JOURNAL OF EASTERN EUROPEAN AND CENTRAL ASIAN RESEARCH
Vol.11 No.3 (2024)

ASSESSMENT OF CYBERSECURITY IN ORGANIZATIONS: AN EMPIRICAL STUDY OF CZECH AND SLOVAK ORGANIZATIONS

Katerina Petrova
Department of Management, Faculty of Business and Management, University of Technology, Brno, Czech Republic

Jan Spatenka
Department of Information Technology, Faculty of Business and Management, University of Technology, Brno, Czech Republic

Lukas Vaclavik
Department of Information Technology, Faculty of Business and Management, University of Technology, Brno, Czech Republic

ABSTRACT

The purpose of this research is to evaluate how companies approach cybersecurity, which measures the companies set, and how it is reflected in relation to organizational learning. A questionnaire was distributed electronically among 124 IT and IS professionals working in companies based in the Czech and Slovak Republic. Hypotheses were tested using the chi-square test of independence, the Mann–Whitney U test, and the Pearson correlation coefficient. The results depict that cybersecurity is a fundamental topic for most companies. Unless companies declare the importance of cybersecurity, they do not tend to set and use security rules unless they are not under security laws. Research shows that costs for cybersecurity are variable, not fixed, and are in correlation with the size of the company and the turnover.

Keywords: cybersecurity; cybercrime awareness; ISMS; organizational learning; ISO 27001

DOI: https://doi.org/10.15549/jeecar.v11i3.1666

INTRODUCTION

Cybersecurity has become a crucial topic for organizations in today's technology-driven world. With the rise of digitalization and the prevalence of e-commerce, organizations have become increasingly reliant on technology to carry out their daily operations. As mentioned by Zheng & Sun (2022), digitalization and digital ownership increase the value of companies, especially if they are focused on internationalization. Digitalization, as defined by Brynjolfsson and McAfee (2014), involves the conversion of analog processes into digital formats, facilitating storage, manipulation, and transmission via electronic devices. On the other hand, digital ownership, elucidated by Lessig (2004), pertains to the legal rights and control over digital assets and intellectual property in virtual environments. This dependence on technology has opened up new vulnerabilities and threats, making cybersecurity a top priority for organizations across all industries.

Cybersecurity, encompassing the protection of computer systems, networks, and electronic devices from unauthorized access and malicious activities, has become paramount. Cybersecurity threats can come in various forms, including malware, viruses, phishing attacks, social engineering, and ransomware. These threats can result in significant financial losses, reputational damage, loss of sensitive data, and legal liabilities for organizations and departments.

The growing sophistication and frequency of cyberattacks have made it imperative that organizations take proactive measures to protect their assets and data. This has led to the emergence of cybersecurity as a crucial component of organizational strategy, requiring a comprehensive approach that involves people, processes, and technology.

In today's rapidly evolving digital landscape, cybersecurity threats have become increasingly sophisticated and frequent, posing significant risks to an organization’s operations, reputation, and financial stability. Therefore, ensuring effective cybersecurity is critical to an organization’s success. However, cybersecurity is not just a technical issue; it is a strategic concern that requires a comprehensive approach that involves people, processes, and technology. Additionally, effective cybersecurity requires a strategic approach that aligns with the organization’s overall strategy. Thus, cybersecurity should be an integral part of its strategic plan, reflecting its mission, vision, values, and goals. By embedding cybersecurity into the organization's strategy, it can ensure that cybersecurity considerations are taken into account in all decision-making processes, from resource allocation to risk management.

Against this backdrop, this study examines the actual state of cybersecurity in Czech and Slovak organizations, highlighting the importance of organizational learning to promote employee awareness of cybersecurity to ensure its effectiveness within the organization. The research focuses on typical incidents that occur during a cyberattack to assess to what extent these incidents vary depending on the security measures and employee learning.

This paper aims to analyze the approach of companies to cybersecurity, its reflection on organizational learning, and experience with cyberattacks, their aftermaths, and measures against these attacks.

To achieve its objective, the paper adopts a quantitative methodology, employing a questionnaire to gather insights from a diverse sample of respondents. The analysis involves processing descriptive-statistical data and applying various analytical techniques, including the chi-square test, Mann-Whitney U test, Pearson's correlation coefficient, and multinomial regression analysis. The paper unfolds in a structured manner, commencing with a theoretical exploration of organizational learning, strategy, cybersecurity, and ISMS. Subsequent sections delve into the methodology, results, and conclusion, with the aim of providing empirical insights into the nexus between organizational factors and cybersecurity efficacy. Although the analysis of relevant studies has shown that factors such as awareness and knowledge of cyberthreats (Alanazi et al., 2022), cybersecurity behaviors (actions taken by an individual to prevent or reduce cyberthreats that they may be susceptible to, such as utilizing protective software, refraining from accessing unsafe websites, being cautious, and data backup), user skills, subjective norms, perceived threat severity, attitude, and behavioral intentions (Mayer et al., 2017) influence the level of cybersecurity, there is not enough evidence to claim how significantly organizational learning and strategic planning affect the level of cybersecurity. Due to these inconsistencies, which are mostly perceived primarily from an uncomplex view of company size, emphasis on organizational education, and information security management systems, the need for comprehensive training programs and robust cybersecurity measures has become increasingly vital. Therefore, the goal of this study is to explore how various factors, such as organizational and technical measures, influence the efficiency of cybersecurity and to what extent incidents related to cyberattacks vary depending on the security measures and organizational learning. Additionally, the proposed hypotheses aim to examine the relationship between an organization’s emphasis on organizational learning and cybersecurity awareness, the level of technical and organizational measures to ensure cybersecurity and to examine the organization's approach to cybersecurity and take proactive measures to implement specific investments as security countermeasures.

By scrutinizing the proposed hypotheses and research questions, the study endeavors to explain the relationship between organizational characteristics, cybersecurity practices, and incident response. Ultimately, the goal is to enrich empirical understanding, paving the way for informed decision-making and enhanced cybersecurity strategies in organizations across diverse sectors.

This leads to the main research areas:

- Research question 1: How deeply are companies focused on organizational learning to ensure employees' awareness of cybersecurity?
- Research Question 2: What technical and organizational measures are used to ensure cybersecurity?
- Research Question 3: What typical incidents befall when a cyberattack occurs?

This pilot study, conducted in the Czech and Slovak Republic, analyzes the phenomenon and challenges of aspects of cybersecurity and helps to understand the relationship between company size, emphasis on organizational learning, and elements of information security management system (ISMS).

LITERATURE REVIEW

Organizational learning

Organizational learning is a critical component of effective cybersecurity, as it helps organizations develop a culture of continuous improvement and adaptability to address new and emerging cyberthreats. Organizational learning is defined as "the process by which an organization acquires, creates, retains, and transfers knowledge, and modifies its behavior to reflect new knowledge and insights" (Argote & Miron-Spektor, 2011). One key aspect of organizational learning is knowledge creation, which involves the development of new knowledge through experimentation and exploration (Nonaka & Takeuchi, 1995). In the context of cybersecurity, the creation of knowledge can involve the development of new cybersecurity policies, procedures, and protocols, as well as the implementation of new technologies to mitigate cyber risks. Another essential aspect of organizational learning is knowledge retention, which involves the storage and retrieval of knowledge within an organization (Argote & Miron-Spektor, 2011). Knowledge retention can be facilitated through the development of knowledge management systems that allow organizations to capture and share knowledge between departments and teams. This involves upholding efficient team collaboration structures and fostering a positive culture of sharing and cooperation founded on equitable relationships within the organization (Nguyen et al., 2023).

Furthermore, organizational learning can be facilitated through the use of social learning processes, which involve the sharing and transfer of knowledge among individuals within an organization (Bandura, 1977). Social learning processes can involve mentoring, coaching and training programs that allow employees to learn from one another and develop new skills and knowledge. Organizational learning is a critical component of effective cybersecurity, as it enables organizations to continuously improve their cybersecurity posture and adapt to new and emerging cyberthreats. By fostering a culture of continuous learning and improvement, organizations can develop the knowledge, skills, and capabilities needed to effectively manage cyberrisks and protect their assets and data (Hornungova, 2022).

Information and Cybersecurity

Within the concept of Industry 4.0, organizations aim to create an intelligent factory that integrates technologies and implements automatization to continue the improvement of the working environment. The main effort of organizations is to ensure cybersecurity in corporate cyberspace (Milichovsky, 2023). In the era of Industry 4.0, where interconnectedness and digitization are paramount, organizations should adapt their organizational learning strategies to keep pace with evolving cyberthreats. With the integration of IoT devices and interconnected systems in Industry 4.0 environments, employees need to be increasingly aware of the cybersecurity risks associated with these technologies. Therefore, understanding how organizations prioritize and implement organizational learning initiatives in the context of Industry 4.0 is crucial for addressing cybersecurity challenges effectively. Technical measures such as encryption, network segmentation, and intrusion detection systems, as well as organizational measures like establishing cybersecurity policies and procedures, are essential in safeguarding Industry 4.0 environments against cyberthreats. Understanding the specific measures adopted by organizations within the Industry 4.0 context provides valuable insights into cybersecurity practices tailored to contemporary technological landscapes.

The primary objective of information security is to ensure business continuity and mitigate business losses by preventing and reducing the potential impact of security incidents (von Solms, 1998). According to the International Standard ISO/IEC 27002:2005, information security is achieved by implementing a suitable array of measures, such as policies, processes, procedures, organizational structures, and software and hardware functionalities. These measures are implemented, monitored, reviewed and enhanced as needed to maintain the confidentiality, integrity, and availability of information and to meet specific security objectives. Within the scope of this standard, information may take many forms, such as a paper record or a record on electronic media, and it may be transmitted in the form of mail, electronic media, or conversation (ISO/IEC 27002:2005 2005).

The concept of cybersecurity encompasses various definitions, including one presented by ISO/IEC 27032:2012, which describes it as the collective endeavor to preserve the confidentiality, integrity, and availability of information within cyberspace. Although cybersecurity and information security are closely related and overlap in some respects, they are not synonymous. Information security generally focuses on the protection of information, while cybersecurity focuses on the protection of information in cyberspace.

Thus, in general, cybersecurity safeguards digital assets, encompassing network resources, hardware, and information that is processed, stored, or transmitted through interconnected information systems (Anon, 2015). Thus, we can say that information security includes cybersecurity as one of its components (von Solms & von Solms, 2018), and the Internet is identified as the main domain for the application of cybersecurity.

Information Security Management System

The Information Security Management System (ISMS), as defined by ISO/IEC 27001, takes a comprehensive and coordinated approach to address an organization's information security risks. It establishes a framework for implementing an extensive set of security measures within the broader context of a comprehensive management system. It is important, however, to recognize that the effectiveness of technical security measures is limited and should be complemented by appropriate management practices and procedures. A successful ISMS relies on the support and involvement of all employees within the organization, as well as stakeholders, suppliers, and other external parties (ISO/IEC 27002 2005). It uses a risk management process and is a strategic decision for the organization, influenced by its needs and objectives. The main benefits to organizations through ISO/IEC 27001 compliance include ensuring the cost-effectiveness of security risks, ensuring compliance with laws and regulations, security awareness among managers and employees, or some form of mutual assurance among business partners through certification (ISO/IEC Standard 27001 2023).

METHODOLOGY

The paper deals with the research on the relationship between organizational characteristics, organizational learning, strategy, and Information Security Management Systems in Czech and Slovak organizations. Its main aim is to identify how the type and size of the organization, the level of learning, and the existing strategy influence the concept of ISMS. The pilot study highlights the importance of organizational aspects in evaluating the security level in the Czech and Slovak Republic as an initial study.

The methodology employed is a quantitative approach, using a questionnaire, with primary data collected through an online survey tool. The questionnaire reflects the complex view of ISMS in organizations based on 5 subcategories: prevention of risks in security, investing in cybersecurity, methodology for working with data, user authorization, and detecting the efficiency of cybersecurity. This system assesses the level of protection of the information system and determines recommendations to balance the weakest part. The questionnaire consists of 7 questions divided into two sections: organizational learning and the information security management system. The sample collected consists of 124 respondents who are representatives of companies from the Czech and Slovak Republics. The survey, conducted in 2022, targeted various sizes of organizations. To link the survey with company size, respondents had to include their company in one of seven size intervals.

In terms of data analysis, the initial phase involved processing the descriptive-statistical data. Subsequently, various analytical techniques were used, including The chi-square test, Mann-Whitney U test, Pearson's correlation coefficient, and multinomial regression analysis with a significance level of p<0.05. Data was analyzed using SPSS software.

Pearson correlation coefficient

The correlation coefficient is used to measure the intensity of linear dependence. The Pearson correlation assesses the strength of the relationship between two variables and ought to be used only for quantitative variables, whereas Spearman or Kendall coefficients are suitable for ordinal variables.

Correlation coefficients, in general, acquire values within the interval of -1 to 1: whereas 0 means linear independence, positive values denote positive dependence, and negative values mark negative correlation. It is also important to note that the Pearson coefficient cannot achieve the value of 1, which needs to be taken into account when interpreting the power of dependence. The Pearson correlation coefficient test can only be applied if the variables can be assumed to be samples from a bivariate normal distribution (Molnár et al., 2012).

Table 1. Interpretation of the correlation coefficient by Schober et al. (2018)

The value of the correlation coefficient	Interpretation
0.00 – 0.10	Negligible correlation
0.10 - 0.39	Weak correlation
0.40 – 0.69	Moderate correlation
0.70 – 0.89	Strong correlation
0.90 – 1.00	Very strong correlation

Source: Schober et al. 2018.

The Chi-square test of independence

The chi-square test is nonparametric or distribution-free, and its purpose is to test hypotheses involving nominal variables. Chi-square is a robust statistical tool with an emphasis on the distribution of the data. It stands apart from most other statistics in that it not only determines the significance of any differences detected but also allows the present detailed information on which specific groups contribute to any differences found. The chi-square test has assumptions that must be met for appropriate use and should always be paired with a suitable strength test. It allows for the evaluation of nominal or ordinal variables, unequal sample sizes, or data that violate the assumptions of a parametric test, such as a seriously skewed or kurtotic distribution or violations of equal variance or homoscedasticity. Additionally, chi-square can be used when continuous data are divided into small groups, rendering the data no longer an interval or ratio (McHugh, 2013).

Mann–Whitney U test

The Mann-Whitney U test, also known as the Wilcoxon rank sum test, is used to compare two independent groups that have an ordinal or continuous dependent variable without requiring a specific distribution. While the Mann-Whitney U test is often considered the nonparametric alternative to the independent t-test, this is not always the case. Unlike the independent-samples t-test, the Mann-Whitney U test allows for different conclusions based on assumptions about the data's distribution. These conclusions can range from determining if the two populations differ to identifying differences in medians between groups; the specific findings depend on the shape of the data distributions. The Mann-Whitney U test is commonly referred to as the nonparametric version of the parametric t-test (McKnight & Najab 2010).

Research model

Currently, cybersecurity is crucial for organizations in the digital age to protect themselves against various threats, such as cyberattacks, data breaches, and theft of sensitive data. Furthermore, the cost of cybercrime is increasing year by year and can lead to several consequences, such as financial losses, loss of reputation, legal liabilities, and decreased customer trust. In an environment where information security is indispensable, most organizations are not aware of the value of information. In determining the key factors that cohere with the efficiency of ISMS and influence the security level, a research model can be constructed to analyze various variables and their impacts on the overall effectiveness of information security management systems.

Organizational learning ensures effective cybersecurity practices in the organization. Cyberthreats are constantly evolving and becoming more sophisticated, so it is essential to have a continuous learning approach to stay up with the latest trends and techniques in cybersecurity. By promoting a culture of learning, employees can be more aware of potential risks and vulnerabilities and improve the skills necessary to prevent and respond to cyber incidents.

The implementation of an ISMS involves the establishment of policies, procedures, and controls to manage the organization's information security risks. These measures aim to protect the organization's sensitive information and critical assets from unauthorized access, theft, or damage. As a result, it is reasonable to assume that organizations with a well-implemented ISMS would have a higher level of security than those without such a system. In addition, an ISMS can provide a framework for continuous improvement in information security practices, which can further enhance the organization's security posture over time. Therefore, organizations that have implemented an ISMS will have a higher security level than those that have not. Regardless of these detections, the following three hypotheses are formulated:

H1: There is a positive relationship between an organization’s emphasis on organizational learning and cybersecurity awareness.

H2: Companies using a higher level of technical and organizational measures to ensure cybersecurity will have a lower rate of cyber incidents.

H3: Organizations that perceive cybersecurity as important and take proactive measures to implement specific investments as security countermeasures are more likely to have a positive organizational attitude towards preventing cybersecurity incidents compared to those who do not prioritize cybersecurity or take reactive measures.

In order to test various hypotheses a hypothetical-deductive methodology is followed that relies on quantitative data gathered from a survey (Arsenault, 2011; Yin, 2012). The hypothetical-deductive approach, mostly used in the social sciences, has proven effective and employs techniques like structural equation modeling (SEM), partial least squares (PLS), and their combination (Nguegang Tewamba et al., 2019).

RESULTS

The results of the research are divided into three main areas - description of the investigated data sample, organizational attitude, countermeasures to prevent cybersecurity incidents, and statistically processed data from the questionnaire survey. The second section is related to organizational attitude reactions to research questions; the last section, where the survey data are statistically processed, corresponds with three given hypotheses.

Description of the investigated data sample

This section contains a description of companies involved in the questionnaire survey and their elementary characteristics from the perspective of company size according to the number of employees and the implementation of ISO 27001 associated with the Information Security Management System.

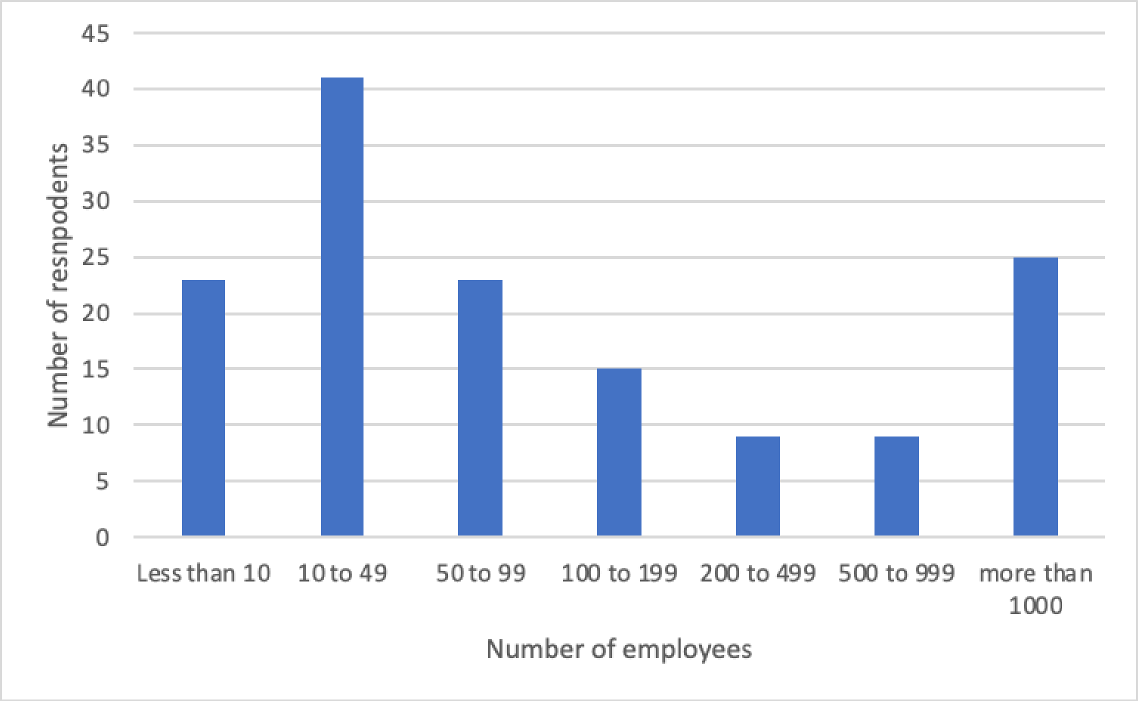

Figure 1. The number of respondents differentiated according to the size
Source: own design.

The results of the questionnaire survey are limited geographically and time-wise. The study draws upon the responses of participants from companies located in the Czech Republic and Slovakia collected in the year 2022. Different company sizes are distinguished, as they are supposed to have an essential influence on the results of the survey.

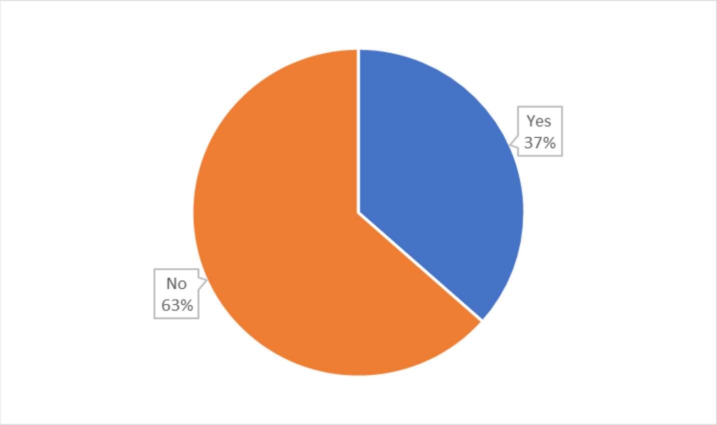

Figure 2. Percentage of ISO 27001 (ISMS) implemented
Source: own design.

To illustrate the profile of the surveyed organizations, 37% of the surveyed organizations have an Information Security Management System (ISMS) according to ISO/IEC 27001, while 63% do not.

Organizational attitude and countermeasures to prevent cybersecurity incidents

This section presents the results of the questionnaire survey related to cybersecurity importance, organizational learning approach, technical and organizational measures against cyberattacks, the occurrence of cyberincidents, and their aftermaths.

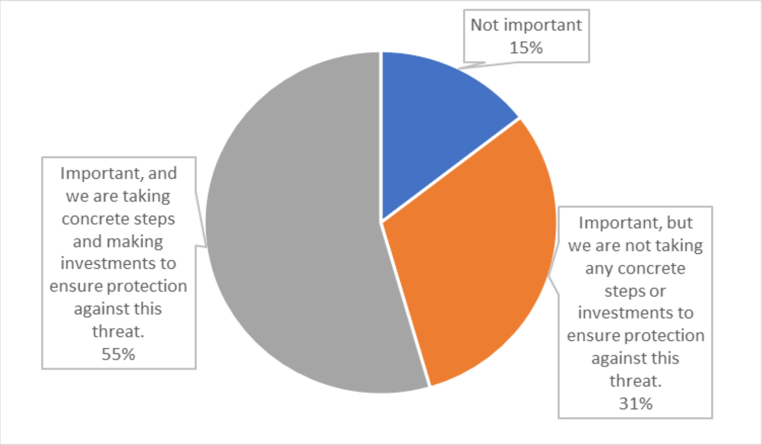

Figure 3. Importance of Cybersecurity

Source: own design.

Figure 3 shows the perspective of organizations or their management on the issue of cybersecurity. Only 15% of respondents do not see this issue as important. The rest of the organizations perceive the threat as important. However, only 55% of the respondents take a proactive role in implementing specific investments as a form of security countermeasures.

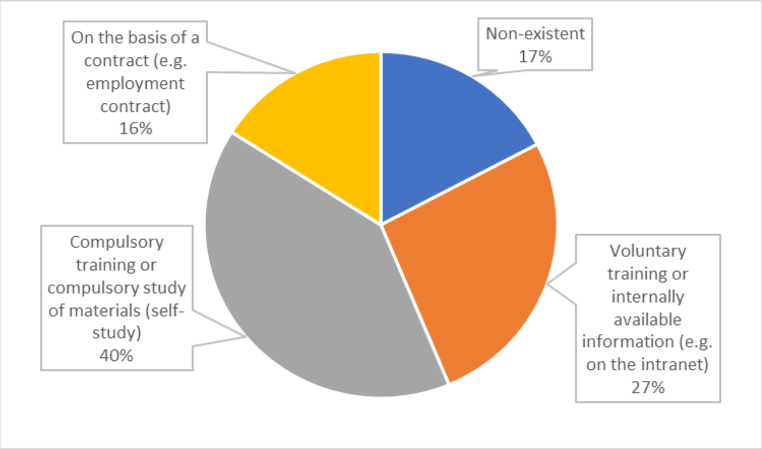

Figure 4. Organizational learning approach to ensuring employees' awareness of cybersecurity

Source: own design.

Figure 4 relates to research question no. 1 and illustrates the approach of the organizations surveyed to ensure awareness of cyber and information security issues among their employees. 17% of the organizations stated that they do not ensure awareness among their employees in this area. In 27% of cases, awareness of these issues is provided through voluntary training or internally available information provided, for example, via the organization's intranet. 40% of organizations include training or studying relevant material (including self-study) in this area as one of the employee's duties, while in 16% of cases, this is included directly in the contractual arrangement between employer and employee (e.g., employment contract).

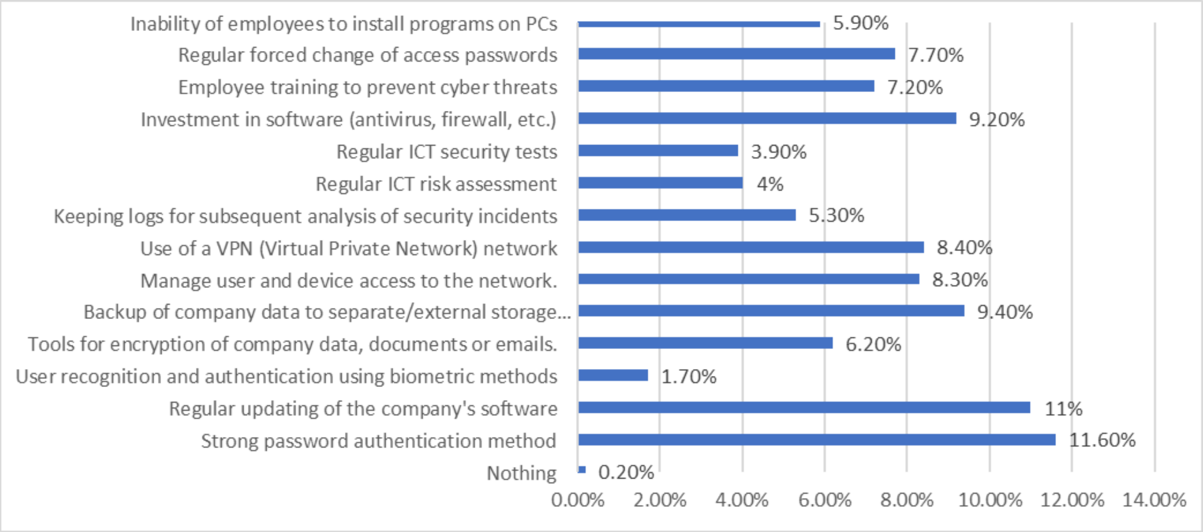

Figure 5. Technical and organizational measures used to ensure cybersecurity
Source: own design.

An answer to research question no. 2 is based on Figure 5, from which it can be concluded that the surveyed organizations overwhelmingly use some measures to ensure ICT security, as only a negligible part of them answered that they do not use any. Only a small percentage of the organizations surveyed use biometric methods such as fingerprint, facial, or voice recognition to authenticate users. This may be influenced by the higher acquisition cost of such technology or the general lack of requirements for such a security method. The organizations surveyed make extensive use (11.6%) of the best-practice policy of strong passwords (a combination of uppercase and lowercase letters, numbers, and special characters) to authenticate access to computers, networks, or applications, with regular enforcement of changes (7.7%). In 11% of cases, organizations carry out regular software updates, and 9.2% make regular investments in security software (antivirus, firewall, etc.). Other security measures used include backing up company data to separate/ external storage, including cloud backups (9.4%) or employee training (7.2%) as a prevention against cyberthreats affecting the human factor of the organization. Other related measures include preventing the installation of programs on employee PCs (5.9%) or the existence of user and device network access management (8.3%). 8.4% of organizations use a Virtual Private Network (VPN) for remote access to data.

Less-used security measures (only 3.9%) are regular ICT security tests in the form of penetration tests or backup system tests. The same findings are observed for the regular ICT risk assessment (4%). The storage of logs for subsequent analysis of past security incidents in only 5.3% of the organizations confirms the fact that they do not have sufficient capacity of security experts for the relevant assessment and prevention of future incidents.

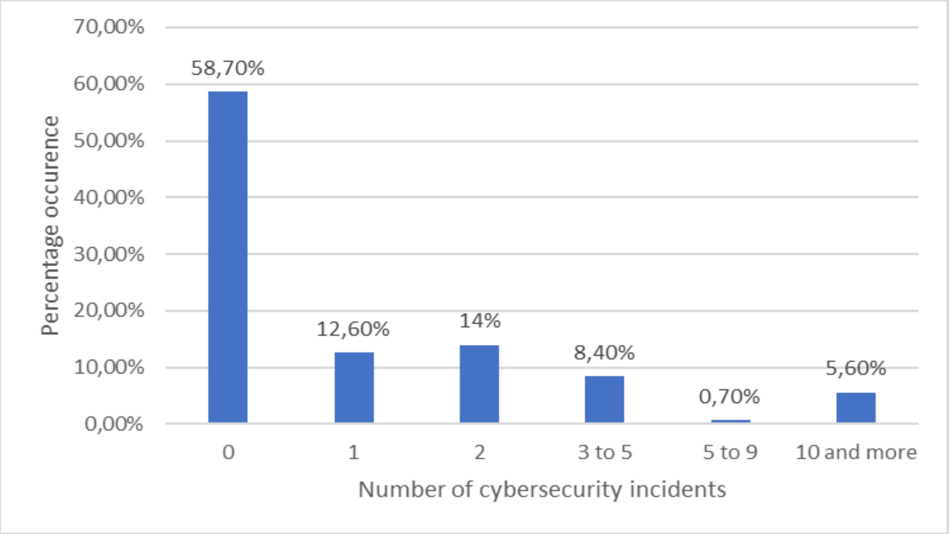

Figure 6. The occurrence of cyberincidents according to the number of incidents in last 3 years
Source: Own design.

The frequency distribution of the number of cyberattacks on the organizations surveyed in the last 3 years can be observed in Figure 6. The vast majority of organizations (58.7%) did not experience any cyberincidents during this period; however, 12.6% and 14% of organizations had encountered one and two incidents, respectively. A total of 9.1% of organizations reported a number between 3 and 9 incidents, and 10 or more incidents were reported by 5.6 % of them.

Organizations affected by a cyberattack reported that in 38.2% of cases, there were no significant problems or loss of essential data. Only a total of 2 cases experienced substantial issues related to the loss of critical data to the organization's operations.

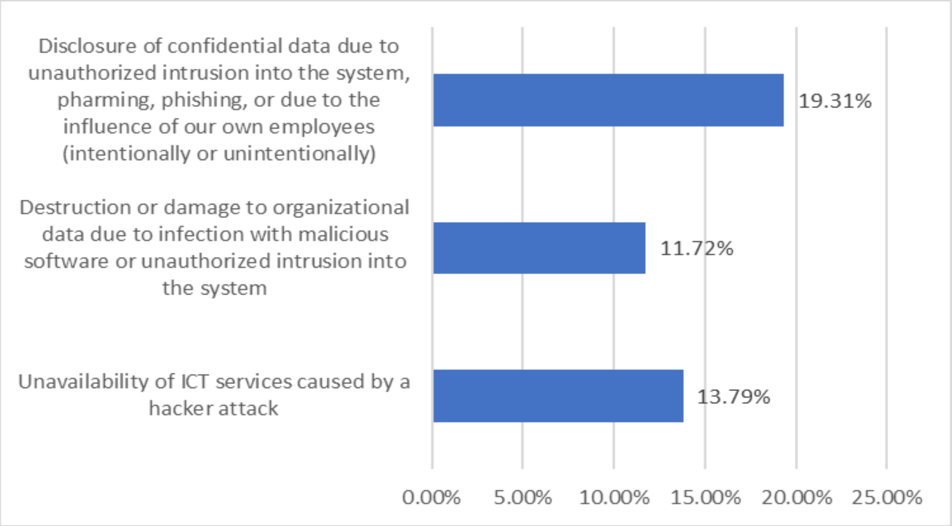

Figure 7. Percentage of impact of cybersecurity incidents in last 3 years
Source: own design.

The responses of organizations to the occurrence of 3 basic types of incidents in the last 3 years can be seen in Figure 7. The inaccessibility of ICT services due to hacker attacks (e.g., DoS/DDoS attacks) affected 13.79% of organizations. Destruction or damage to the organization's data due to malware infection (e.g., ransomware) or unauthorized intrusion into the system affected 11.72 % of respondents. The most common security incident (19.31%) observed among the respondent group was the disclosure of confidential data as a result of unauthorized intrusion, pharming, phishing, and intentional or unintentional disclosure by the organization's employees.

Statistically processed data from the questionnaire survey

The Chi-square test of independence

The chi-square independence test reveals whether two variables are likely to be related or not. Specifically, the relationship between companies falling under cyber law and the existence of security rules is analyzed.

Table 2. Relationship between the fact that the company falls under the cyberlaw and the existence of security rules evaluated by chi-square tests

The value of the correlation coefficient	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	16.718**	3	<.001
Likelihood Ration	17.948	3	<.001
Linear-by-Linear Association	16.577	1	<.001
N of Valid Cases	143		<.001

**. 2 cells (25.0%) have an expected count less than 5. The minimum expected count is .42.

Source: own design.

Table 2 includes the results of the χ2 test of independence. The value of the test criterion for the classic Pearson χ2 test is 16.718. The value is compared to the critical value of the χ2 distribution, listed in the column of asymptotic significance. If the value is lower than the chosen significance level of the α test, then we reject the null hypothesis, and the alternative hypothesis is accepted. In this case, the p-value for the classic Pearson's χ2 test is lower than 0.001, so at a significance level of 5%, the null hypothesis about the independence of the company falling under the cyberlaw and the existence of security rules is rejected and the alternative hypothesis (H1) is accepted.

Mann–Whitney U test

The nonparametric Mann-Whitney U test determines whether there is equality or inequality between the means of two samples. The null hypothesis determines there is no difference between end-user education support for organizations that have faced a cyberattack and those that have not encountered a cyberattack.

Table 3. Correlation between cyberattack-facing organizations and higher declaration of organizational learning in the field of cybersecurity

	End-user education support
Mann – Whitney U	1563.50
Wilcoxon W	3103.5
z	-3.368
Asymp. Sig. (2-tailed)	<.001

Grouping Variable: faced a cyberattack

Source: own design.

With a p-value of less than 0.001, the null hypothesis (H2) is rejected that there is a relationship between end-user education support and the circumstances surrounding cyberattacks experienced by the organization can be inferred.

Pearson correlation

The Pearson correlation coefficient assesses the strength and direction of the linear association between two variables, specifically the number of employees and the annual cost of IS security. The value .709 indicates that the variables are tightly grouped around the imaginary line; the correlation is significant at the 0.01 level. The 2-tailed significance value is less than .001 and indicates that the correlation is highly significant, not just a function of the random sampling error. The null hypothesis (H3), therefore, is supported, indicating a substantial correlation between the variables.

Table 4. Correlation between the number of employees and the rising costs of cybersecurity

		Number of employees	Annual cost of IS security
Number of employees	Pearson Correlation	1	.709**
	Sig. (2-tailed)		<0.001
	N	143	143
The annual cost of IS security	Pearson Correlation	.709**	1
	Sig. (2-tailed)	<0.001	
	N	143	143

**Correlation is significant at the 0.01 level (2-tailed).

Source: own design.

Results reveal that the strength of a linear relationship between the annual cost of IS security and annual turnover is .652. The variables of interest exhibit a positive correlation. From a translation of the correlation coefficient into descriptors, it can be concluded that a moderate correlation exists between the variables. The low level of significance indicates whether it is not a random coincidence of variables. The null hypothesis (H3) is supported, indicating a moderate correlation between the variables.

Table 5. Correlation between company turnover and cybersecurity budget

		Annual cost of IS security	Annual turnover
Annual cost of IS security	Pearson Correlation	1	.652**
	Sig. (2-tailed)		<0.001
	N	143	143
Annual turnover	Pearson Correlation	.652**	1
	Sig. (2-tailed)	<0.001	
	N	143	143

**Correlation is significant at the 0.01 level (2-tailed).

Source: own design.

DISCUSSION

Due to the length of the data collection period, the research affected by the experience of the participants before and with the pandemic can be observed and compared. This aspect can be a suggestion for further research, and it is appropriate to follow up on the response and target how an unprecedented situation (such as the pandemic) can influence the attitude toward the level of cybersecurity within organizations.

There are several interesting research results. It is obvious from Figure 3 that cybersecurity is a crucial area in which companies focus their attention. This is also manifested in the approach to organizational learning in connection with the extension of end-user knowledge in the field of cybersecurity (see Figure 4). This figure also answers research question no. 1 - there is no doubt that companies are strongly focused on organizational learning in the field of cybersecurity. More than 80% invest in compulsory or voluntary learning of employees in this area.

On the other hand, companies probably do not deal with the issue systematically because – as is shown in Figure 2 - only 37% of the companies successfully implemented ISO 27001 of ISMS. From this point of view, the results of H1 made by the chi-square test are also surprising. Even though companies declare the importance of cybersecurity, there is a strong dependence between companies under the cyberlaw and the existence of security rules to ensure cybersecurity awareness. This means that the others do not tend to set and use security rules to such an extent. In answer to research question no. 2, it is obvious that companies mostly react to cyberthreats through a strong password authentication method and regular updating of the company's software.

The fact that more than 40% of companies have already faced a cybersecurity attack in the last three years has been strongly manifested in a desire to enlarge organizational learning related to the cybersecurity evangelization of employees. This output of H2 of the Mann-Whitney U Test is in accordance with Figure 4, where only 17% of companies declare that they do not focus on organizational learning in the cybersecurity area. The motivation for this might be seen in the strong impacts of cyberattacks, which are, in relation to the answer to research question no. 3, presented in Figure 7.

Two performances of Pearson correlation to verify hypothesis H3 show that costs related to cybersecurity and its measures are unequivocally variable costs, not fixed. This was presented in correlation with company size in the form of number of employees and annual turnover.

CONCLUSION AND RECOMMENDATION

The results of this study are based on quantitative research of more than 120 survey respondents. The sizes of Czech and Slovak set the limits of the research.

The paper responds to three research questions related to organizational learning: to ensure employees' awareness of cybersecurity, measures to ensure cybersecurity, and typical incidents occurring when a cyberattack happens.

There are also three hypotheses aimed at an organization’s emphasis on organizational learning and cybersecurity awareness: using a higher level of technical and organizational measures to ensure cybersecurity, and taking proactive measures to make specific investments as security countermeasures.

It would be appropriate and valuable to carry out follow-up research, continuing with deeper research of costs of cybersecurity measures per employee within the company size or the correlation between costs invested in organizational learning and the other measures and the amount of occurrence of cyberattacks in the company.

REFERENCES

Alanazi, M., Freeman, M., & Tootell, H. (2022). Exploring the factors that influence the cybersecurity behaviors of young adults. Computers in Human Behavior, 136, 107376. https://doi.org/10.1016/j.chb.2022.107376

Anon. (2015). *Cybersecurity Fundamentals Study Guide*, USA: ISACA.

Argote, L., & Miron-Spektor, E. (2011). Organizational Learning: From Experience to Knowledge. Organization Science, 22(5), 1123–1137. https://doi.org/10.1287/orsc.1100.0621

Arsenault, M. (2011). R. K. Yin. (2012). Applications of Case Study Research. Thousand Oaks, CA : Sage. 231 pages. Canadian Journal of Program Evaluation, 26(2), 104–107. https://doi.org/10.3138/cjpe.26.008

Bandura, A. (1977). Social learning theory, Englewood Cliffs, N.J.: Prentice Hall.

Brynjolfsson, E. and McAfee, A. (2014), The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies, Norton, New York, NY.

Hornungova, J. (2022). Human resource management in work-life balance issues in the context of Covid-19 Pandemic: an Interpretative Phenomenological Analysis. *Journal of Interdisciplinary Research*, *12*(2), 60-64.

Lessig, L. (2004). Free culture: How big media uses technology and the law to Lock Down Culture and control creativity. Penguin.

Mayer, P., Kunz, A., & Volkamer, M. (2017). Reliable Behavioural Factors in the Information Security Context. Proceedings of the 12th International Conference on Availability, Reliability and Security. https://doi.org/10.1145/3098954.3098986

McHugh, M. L. (2013). The Chi-square test of independence. Biochemia Medica, 143–149. https://doi.org/10.11613/bm.2013.018

McKight, P. E., & Najab, J. (2010). Kruskal-Wallis Test. The Corsini Encyclopedia of Psychology, 1–1. Portico. https://doi.org/10.1002/9780470479216.corpsy0491

Milichovský, F., & Kuba, K. (2023). Expected Impact of Industry 4.0 on Employment in Selected Professions in the Czech Republic and Germany. *Processes*, *11*(2), 516. MDPI AG. https://doi.org/10.3390/pr11020516

Molnár, Z. et al. (2012). *Pokročilé metody vědecké práce*, [Zeleneč]: Profess Consulting.

Nguegang Tewamba, H., Robert Kala Kamdjoug, J., Bell Bitjoka, G., Fosso Wamba, S., & Nkondock Mi Bahanag, N. (2019). Effects of Information Security Management Systems on Firm Performance. American Journal of Operations Management and Information Systems, 4(3), 99. https://doi.org/10.11648/j.ajomis.20190403.15

Nonaka, I., & Takeuchi, H. (1995). The Knowledge-Creating Company. https://doi.org/10.1093/oso/9780195092691.001.0001

Schober, P., Boer, C., & Schwarte, L. A. (2018). Correlation Coefficients: Appropriate Use and Interpretation. Anesthesia &amp; Analgesia, 126(5), 1763–1768. https://doi.org/10.1213/ane.0000000000002864

Thanh Nguyen, L., Tat, T. D., & Dang, M. H. (2023). The impacts of organizational culture on the organizational commitment: A case study of Vinaphone's business centers in Southwest Vietnam. Journal of Eastern European and Central Asian Research (JEECAR), 10(2), 213–226. https://doi.org/10.15549/jeecar.v10i2.976

von Solms, B., & von Solms, R. (2018). Cybersecurity and information security – what goes where? Information &amp; Computer Security, 26(1), 2–9. https://doi.org/10.1108/ics-04-2017-0025

von Solms, R. (1998). Information security management (3): the Code of Practice for Information Security Management (BS 7799). Information Management &amp; Computer Security, 6(5), 224–225. https://doi.org/10.1108/09685229810240158

Zheng, X. & Sun, A. (2022). Digitalization and internationalization: a study of the manufacturing industry in China. *Transformations in Business & Economics*, *21*(2B), 772-791.

ABOUT THE AUTHORS

Katerina Petrova, email: xphornungova@vutbr.cz (Corresponding Author)

Katerina Petrova is a doctoral student at the Department of Business and Management since 2019. She has been an assistant in this department since 2022. Her professional interests include management, organizational culture, and digital transformation.

Jan Spatenka is a doctoral student at the Department of Informatics. He has been a part of the research team since 2020. His expertise is in the implementation of information systems and project management, including agile and scaled agile framework. He is also involved in the research of teal organizations.

Lukas Vaclavik has been a doctoral student at the Faculty of Business and Management, Department of Informatics, since 2020. His research scope includes mainly the area of cybersecurity and its economic aspects.