INVESTMENT MODELS FOR CYBERSECURITY AND INFORMATION SECURITY OF BUSINESSES – SYSTEMATIC LITERATURE REVIEW

Lukáš PODEŠVA[a] *, Miloš KOCH[b], Jan LUHAN[c]

[a,b,c]Brno University of Technology, Czech Republic

ABSTRACT

Science has always been here to respond to present-day problems, to improve people's lives and push borders of human capabilities. The focus of this paper contributes to the issue of cybersecurity and information security of businesses that has been becoming ever more topical with the development of online technologies.

This article analyses current scientific literature that deals with investment models for cybersecurity and information security. Within this systematic literature review, the found models were assessed mostly in terms of the used economic and mathematical methods, and scientific approach. The conclusion presents the main findings, drawbacks and possible directions of further research in the area.

KEYWORDS: *cyber security, information security, cyber-attack, cyber crime, investment*

DOI: 10.24818/IMC/2021/01.03

1. INTRODUCTION

The development of information and communication technologies in recent years has changed our society into an information society. Information has got a new meaning and awareness of the environment its status and ongoing processes has become increasingly important. We can now hardly imagine doing business without the right information, its meaningful processing and evaluation. As early as 1993, Peter Drucker claimed that ***"information is the only meaningful business resource and the other factors of production (labour, land, capital) are only secondary".*** *(Drucker, 1993)*

Thus, information has become a very valuable commodity that needs to be protected. As the use of computers and the Internet in everyday life has become more common, the risk of abuse has also increased, in particular the risk of infecting our device by some kind of a harmful code or it being attacked by hackers. Therefore, it is necessary to understand the importance of computer security and data protection. These days, users are threatened by ever new infiltrations and resourcefulness of the attackers. The number of threats and risks in the digital space increases every year, similarly to the number of successful cyber-attacks. Everyone who currently operates in the digital world is facing a certain risk of becoming a target of cybercrime. In this respect, the risk may not be faced only by individuals or small and medium-sized businesses but also by whole sectors, states and their economies.

Of course, by following certain fundamental rules, these cyber threats can be significantly mitigated. Companies must pay attention to the suitable security of their information and communication technologies and invest a sufficient amount of money in their protection. Cybersecurity economics is the particular area focusing on whether organizations make sufficient investments in the security of their assets and whether the budget allocated to security is invested in

* Corresponding author. E-mail address: lukas.podesva@vutbr.cz

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 cybercrime and economic espionage present ever growing problems to businesses.
The aim of the paper is to analyse current scientific literature that deals with investment models for cybersecurity and information security. Within this systematic literature review, the found models were assessed mostly in terms of the used economic and mathematical methods, and scientific approach. The conclusion presents the main findings, drawbacks and possible directions of further research in the area.

2. LITERARY REVIEW

Cybersecurity economics is an area focusing on whether organizations 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 cybercrime and economic espionage present ever growing problems to businesses.
Literature on optimization of investments in cybersecurity is very limited. The traditional approach is presented in the paper by Bojanc and Jerman-Blažič (2008), proposing a standard method for evaluation of necessary countermeasures in the area of ICT security. The method classifies threats, assets and vulnerable spots of ICT systems by analysing security risks. It shows a quantification of an investment in ICT security, which makes the method applicable for business security risk scenarios.
However, the most important study is Gordon and 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 optimization as a non-linear programming problem by means of a cooperative game.
Bakshi and 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, 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.

3. RESEARCH METHOD

Scientific literature describes many approaches to support the decision-making process for investments in information security and cybersecurity of businesses in organizations. For this reason, a systematic literature review was conducted in SCOPUS and Web of Science (WOS) databases. The research method is shown in Figure 1.

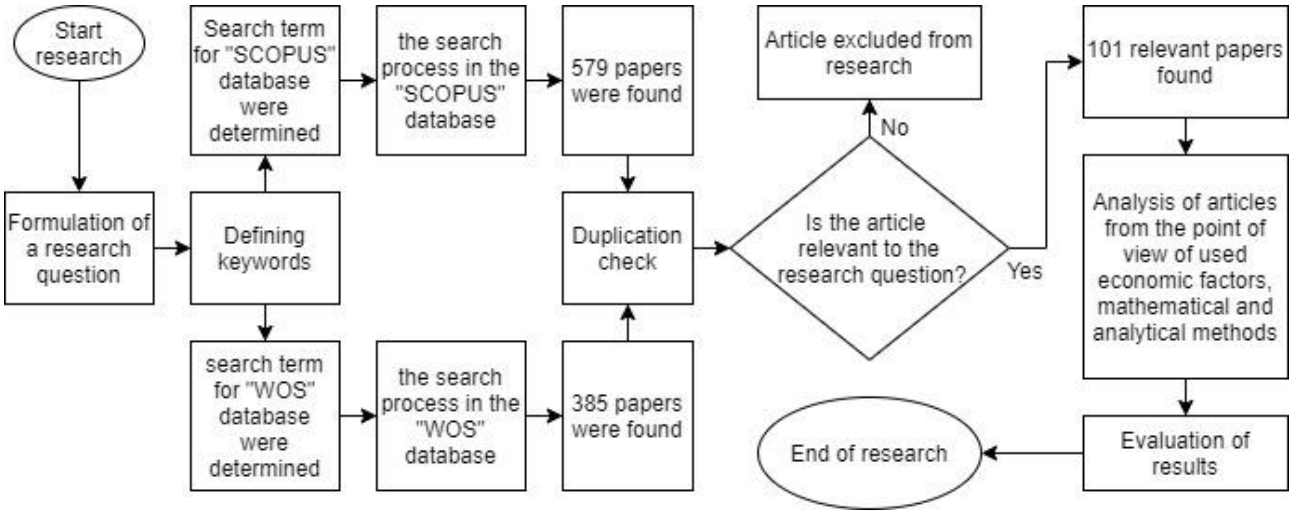

Figure 1. Research method
Source: own processing

First, a research question was posed: **"What approaches are described in literature to support the decision-making process for investments in information security and cybersecurity in organizations (with regard to economic factors and mathematical and analytical methods)?"**
Subsequently, key words were defined (cybersecurity, Information security, economy, investments, costs, finance, benefits, spend, analysis, framework, decision, justification, 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 ((econom* 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)).
(b) **WOS:** ((cybersecurity OR "Information security" OR "cyber security" OR "IT security" OR "ICT security")) NEAR ((econom* 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. The majority of the papers were located 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. CURRENT STATE ANALYSIS

The papers were analysed from several viewpoints, in particular in terms of economic factors and mathematical and analytical methods used in their models. The publications were also assessed based on the main author institution origin; the first thirteen from the total number of twenty-nine countries are shown in figure 2. We can see the dominance of the USA, followed by China and England.
In terms of the general scientific approach to solution of the problem, the publications were divided into three main categories, as shown in figure 3.
It is obvious that the predominant majority of the models have been designed on a purely theoretical basis (92 papers) without empirical verification, 55 papers of which have been supported by mathematical modelling or a simulation. Only 9 papers of all investment models proposed in the evaluated publications were based on empirical research.

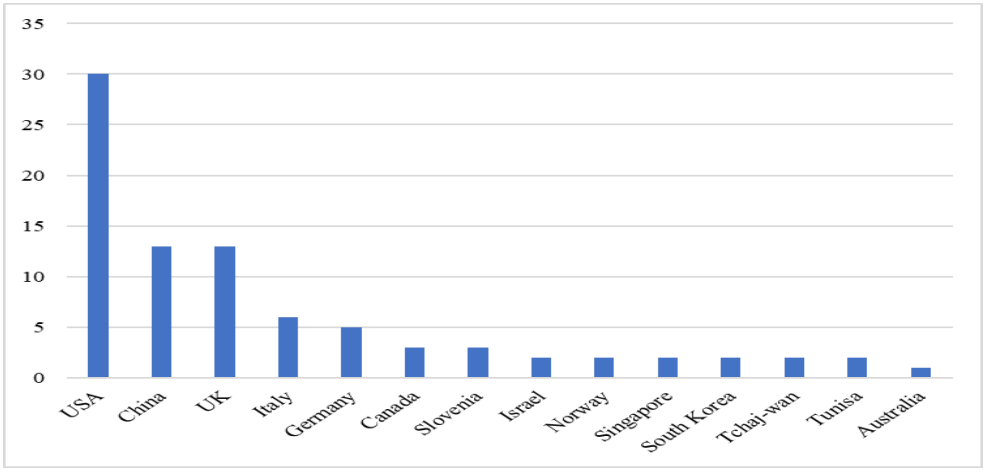

Figure 2. Number of publications based on country of origin
Source: own processing

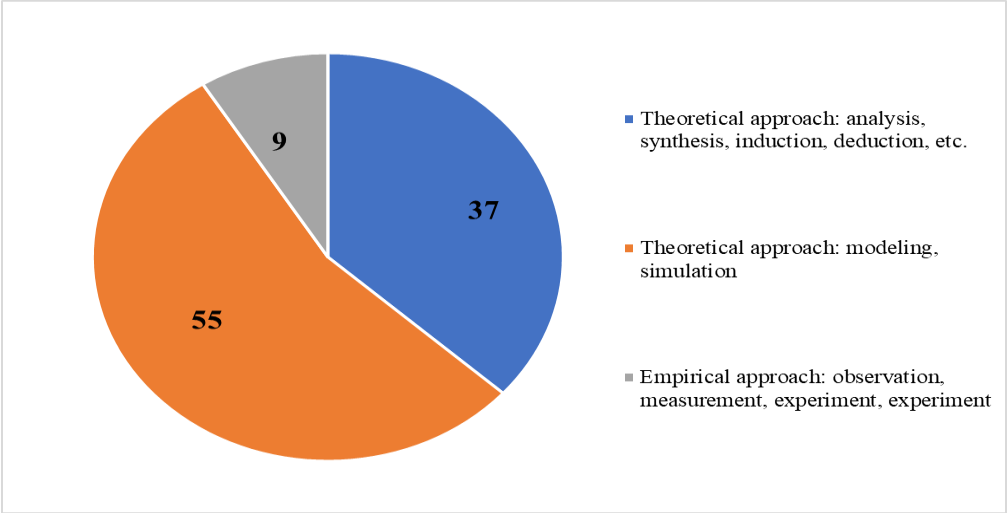

Figure 3. Number of publications based on scientific approach
Source: own processing

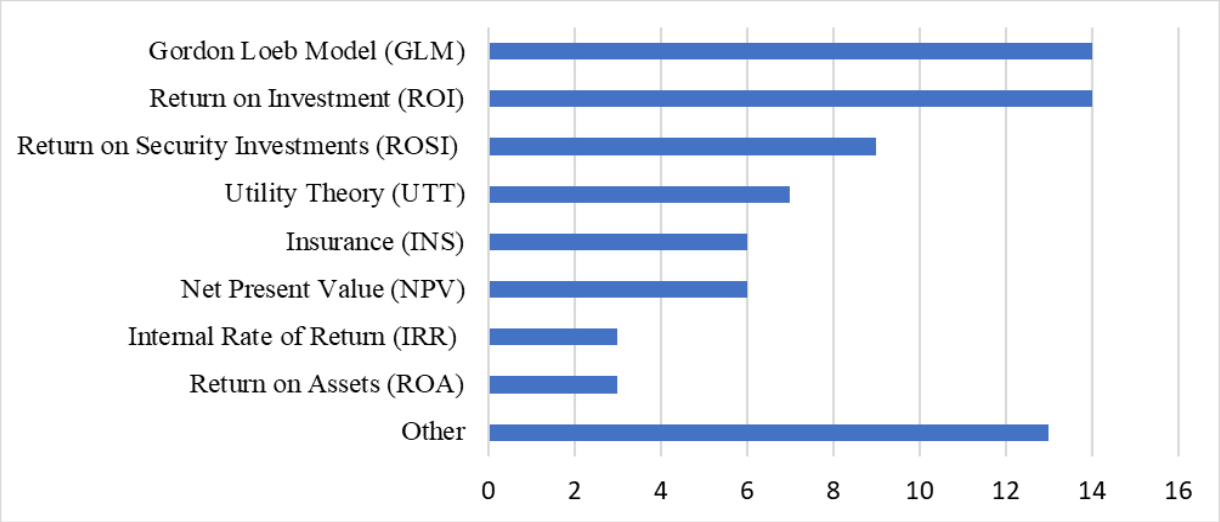

Figure 4. Number of publications based on economic factors
Source: own processing

The evaluation based on the economic factors used in the models to support decision-making on investments in cybersecurity and information security is shown in figure 4. The most common approaches in terms of economic factors include the "Gordon-Loeb model", "return on investment", and the derived "return on investments in security", "utility theory", "net present value" and calculations based on "risk insurance".

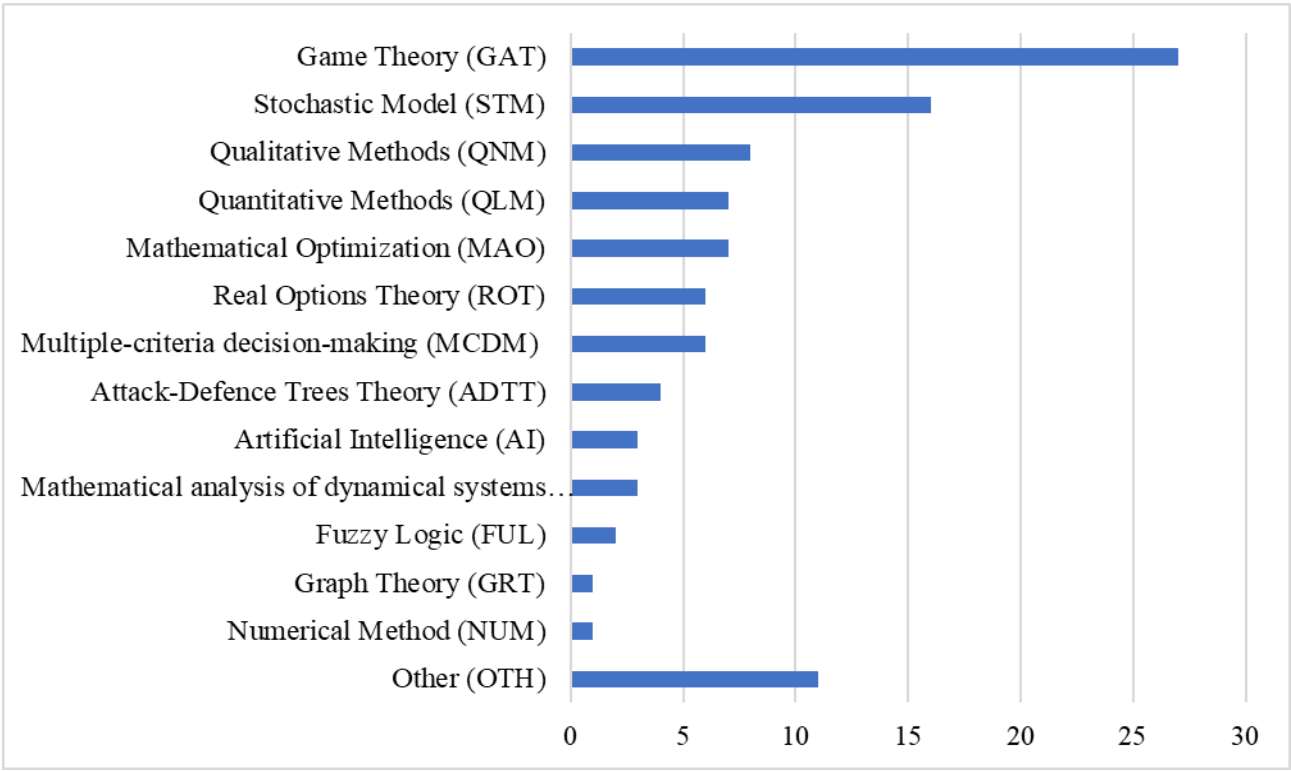

Figure 5. Number of publications based on mathematical and analytical methods
Source: own processing

The most frequently used mathematical approaches include the "game theory" and "stochastic methods (Bayesian Theorem, Bayesians Networks, Markov Chain Monte Carlo, Monte Carlo, Petri Nets, Jump Diffusion, Nonparametric statistics, Binomial Model)", used mostly for simulation and

modelling of phenomena. Others include "quantitative methods" and "qualitative research methods (Grounded theory)" and "mathematical optimization (Lagrange Multipliers, Multiobjective Optimization, Combinatorial Optimisation, Knapsack problem, Particle Swarm Optimization)". Surprisingly, "artificial intelligence" and "fuzzy logic" are used very rarely, as shown in figure 5.
During the literature analysis, no terms related to risk management and the decision-making process were taken into account since the terms from these two areas were present in nearly all of the researched publications

5. CONCLUSIONS

The existing research serves as a research basis and provides research methods for dealing with problems concerning decisions on investments in information security of businesses. It points out the theoretical and practical significance of research on decision-making on investments in business information security. However, due to new issues with business information security, systematic consideration of the effect of inter-business relationships on investments decisions concerning security of business structures.
Based on the conducted systematic literary review, the following findings were revealed:

a) Study results often point out the advantages of cooperation among companies and information exchange in the area (cost reduction and protection enhancement).
b) The results imply the benefits of government interventions in the field of cybersecurity and information security, both in the form of regulations and state aid.
c) It appears it is impossible to find a single universal model for all businesses; the differences will stem mostly from the field of business activity, company size and whether the business is part of critical infrastructure.
d) Only the strategies of defenders (businesses) are simulated, not those of the attackers (hackers).
e) The return on investments in cybersecurity and information security cannot by quantified.
f) A predominant majority of the models have not been empirically verified in a real environment.
g) Some models fail to cover the area as a whole and focus solely on certain aspects (e.g. network security).
h) The proposed models only rarely use artificial intelligence and fuzzy logic.

There are certain limitations to the systematic literature review, mostly due to the fact that only two databased were chosen (SCOPUS and WOS) and only publications in English were analysed. This could have reduced the amount of relevant literature found. However, since the proposed models often applied similar approaches, it can be assumed that the most prominent approaches to the solution of the problem have been included in the review.
To conclude, it can be stated that the literature review confirmed the topicality of the problem of concern. The most significant gap in the scientific research is the fact that artificial intelligence and fuzzy logic are almost unused in this area. This is a very surprising finding as for instance in medicine, and in particular in disease diagnostics, these methods have been used abundantly and their scientific and practical benefits have already been proven. Another gap is the lack of empirical verification of the investment models, mostly replaced by mathematical modelling and simulation. Please read these instructions carefully. Prepare your manuscript exactly according to the instructions. Please use the Template, and insert the text of your paper without alter it. That is the easiest and the most efficient way to have a good published manuscript.

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), 583-603. https://doi.org/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), 216-222. https://doi.org/10.1016/j.csi.2007.10.013

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), 1682-1691. https://doi.org/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), 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), 3-17. https://doi.org/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), 461-485. https://doi.org/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), 407-435. https://doi.org/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), 338-349. https://doi.org/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. https://doi.org/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), 95-107. https://doi.org/10.1016/j.dss.2011.05.007