# ECONOMIC ASPECTS OF CYBERSECURITY

***Lukáš VÁCLAVÍK****

* *Brno University of Technology, Faculty of Business and Management, Czech Republic*

**ABSTRACT**

*The ever-increasing trend of the involvement of various computing tools in the reality of organisations of all sizes brings with it the need to evaluate their security, even in the context of the activities of the entity. Virtually all organisations try to eliminate the cyber risks that arise from the use of various ICT tools by using various security tools. The implementation of these techniques entails costs that need to be justified and evaluated from the perspectives of different stakeholder groups. This text will present selected indicators assessing cybersecurity in terms of he resources invested. In addition to these metrics, selected models evaluating security investments with respect to, among other things, the existence of vulnerabilities and threats will also be presented. As this is a complex discipline, the text concludes by recommending a comprehensive approach to addressing security assurance, taking into account the requirements of the organisation, the value of its assets, the level of vulnerability or the requirements of its stakeholders.*

**KEYWORDS:** *cybersecurity, cyber attack, cyber investment, cyber threats, data security.*

**DOI: 10.24818/IMC/2022/03.02**

## 1. INTRODUCTION

As part of digital transformation, organisations have been making extensive use of a wide range of ICT options. Among the tools used, various mobile devices, cloud services, social media, IoT services and others can be included without a doubt. This fact implies a direct dependence of organisations on these tools as the organisations practically cannot exist in today's world without them. However, these options bring certain risks (Smejkal & Rais, 2013) in addition to the benefits, as the likelihood of an organisation being hit by a cyber-attack with the intention of destroying its physical or information assets increases with the growing number of connected network components. These attacks occur through a number of attack vectors which, in addition to technological ones, include social engineering techniques or insider abuse (Trautman, 2017).
The issue of cybersecurity assurance will require the use of more robust metrics to control and reduce the costs associated with cyber risk management. However, there is currently still no comprehensive standard for measuring and controlling the costs associated with the deployment of cybersecurity tools (Radziwill & Benton, 2017).

## 2 ECONOMIC ASPECTS OF CYBERSECURITY

Cybersecurity economics applies the principles of economics to the analysis of cybersecurity problems. The discipline has recently begun to develop rapidly and has also attracted attention

*Corresponding author: E-mail address*: xvacla21@vutbr.cz*

among legislators. Based on a McKinsey report, cyberspace accounted for 4% of global GDP in 2010 (Moore, 2010).

It is often assumed that information security comes along with technical measures. However, according to (Anderson & Moore, 2006), information security failures are caused by both poor design and poor incentives. This suggests that better incentives are needed to increase investment in cybersecurity.

One of the primary goals in ensuring the security of cyberspace at the national level is the nation's ability to sustain its economic activity through the tools of information and communication technology. Safe maintaining the functionality of key industries that are directly linked to cyber assets is a priority objective for stakeholders around the world. These include the banking sector, the service sector, public administration, etc. (Brangetto & Aubyn, 2015).

### 2.1 Market Challenges for Cybersecurity

This section will present the main economic barriers to effective cybersecurity.

**Externalities**

Economists have been trying to determine whether a socially optimal amount of resources is being invested in cybersecurity. If individuals do not eliminate their private cyber risks, any losses resulting from these risks may be passed on to other users. According to (Moore, 2010), in the IT field, the following types of externalities are generally distinguished:

- **Network externalities** – The value for each individual member increases with the increasing number of members (Windows operating system);
- **Insecurity externalities** – the lack of investment in cybersecurity of the individual may affect the security of others (otherwise there may be a positive externality, when investment in security of the individual creates a higher level of security for others);
- **Interdependent security** externalities – if the individual's investment creates a positive externality for others, which discourages them from investing in their own investment and they "parasitise" on this investment.

**Information Asymmetry**

The information systems of today are characterized by a huge amount of data whose accuracy and reliability is difficult to determine in practice. This problem can be observed in estimates of the cost of cybercrime due to the lack and inaccuracies of data. The root cause is that the affected organisations tend to hide or possibly underreport the data. This may be due to concerns about reputational damage or the discovery of any lingering vulnerabilities.

**Incentives**

There is very little empirical evidence of incentives in relation to cybersecurity demonstrating positive or negative externalities (Bauer & van Eeten, 2009). Companies that choose to disclose threats and weaknesses in their systems may often be encouraged to do so through certain legislative incentives. Yet others may be deterred from disclosing this information because of risks such as reputational and trust damage or the impact on financial markets (Brangetto & Aubyn, 2015).

### 2.2 Government Interventions

There is an ongoing debate in the professional community about whether to label cybersecurity as a public or private good (Taddeo, 2019). At the same time, the question arises whether government intervention is necessary and justified to regulate this market. Even though individuals, businesses and to some extent governments have made investments in this area, it cannot be left to the private sector alone to address the issue. This is especially true in the area of cybersecurity of a country's critical infrastructure. The situation has allowed some governments to justify their intervention by various means (regulatory, supervisory, coordinating or financial) (Brangetto & Aubyn, 2015).

Economic theory distinguishes between private and public goods. Public goods are characterised by their non-excludability in consumption and also by the fact that their use by an individual does not prevent their use by others. Private goods, on the other hand, are the exact opposite.
One problem with public goods may be the "stowaway" paradox, whereby these individuals use a public good without contributing to it. However, the opposite situation may also occur, where individuals live under the belief that there will never be enough contributors to a given public good, and therefore avoid contributing to it (Kianpour et al., 2022).
Cybersecurity is usually considered a private good that is sold by private entities to customers, such as governments, private companies, and individuals. However, certain types of cybersecurity solutions exhibit the characteristics of a public good. These may include information about threats and vulnerabilities related to new and evolving cyber attacks. Misunderstanding of the concept of public goods explains the reluctance to share information and is often reflected in legislative and regulatory initiatives (Brangetto & Aubyn, 2015).

### 2.3 Cybersecurity Measurement

When deciding whether or not a particular security measure should be used, traditional models often use a cost-benefit analysis of the investment in question. This will determine whether the investment is justified, i.e. whether its benefits ultimately outweigh its costs. Or rather, what the difference between these values is. For organisations, estimating direct and indirect costs is as problematic as estimating benefits. Especially if tangible benefits cannot be estimated. Nevertheless, in order to use this model, it is necessary to know and determine these values. This fact combined with uncertainty often leads to an approach where companies reactively make security investments only after a data breach or leak (Brangetto & Aubyn, 2015).

**Return On Security Investment (ROSI)**

As mentioned above, each organisation must decide how much it wishes to invest in cybersecurity. The use of the standard ROI indicator, i.e. the evaluation of the return on investment, suggests itself. In this case, however, its use is not appropriate, as investments in cybersecurity do not generate profit, but they do prevent potential losses. For this purpose, the ROSI indicator was created as a key identifier for organisations to measure the effectiveness and efficiency of IT security spending against its benefits. It allows an organisation to assess whether it is investing enough resources in security and whether or not the investment is cost-effective.
For such an assessment, the amount of potential loss that can be avoided by the investment in security must be quantified against the monetary amount of the investment to reduce the risk.
The quantification of risk can be performed using the following formula:

$$ALE = Single\ Loss\ Expectancy\ (SLE) * Annual\ Rate\ of\ Occurence\ (ARO) \quad (1)$$

where:

- **SLE**.tangible and intangible loss expectancy
- **ARO**.annual rate of occurrence

The ROSI model then combines a quantitative risk assessment and the cost of implementing security for a particular risk. There are many other models based on this indicator, which reflect various other factors (Brangetto & Aubyn, 2015).

The basic ROSI calculation is as follows:

$$ROSI = \frac{(ALE * risk\ mitigated) - cost\ of\ security}{cost\ of\ security} \quad (2)$$

where:

- **risk mitigated**...estimated effectiveness of the security solution [%]

These calculations are usually based on metrics that have been collected from within the organisation or from external sources. However, this data from external sources may be deliberately distorted, for example to avoid reputational damage. Similarly, calculations can easily be influenced by subjective perceptions of risk and its value to suit their users in order to justify their decision (Brangetto & Aubyn, 2015).

**Total Return on Investment (TROI)**

Purser also sees ROI as more of a measure of the efficiency of using capital to generate profits. He argues that the process of improving information security enhances the value of an organisation by reducing the level of risk associated with that information and information systems.

The resulting formula is as follows:

$$TROI = \frac{Generated\ revenue + Generated\ cost\ savings - Value\ of\ change\ in\ risk}{Investment} \quad (3)$$

where all input variables are measured in the same monetary units.

The use of this indicator allows an organisation to put its information security management initiative on the same level as other business initiatives in an effort to achieve a positive value for this indicator. It is also useful to distinguish between tactical and strategic initiatives with regard to compliance with various legal and regulatory requirements. The tactical initiatives are driven by short-term business opportunities and allow the organisation to act quickly, while the strategic ones are driven more by the requirement to establish a certain risk profile for the whole organisation. However, according to him, the return on investment (ROI) analysis is clearly a general policy prerequisite for the approval of most IT investments (Purser, 2004).

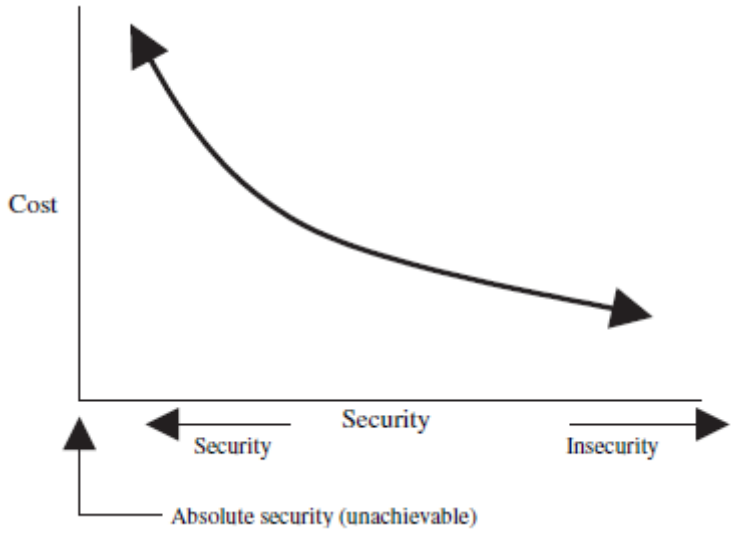


**Figure 1: Correlation between cost and safety**
*Source:* (Tsiakis & Stephanides, 2005)

Figure 1 is a summary of the information security and information systems cost problem. As

The level of security increases, the cost of the security increases exponentially towards a state of perfect security (100%).

**Other Metrics**

In general, given the significant investment in cybersecurity by both the private and public sectors, it is important to determine what metrics to use in decision-making and how to assess the effectiveness of such metrics. Cybersecurity strategies should generally implement additional metrics, beyond those already mentioned.

In the case of government cybersecurity strategies, these include:

- cost effectiveness;
- useful information sharing;
- positive and negative impacts on security level;
- costs for businesses;
- economic growth in the use of the Internet and the economy.

Some believe that concepts such as basic human rights should be included in these metrics. Others would like to measure the level of international participation before and after the policy introduction. Several assessment methods have been published by ENISA and provide an overview of the different options and key performance indicators for measuring the effectiveness of national cybersecurity strategies (Brangetto & Aubyn, 2015).

## 2.4 The Gordon-Loeb Model

Gordon and Loeb discussed the economics of investing in information security. In 2002, they created a theoretical economic model that determines the optimal amount to invest in protecting a given set of information. The model takes into account the vulnerability of information to breach and the amount of potential loss. They came up with the idea that it is not economical to concentrate investments on the information files with the highest vulnerability, as such protection can be extremely costly. Allegedly, protecting files with medium vulnerability would be a better option. As regards the amount of investment in protecting this information, they argue that the optimal amount should not exceed 37% of the expected loss resulting from its theft. Since their research only represents a theoretical basis that is not supported by empirical data, they themselves at the end of their publication call for verification by real data obtained from organisations (Gordon & Loeb, 2002).

They also addressed the issue of implementing the NIST Cybersecurity Framework, which has become law for U.S. government agencies and companies that want to work with these organisations. This cybersecurity framework has been adopted by organisations around the world. In their work, they focused on the ratio of costs incurred to benefits obtained in implementing the higher tier of the framework. Together, they created the Gordon-Loeb Economic Model (GL Model) to help organisations find the right level of investment in cybersecurity. It assesses the value of protected information and its vulnerabilities, including threats, as security investments increase.

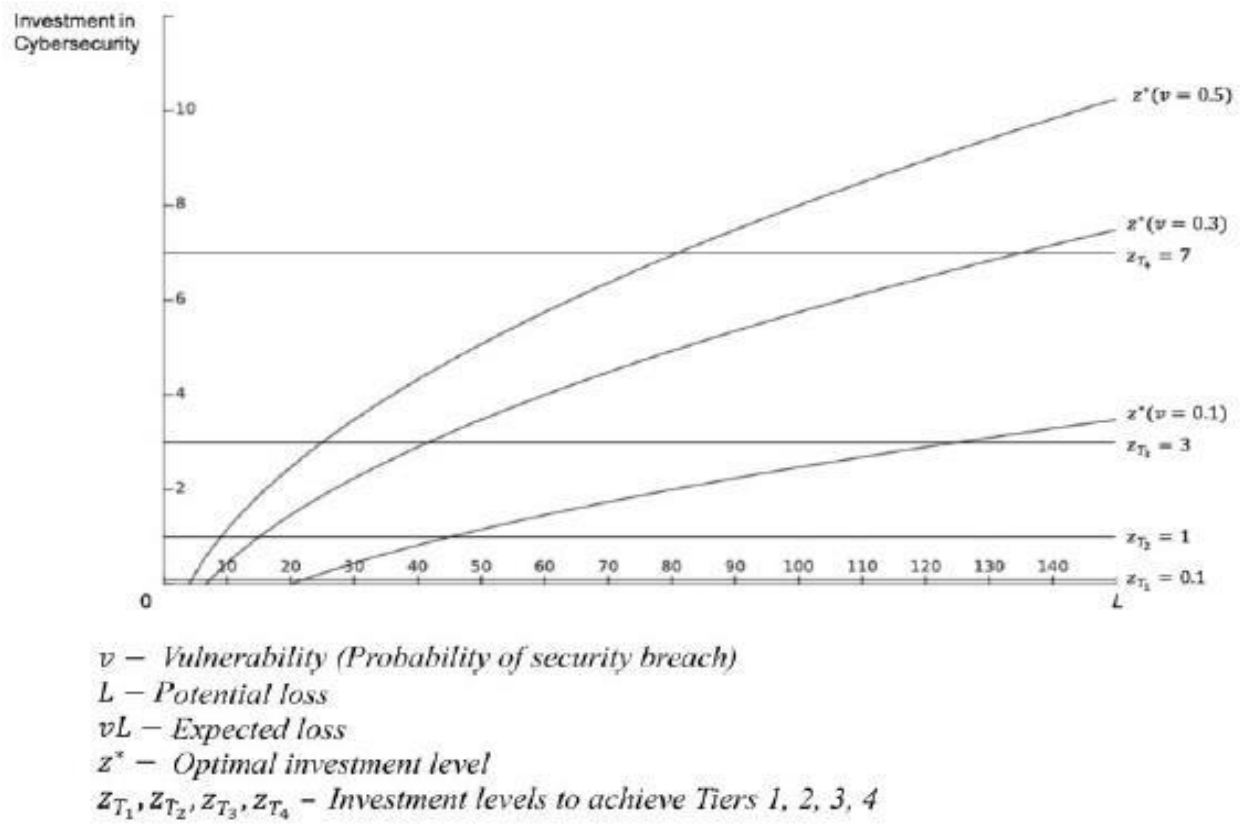


**Figure 2. Optimal cybersecurity investment value for each tier of the NIST framework**
*Source:* (Gordon et al., 2020)

Together, they have thus created a framework for decision-making in selecting an organisation's security level (Tier 1–4) to follow. This certainly makes the often difficult decisions easier for businesses and managers. At the beginning, the value of the protected information (L) and the probability of a security breach (v) must be determined. Based on this, the graph in Figure 2 can be used to derive the suitability of using the framework and the optimal amount of investment in security (Gordon et al., 2020). However, this is still a theoretical framework that would need to be tested on real data from organisations.

### 2.5 Gilligan's Model

Gilligan talks about the fact that cyber attacks using less sophisticated techniques may not always have the most significant economic impact. However, they represent the largest number of attacks and experience shows that a potential attacker will usually take the path of least resistance. He also notes that organisations are interested in protecting their most critical data and functions. They therefore prefer to invest in protecting these rather than protecting low-value data and functions. Higher priority data protection investments are shown in Figure 3 on the right.

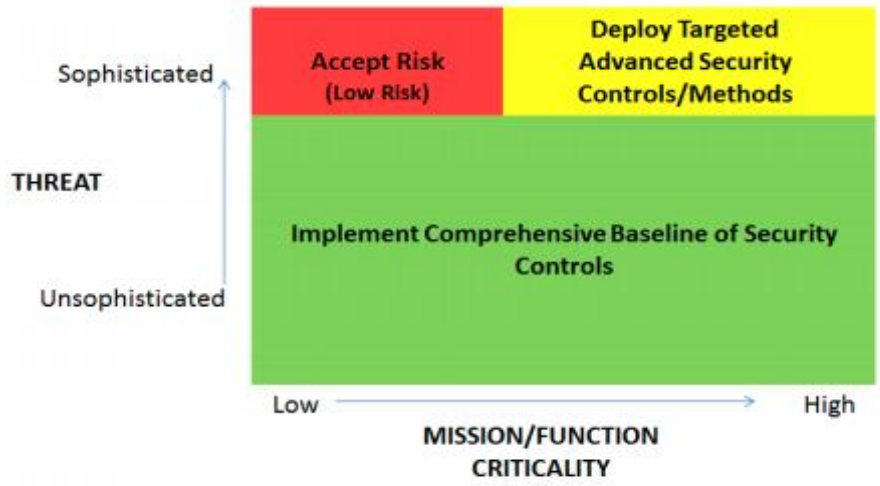


**Figure 3: Gilligan's Cybersecurity Model**
*Source:* (Gilligan, 2013)

This model highlights several principles that should guide decision-making when investing in cybersecurity. The first principle is that it is economically viable to implement a comprehensive base level of security that protects against low and medium intensity threats. The second principle is to target additional investments to protection of data and functions that are most beneficial to the organisation. As the third principle, he refers to the fact that an organisation should accept the risk of unprotected data and functions in sophisticated attacks if the data are unimportant and the cost of protecting them would outweigh the benefit of protecting them (Gilligan, 2013).
Douglas Kelly focused on the issue of cybersecurity from a more microeconomic point of view and also builds on Gillian's model, among others. He addressed the issue of market failure due to information asymmetry, IT externalities and government regulations. He argues that the reason why the profits from cybercrime are so high is, among other things, the uncertain cost of protection against cybercrime. He also mentions that without a precise understanding of the economics of the risks of cyber attacks and defence against them, investments in this sector will be inefficient and insufficient (Kelly, 2017).

## 3. DISCUSSION AND CONCLUSIONS

According to Cybersecurity Ventures, one of the world's leading cybersecurity researchers and contributors, the predicted global cost of fighting cybercrime is $6 trillion per year. Compared to 2015, this represents a 100% increase in the annual expenditure. The prediction was supported by universities, government agencies and private companies around the world (*The Hot 150 Cybersecurity Companies To Watch In 2020*, 2019). However, this also means that the price of these specialists will rise in the future, and with it the cost of protecting systems from cyber attacks. In the U.S., the public and private sectors have suffered from a persistent shortage of knowledgeable cybersecurity professionals for several years (*The Hot 150 Cybersecurity Companies To Watch In 2020*, 2019). This will entail the need to develop a certain methodology for organisations that will be forced to implement appropriate methods and procedures to protect their data in their information systems of various types.
In primarily private sector organisations, it is often difficult to convince managers to invest their own resources in processes that do not generate additional profit. In this respect, the situation becomes even more complex when dealing with people who have any direct interest in the financial

performance of the company. These include direct owners, shareholders, managers, as well as other employees rewarded according to results or savings.

Under these circumstances, explaining the information risks of systems, even if they work with sensitive company data, can be very difficult. Organisations need to understand the value of their data versus the cost of protecting them and determine which data are critical to them. These data should be protected as a matter of priority. On the contrary, to effectively allocate resources to data and system protection, it is also necessary to determine which data are not essential for the organisation and its functioning. Next, it is necessary to define the level of sophistication of cyber attacks the data are supposed to be protected from, again taking into account the importance and criticality of the data. The framework according to (Gilligan, 2013) can serve as a helpful tool. In general, for significant data, protection against threats and attacks of lower sophistication is economical, too. This is because attackers often resort to attacks by way of "lesser resistance". According to the GL model, the optimal amount invested in cybersecurity of information should not exceed 37 % of the expected loss resulting from its theft (Gordon et al., 2020).

To assess whether an organisation is investing sufficient resources in data protection, ROSI can be used, combining a quantitative risk assessment with the cost of implementing security for a specific risk. Alternatively, TROIs can also be used. For individual stakeholders, quantification in the form of such an indicator represents a higher level of clarity when making decisions concerning this type of security. However, many studies report that company executives are much more likely to be guided by their own intuition than by real data (Bullini Orlandi & Pierce, 2020). This fact may therefore complicate the issue. Unfortunately, for specialists and experts within an organisation, early warnings of cybersecurity risks can go unheeded until an adverse event actually happens. This has been evidenced by the increasing frequency of data leaks of organisations, including user data (Swinhoe, 2021).

To prevent cybercrime along with reducing the success rate of attackers, sharing data on cyber threats and incidents among organisations is advisable. However, the realization of this vision is hampered by the reluctance of individual entities to share the data in question for various reasons. They may fear various risks in the form of reputational damage, loss of customer trust and more. It is not only for this reason that a stronger role of the state and government interventions to define requirements in the field of cybersecurity, as is already the case for example in the field of critical infrastructure, may and does suggest itself.

In the case of cybersecurity strategies, it is advisable to take a comprehensive approach to this issue. Other extension metrics (Brangetto & Aubyn, 2015) may be used, with respect to the characteristics and protection requirements of the entity.

## REFERENCES

Anderson, R., & Moore, *T. (2006).* The Economics of Information Security. Science, 314(5799), 610-613. https://doi.org/10.1126/science.1130992

Bauer, J., & van Eeten, M. (2009). Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy*, *33*(10-11), 706-719. https://doi.org/10.1016/j.telpol.2009.09.001

Brangetto, P., & Aubyn, M. (2015). Economic aspects of national cyber security strategies. In Dr. *Mustafa AFYONLUOGLU* - Kişisel Web Sitesi. NATO Cooperative Cyber Defence Centre of Excellence. https://afyonluoglu.org/PublicWebFiles/library/ccdcoe/LIB_0021.pdf

Bullini Orlandi, L., & Pierce, P. (2020). Analysis or intuition? Reframing the decision-making styles debate in technological settings. Management Decision, *58(*1), 129-145. https://doi.org/10.1108/MD-10-2017-1030

Gilligan, J. (2013). The Economics of Cybersecurity: A Practical Framework for Cybersecurity Investment. AFCEA Cyber Committee. Retrieved 2021-06-16, from https://www.afcea.org/mission/intel/documents/EconomicsofCybersecurityFinal10-24-13.pdf

Gordon, L., & Loeb, M. (2002). The economics of information security investment. ACM Transactions on Information and System Security, *5*(4), 438-457. https://doi.org/10.1145/581271.581274

Gordon, L., Loeb, M., & Zhou, L. (2020). Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model. *Journal of Cybersecurity*, *6*(1). https://doi.org/10.1093/cybsec/tyaa005

Kelly, D. (2017). The economics of cybersecurity. Reading: Academic Conferences International Limited. Retrieved from https://www.proquest.com/conference-papers-proceedings/economics-cybersecurity/docview/1897683119/se-2

Kianpour, M., Kowalski, S., & Øverby, H. (2022). Advancing the concept of cybersecurity as a public good. *Simulation Modelling Practice and Theory*, *116*. https://doi.org/10.1016/j.simpat.2022.102493

Moore, T. (2010). Introducing the Economics of Cybersecurity: Principles and Policy Option. Proceedings *of a Workshop on Deterring Cyberattacks:* Informing *Strategic* and Developing Options for US policy. https://cs.brown.edu/courses/csci1800/sources/lec27/Moore.pdf

Moore, T. (2010). The economics of cybersecurity: Principles and policy options. International Journal of Critical Infrastructure Protection, *3*(3-4), 103-117. https://doi.*org/10.*1016/*j*.ijcip.2010.10.002

Purser, S. (2004). Improving the ROI of the security management process, *23*(7), 542-546. https://doi.org/10.1016/j.cose.2004.09.004

Radziwill, N., & Benton, M. (2017). Cybersecurity Cost of Quality: *Managing the* Costs of Cybersecurity Risk Management. https://arxiv. org/ftp/arxiv/papers/1707/1707.02653. pdf

Smejkal, V., & Rais, K. (2013). *Řízení rizik ve firmách a jiných organizacích* (4., aktualiz. a rozš. vyd). Grada.

Swinhoe, D. (2021). The 15 biggest data breaches of the 21st century. In CSO | Security news, features and analysis *about prevention, protection and business innovation.*. CSO. https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

Taddeo, M. (2019). Is Cybersecurity a Public Good?. *Minds and Machines*, *29*(3), 349-354. https://doi.org/10.1007/s11023-019-09507-5

The Hot 150 Cybersecurity Companies To Watch In 2020. (2019). Retrieved 2020-05-11, from https*://cybersecurityventures.com/the-hot-150-cybersecurity-companies-to-watch-in-2020/*

Trautman, *L. (2017). Industrial Cyber Vulnerabilities: Lessons* from Stuxnet and the Internet of Things. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2982629

Tsiakis, T., & Stephanides, G. (2005). The economic approach of information security, *24*(2), 105-108. https://doi.org/10.1016/j.cose.2005.02.001