be limited to 1 / e by investigating four classes of marginal yields from security investments (decrease, initial increase followed by a decrease, increase, and constancy). Yet the findings of this paper were mentioned by the authors of the Gao *et al.* (2017) study, when they investigated how to determine the investment in security and information sharing of two companies through the function of security failure probability. The publication by Hoang *et al.* (2018) proposes models for conducting an analysis of costs and benefits of investments in security with reduction of anticipated yearly loss and it turns out the upper limit of the optimum investment can be 1 / e, or another percentage of the value at risk, based on the model of cyber threat probability. Thus the Gordon-Loeb modelling hypothesis is adjusted by anchoring to comparative expenses.

Moreover, Gordon *et al.* (2003) found that information sharing may help businesses to achieve the optimal level of cybersecurity and information security at a reduced price. He claims this must be accompanied by suitable motivation mechanisms (on the part of the state) to prevent parasitisation and subsequent insufficient investments in security. Harrington *et al.* (2005) proposed a model of investment optimisation as a non-linear programming problem by means of a cooperative game.

Bakshi, Kleindorfer (2009) demonstrated, using Nash equilibrium and the cooperative game theory, how sharing information concerning investments will lead to increased resilience in global supply chains. Gordon *et al.* (2015) confirmed that sharing results in an increased level of information security. He evaluated the effectiveness of the government role in suppressing the tendency to underinvest in cybersecurity among private sector companies through incentive mechanisms and regulations. They found that government success in increasing private sector company investments depends on: (a) whether the companies can determine an optimal combination of cybersecurity inputs, and (b) whether the companies are able and willing to increase their investments in cybersecurity. However, this finding is not in accordance with Liu *et al.* (2011), where the authors analysed the relationship between an investment in information security and information sharing between two affiliated companies and found that the collaborating companies are naturally motivated to information sharing and co not need any external influence to share the information.

2. Gordon – Loeb model

Gordon and Loeb proposed an economic model for optimising corporate information security investments, where it was found that for a given potential loss, a company may not always invest in information assets with the greatest security risks (Gordon, Loeb, 2002).

The authors (Gordon, Loeb, 2002) further propose a model for companies considering providing additional security to protect a specific information set. The set of information can take many forms, such as a customer list, a commitment book, a strategic plan, or a company website. Enhanced security could be provided to protect the confidentiality, integrity, authenticity, non-repudiation, or availability of the information set to authorised users. The set of information is characterised by three parameters: λ, t, v, which represent the loss due to the occurrence of the intrusion, the probability of the threat and vulnerability.

2.1 Input variables

The λ parameter represents the financial loss of the company caused by a breach of the security of the information file. Loss of confidential data (*e.g.* loss due to disclosure of strategic information to competitors or fraudulent use of credit card information by hackers), loss of integrity (*e.g.* loss due to a corporate decision based on intruder data), and unavailability of services (*e.g.* loss due to missed sales from authorised users who were denied legitimate access). Although λ would normally depend on the use of information (by the company itself, competitors, or hackers) and would change over time, for simplicity the authors consider λ to be a fixed amount estimated by the company (*e.g.* the present value of lost profits from current and future lost sales).

Parameter $t \in (0,1)$ indicates the probability of an attempt occurrence to breach the information set. The authors (Gordon, Loeb, 2002) made a simplifying limitation that there is one threat for a one set of information.

Parameter $v \in (0,1)$ (1, 2) indicates the vulnerabilities of the information set, which means that without additional security, the threat that is implemented will lead to a breach of the set and loss λ.

The threat to the information set and its vulnerability would usually lie within the intervals $0 < t < 1$ and $0 < v <1$. V In the case of $v = 0$, the set of information is completely invulnerable (computer without the Internet access in a safe 50 m underground). Conversely, in the case of $v = 1$, the set of information is completely vulnerable (profit and loss statement available on the Internet).

For a given set of information, the probability of loss (sometimes called the risk of loss) is the result of vulnerability and the probability of a threat. The product $v \cdot t \cdot \lambda$ therefore represents the expected loss (due to no investment in information security) associated with a specific information set. Thus, for any positive threat ($t > 0$), the expected loss increases with vulnerability.

For the purposes of this model, the authors (Gordon, Loeb, 2002) make a simplistic assumption that firms can influence the vulnerability of a set of information (v) by investing in information security, but the firm cannot invest in reducing the threat. Therefore, the probability of a violation attempt (t) is constant, then:

- The parameter $L = t \cdot \lambda$ (1, 2) expresses the loss or potential loss associated with the information set.
- The parameter z (1, 2) represents a monetary investment in security to protect the

information set. The purpose of investing in is to reduce the likelihood that a set of information will be violated.

- The parameter S (z, v) (1, 2) indicates the probability of a security breach. That there will be a breach of a set of information with vulnerabilities in, conditional on the implementation of the threat and because the company has invested in the security of information from to the protection of this information.

2.2 Model principle

In order to determine the amount to be invested in information security for a risk-neutral company, the expected benefits of the investment are compared with the costs. The expected benefits of investing in information security (EBIS), are equivalent to reducing the company's expected loss due to exceptional security (Gordon, Loeb, 2002):

$$EBIS(z) = [v - S(z, v)] \qquad (1)$$

EBIS is written above as a function of z, because the investment in information security is the only variable of the company's decision-making (v and L are the parameters of the information set). Expected net return on investment in information security (ENBIS) equals EBIS less investment costs (Gordon, Loeb, 2002):

$$ENBIS(z) = [v - S(z, v)]\ L - z \qquad (2)$$

2.3 Main benefits

Based on mathematical modelling, the dependence of how vulnerability affects the optimal level of investment in information security was determined, as shown in Figure 1.

The optimal amount spent on information security will never exceed 37% of the expected loss resulting from the security breach (and is usually much less than 37%). Companies should also not focus their investments on files with the highest vulnerabilities, as this is highly expensive.

3. Return on security investment

The method for calculating the return on investment in ROSI security is an extension of the popular accounting metric to compare ROI (Return on investment) investments.

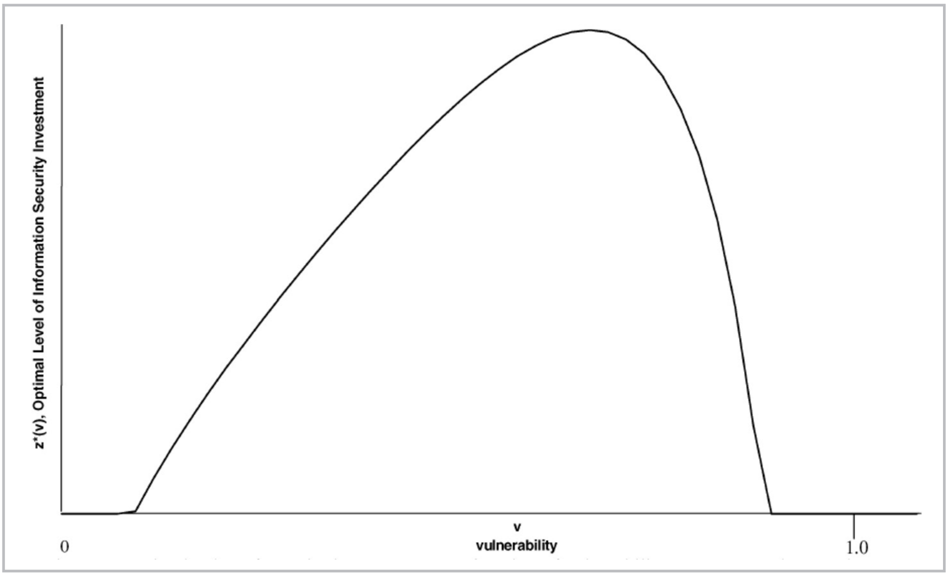

Figure 1. Optimal value of security investments as a function of vulnerability. Source: Gordon, Loeb, 2002.

ROI simply defines how much an organisation gets from the amount of money spent. Therefore, ROI can help an organisation decide which of the possible options provides the highest value for money, as follows from the following formula (Bojanc, 2008):

$$ROI = \frac{Benefits \text{ - } \mathrm{Cos}t\ of\ investment}{\mathrm{Cos}t\ of\ investment} \quad (3)$$

The cost of investing in information security should be considered as a mixture of specific system configuration costs (usually one-off costs of purchasing or developing, testing and implementing a defence solution that protects information assets from potential threats) and operating costs (annual maintenance, updating), and repair of defence solutions, training of users and network administrators, and monitoring of solutions); this value can be obtained very easily (Mizzi, 2005).

On the other hand, it is very difficult to define, assess, or measure the benefits. Firewalls, IDS, antivirus software, and other security solutions simply do not generate measurable revenue. The benefits of investing in information security are therefore measured as the cost savings that result from preventing information security breaches. The benefits can therefore be represented as the difference between the annual expected ALE losses without security investment and the annual expected ALE losses with security investment (Bojanc, 2008):

$$Benefit = ALE_{without\ investment} - ALE_{with\ investment} \quad (4)$$

A simple equation for calculating the return on security investment (ROSI) is as follows (Bojanc, 2008), formula (5).

Calculating the return on investment in security is a very simple and easy-to-use method, ROSI only tells us what percentage of return on investment will be provided over a specified period of time but does not say anything about the scope of the project. The separate use of this method (ROSI) provides us with very limited results and it is advantageous to combine it with other methods, such as Net present value NPV and Internal rate of return IRR (Bojanc, 2008).

4. Analysis of the use of the Gordon-Loeb model and ROSI in the scientific literature

Scientific literature describes many approaches to support the decision-making process for investments in information security and cybersecurity of businesses in organisations. The Web of Science (WOS) and SCOPUS databases were used for this analysis.

4.1 Methodology

A research question was: "*What approaches are described in literature to support the decision-making process for investments in information security and cybersecurity in organisations (with regard to economic factors and mathematical and analytical methods)?*"

Subsequently, keywords were defined (cybersecurity, Information security, economy, investments, costs, finance, benefits, spend, analysis, framework, decision, justification, and evaluation) and based on the words and Boolean algebra, search terms were determined:

(a) Scopus: *((cybersecurity OR "Information security" OR "cyber security" OR "IT security" OR "ICT security")) W / 15 ((economy* OR invest OR investment* OR investing OR cost* OR finance* OR benefit* OR spend) W / 15 (model* OR analysis OR framework OR decision OR justification OR *valuation)).*

$$ROSI = \frac{ALE_{without\ investment} - ALE_{with\ investment} - Cost\ of\ investment}{Cost\ of\ investment} \quad (5)$$

(b) WOS: *((cybersecurity OR "Information security" OR "cyber security" OR "IT security" OR "ICT security")) NEAR ((economy* OR invest OR investment* OR investing OR cost* OR finance* OR benefit* OR spend) NEAR (model* OR analysis OR framework OR decision OR justification OR *valuation))*.

In the SCOPUS database, a total of 579 papers were found; 385 papers in total were found in WOS. Most of the papers were in both databases and after a relevance analysis and duplicity removal, the final number of papers and conference contributions relevant for the research question was 101.

4.2 Findings

Of the 101 articles found that addressed investment models in cybersecurity, 23 used the ROI / ROSI method and 14 used the Gordon-Loeb method (Figure 2).

The most used economic approaches, mathematical methods, and standards that have been used in the scientific literature in conjunction with the Gordon-Loeb model are shown in Figure 3.

The most used economic approaches, mathematical methods, and standards that have been used in the scientific literature in conjunction with the ROI / ROSI model are shown in Figure 3.

5. Conclusion

There is currently no standardised approach for deciding the size of cyber and information security investments. This is a very

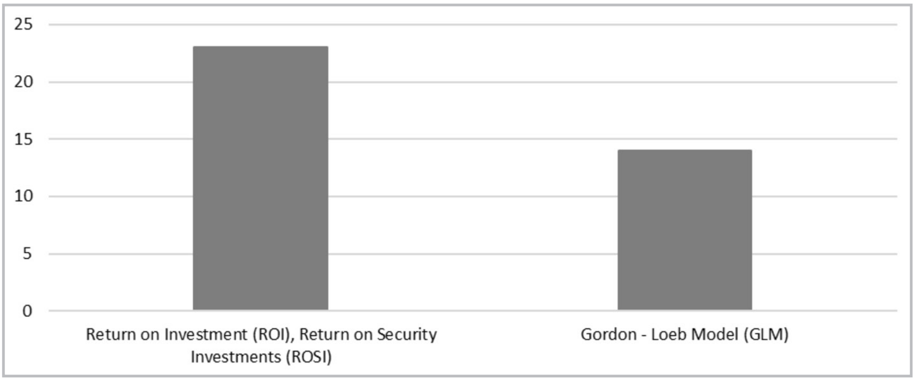

Figure 2. Using the ROI/ROSI and Gordon-Loeb model to evaluate investments in cyber and information security in the scientific literature. Source: own processing.

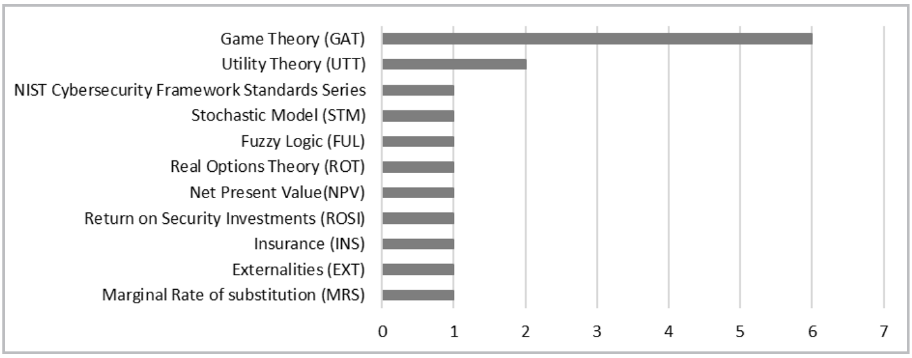

Figure 3. The most used economic approaches, mathematical methods, and standards together with the Gordon-Loeb Model. Source: own processing.

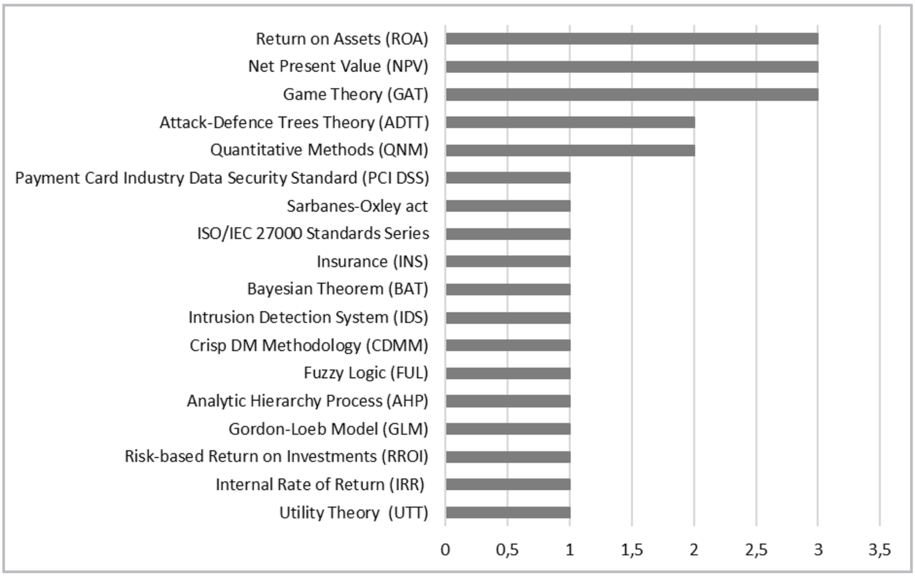

Figure 4. The most commonly used economic approaches, mathematical methods and standards together with the ROI / ROSI Model. Source: own processing.

complex issue, and it is very difficult to find one universal model. Nevertheless, there are several models that help in this decision-making process, and the most important are the Gordon-Loeb model (Gordon, Loeb, 2002) and ROI / ROSI (Bojanc, 2008).

Organisations should invest in security solutions up to the point where net benefits (*e.g.* benefits minus costs) are maximised. In the Gordon-Loeb model, optimal investments in information security range from 0% to 36.8% of potential loss due to security breaches (Gordon, Loeb, 2002). It was later found that in some special scenarios, up to 50% (or even up to 100%) of the average cost is allowed to be invested (Willemson, 2006). This model has also been used successfully in some empirical analyses (Tanaka *et al.*, 2005).

The analysis shows that the ROI / ROSI method is more often used in the scientific literature, mainly due to its simplicity. Nevertheless, this method does not seem suitable for further research because it only tells us what percentage of return on investment will be provided during a given period. The separate use of this method (ROI / ROSI) gives us very limited results and it is advantageous to combine it with other methods, such as Net present value NPV or Internal rate of return IRR (Bojanc, 2008).

On the other hand, the Gordon-Loeb model is much more complex despite several limitations, especially for coefficients λ and *t*. Further research will therefore focus on the constant t (probability of attack on a given information set) will be modeled based on the SIR epidemic model on network with standard incidents (Podešva, Koch, 2019).

Acknowledgment

This article and the results achieved were supported by a grant within the project Quality Internal Grants of BUT (KInG BUT), Reg. No. CZ.02.2.69 / 0.0 / 0.0 / 19_073 / 0016948, which is financed from the OP RDE and by grant FP-S-20-6376 of the Internal Grant Agency at Brno University of Technology.

References

Bakshi, N., Kleindorfer, P. (2009). Co-opetition and Investment for Supply-Chain Resilience. Production and Operations Management, 18(6), pp. 583–603. DOI:10.1111/j.1937-5956.2009.01031.x.

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

Cavusoglu, H., Mishra, B., Raghunathan, S. (2005). The Value of Intrusion Detection Systems in Information Technology Security Architecture. Information Systems Research, 16(1), pp. 28–46. DOI:10.1287/isre.1050.0041.

Chronopoulos, M., Panaousis, E., Grossklags, J. (2018). An Options Approach to Cybersecurity Investment. IEEE Access, 6, pp. 12175–12186. DOI:10.1109/ACCESS.2017.2773366.

da Silva, C. A., de Geus, P. L. (2015). Return on security investment for cloud computing. In Proceedings of the 7th International Conference on Management of computational and collective intElligence in Digital EcoSystems, pp. 156–160. ACM. DOI:10.1145/2857218.2857254.

Dor, D., Elovici, Y. (2016). A model of the information security investment decision-making process. Computers & Security, 63, pp. 1–13. DOI:10.1016/j.cose.2016.09.006.

Feng, N., Wang, H. J., Li, M. (2014). A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. Information Sciences, 256, pp. 57–73. DOI:10.1016/j.ins.2013.02.036.

Fowler, S., Chen, P. P. (2017). CsPI: A New Way to Evaluate Cybersecurity Investments. In 2017 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), pp. 283–284. IEEE. DOI:10.1109/QRS-C.2017.55.

Gao, X., Zhong, W., Mei, S. (2017). A game-theoretic analysis of information sharing and security investment for complementary firms. Journal of the Operational Research Society, 65(11), pp. 1682–1691. DOI:10.1057/jors.2013.133.

Gordon, L. A., Loeb, M. P. (2002). The Economics of Information Security Investment. ACM Transaction on Information and System Security, 5(4), pp. 438–457.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., Zhou, L. (2015). Increasing cybersecurity investments in private sector firms. Journal of Cybersecurity, 1(1), pp. 3–17. DOI:10.1093/cybsec/tyv011.

Gordon, L. A., Loeb, M. P., Lucyshyn, W. (2003). Sharing information on computer systems security: An economic analysis. Journal of Accounting and Public Policy, 22(6), pp. 461–485. DOI:10.1016/j.jaccpubpol.2003.09.001.

Harrington, J. E., Hobbs, B. F., Pang, J. S., Liu, A., Roch, G. (2005). Collusive game solutions via optimization. Mathematical Programming, 104(2–3), pp. 407–435. DOI:10.1007/s10107-005-0622-3.

Hausken, K. (2007). Returns to information security investment: The effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability. Information Systems Frontiers, 8(5), pp. 338–349. DOI:10.1007/s10796-006-9011-6.

Hoang, D. T., Niyato, D., Wang, P., Wang, S. S., Nguyen, D., Dutkiewicz, E. (2018). A stochastic programming approach for risk management in mobile cloud computing. In 2018 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1–6. IEEE. DOI:10.1109/WCNC.2018.8377035.

Liu, D., Ji, Y., Mookerjee, V. (2011). Knowledge sharing and investment decisions in information security. Decision Support Systems, 52(1), pp. 95–107. DOI:10.1016/j.dss.2011.05.007.

Markovic-Petrovic, J. D., Stojanovic, M. D. (2014). An Improved Risk Assessment Method for SCADA Information Security. Elektronika ir Elektrotechnika, 20(7), pp. 69–72. DOI:10.5755/j01.eee.20.7.8027.

Mizzi, A. (2005). Return on information security investment. Are you spending enough? Are you spending too much. ACM IT Security Toolbox.

Podešva, L., Koch, M. (2019). Mathematical and numerical study of a SIR epidemic model on network with standard incidents. In Perspectives of Business and Entrepreneurship Development in Digital Transformation of Corporate Business, pp. 189–197. Brno University of Technology, Faculty of

Business and Management.

Podešva, L., Koch, M., Luhan, J. (2021). Investment models for cybersecurity and information security of businesses – systematic literature review. In the 15th international management conference: Managing People and Organizations in a Global Crisis. Bucharest University of Economic Studies.

Qian, X., Liu, X., Pei, J., Pardalos, P. M., Liu, L. (2017). A game-theoretic analysis of information security investment for multiple firms in a network. Journal of the Operational Research Society, 68(10), pp. 1290–1305. DOI:10.1057/s41274-016-0134-y.

Schilling, A., Werners, B. (2013). A Quantitative Threat Modeling Approach to Maximize the Return on Security Investment in Cloud Computing. In Proceedings of the International Conference on Cloud Security Management, pp. 68–77. Academic Conferences and Publishing International Limited.

Tanaka, H., Kanta, M. (2005). Vulnerability and effects of information security investment: A firm level empirical analysis of Japan. In International Forum of Financial Information Systems and Cybersecurity: A Public Policy Perspective, 26.

Willemson, J. (2006). On the Gordon Loeb Model for Information Security Investment. In 5th Annual Workshop on the Economics of Information Security (WEIS 2006). Robinson College, University of Cambridge.

Received: 20. 1. 2022
Reviewed: 13. 6. 2022
Accepted: 30. 6. 2022

Ing. Lukáš Podešva
Brno University of Technology
Faculty Business and Management
Department of Informatics
Kolejní 2906/4,
Brno, 612 00
Czech Republic
Phone: +420 54114 2601
E-mail: lukas.podesva@vutbr.cz

doc. Ing. Miloš Koch, CSc.
Brno University of Technology
Faculty Business and Management
Department of Informatics
Kolejní 2906/4,
Brno, 612 00
Czech Republic
Phone: +420 54114 2601
E-mail: koch@vut.cz