



The Influence of Organization's Size and Sector on Its Level of Cybersecurity

Lukáš Václavík¹, Marie Soukupová^{*2}

Abstract

The impact of both organizational size and sector on various cybersecurity practices, investments, attack exposure, and perceived barriers has long been discussed. Using survey data of 254 respondents collected from May 2024 to May 2025 across diverse industries, Spearman's rank-order correlation and Kruskal-Wallis tests are applied to analyze relationships between organizational characteristics and cybersecurity outcomes. Larger organizations tend to invest more in cybersecurity, perceive particular cyber threats as more severe, and in case of a cyberattack, experience more severe consequences such as data loss and contractual penalties. In contrast, the sector shows only weak or non-significant correlations with most variables, except for perceived importance of cybersecurity, which IT organizations rated significantly higher than others. These findings suggest that organization's size may play a more influential role than sectoral affiliation in shaping cybersecurity preparedness and exposure, although sector-specific characteristics should still be taken into account.

Keywords

Organization Size, Sector, Cybersecurity, Perceived Barriers, Threats

I. Introduction

Cybersecurity differs across industries and countries (Knopová and Knopová, 2014). This article compares the cybersecurity landscape in the Czech and Slovak Republics across key sectors (manufacturing, healthcare, energetics, services, IT, trade) (as also defined by Tariq et al. (2014), Arachchilage and Love (2014), Rocha Flores and Ekstedt (2016), Kearney and Kruger (2016). The paper aims to assess the level of cybersecurity of organizations across sectors within the two countries and tackle the key aspects impacting the overall level of cybersecurity using adequate statistical methods. The research identifies the key aspects

¹ Brno University of Technology, Faculty of Business and Management, Antonínská 548/1, 602 00 Brno, Czech Republic. E-mail: Lukas.Vaclavik1@vutbr.cz.

^{*} Corresponding author

² Brno University of Technology, Faculty of Business and Management, Antonínská 548/1, 602 00 Brno, Czech Republic. E-mail: Marie.Soukupova1@vutbr.cz.

as investments, perceived cyber threats, barriers to implementing security measures, and incident impacts. These are analyzed in detail in the Research Framework.

Countries of Operations

Organizations often overlook official cybersecurity guidelines (Wilson and McDonald, 2024). While the Czech authority (NÚKIB, 2022) enjoys a solid reputation, the Slovak government recently faced cybersecurity challenges (Hundreds of schools paralyzed by a bomb threat sent from an alleged Russian email, 2024, Antoniuk, January 10th, 2025). Interestingly, during data collection, several Slovak respondents viewed the email invitation as a cyber threat, whereas Czech respondents thoroughly fact-checked the researchers' legitimacy before participating. Research (Dvoulety, 2025, Hyk, 2026 and Kliuchnyk, 2025) shows that countries' cybersecurity importance is rising together with the progressing digitalization of processes as well as by adopting new technologies such as artificial intelligence. This fact underlines the importance of the introduced research.

Division of Organizations

Within the questionnaire, the respondents' organizations were divided based on their size derived from the number of employees (where a micro-organization consists of less than 10 employees, small of less than 50, medium of less than 250 and large of more than the stated amount). At the same time, organizations were also divided by industries into manufacturing, healthcare, energetics, services, IT and other (as also defined by (Tariq et al., 2014, Arachchilage and Love, 2014, Rocha Flores and Ekstedt, 2016, Kearney and Kruger, 2016)).

Commonly, different organizations represent different specifics when it comes to cybersecurity whereas oftentimes, researchers consider all organizations a homogenous group therefore providing them with a standard set of recommendations (Chaudhary et al., 2023, Heidt et al., 2019). That is why SMEs often do not consider these recommendations relevant and do not implement them in their day-to-day operations. However, with the new regulation also known as NIS2 (Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), 2022), a considerable number of SMEs will be demanded to follow stricter security guidelines which should reflect their uniqueness (e.g. size, but also sector – as proven by our data).

Types of Cybersecurity Investments

When it comes to investments in cybersecurity measures, ever so often, multiple solutions are said to have a similar level of effect. Speaking of similar net effects, the least expensive measure should consistently be prioritized. However, costs are not the only factor to distinguish. Another examined parameter should definitely be the impact that the measure has on the processes and work of staff (Fielder et al., 2016) since it is not difficult to invent a secure measure, but it can be considerably more difficult to invent one that also makes the process simple.

Furthermore, research (Dinkova et al., 2024) shows that the size of the organization does not matter much in the sense of the amount of cybersecurity investments. Apparently, while SMEs do invest less in security measures, they also report less cyber incidents or their lower impact which seems to be a logical proportion. However, the authors claim that organizations not investing enough, namely in their detection measures, often may not be aware of incidents within their perimeter and therefore do not report them.

Consequently, although the figures may be calming to policymakers, suggesting that even small organizations invest suitable resources since they prevent them from incidents, one must consider the fact that many threats reveal themselves only after long periods of time of destroying the network gradually from within (Noor et al., 2018).

Budget is one of the most common challenges that the employees (and CISOs) are facing when trying to implement new cybersecurity measures (Fielder et al., 2016). Although it is claimed that the measure shall only cost a fragment of the foreseen loss due to a cyberattack (Fielder et al., 2016), in today's reality of abundance of cybersecurity products, multiple aspects must be considered. While previous research (Fielder et al., 2016) formulated diverse optimization problems, authors are quite scarce when it comes to estimating the precise percentage of recommended investment. The authors are aware of the common misconception among different departments of an organization, some handling the financial and others the technical part of measures, creating obstacles for one or the other to advocate for the measure from all aspects into detail (e.g. it is quite common for the IT staff not to be aware of the exact figures of investments of the organization and for the economic department not to be capable of describing the technical effects of each measure). Consequently, perceptions of staff rather than exact figures were studied in this paper.

A single measure on its own, although aligning with budget expectations, can not be effective without a complex minimum security level of the organization (Kauffman and Sougstad, 2014). The strategy and perceived importance of cybersecurity (based on the trend of measures implemented within the organization) therefore also play an important role in the aspect of cybersecurity investments. Confidence of the workers in the organization's cybersecurity and IT is proved to be equally important as the security measures themselves (Ghernaouti-Helie, 2012). For this reason, the paper left space for estimations of the respondents related to their confidence in their organizations' cybersecurity levels.

Financial Implications of Cyberattacks

Previous research (Wilson and McDonald, 2024) estimated the cost of an attack at approximately 1740 EUR for micro and small organizations and 5100 EUR for medium and large organizations, although the authors question the validity of these figures. Estimating the costs is problematic since each organization may take different costs into consideration – implicit costs such as internal employees' wages often being overlooked or difficult to assess. That is the reason why the authors of this research decided to leave the space for estimation of financial damage open for the respondents to interpret.

Although the scientific community has been trying to assess the costs of cyberattacks and the financial damage done for quite some time, Riek and Böhme (2018) point out that the estimations are still rather unsound based on their origin in small surveys created with the intention to exaggerate costs. That is why the authors decided to let the respondents freely express their estimates without forcing them to choose among predefined scales in order to get the most authentic answers.

An approach used to estimate the financial impact of incidents consists of monitoring the fluctuations in market valuations of organizations before and after their announcement of being affected by cyberattacks (Dinkova et al., 2024). Since market valuation is published on stock markets where specifically large companies are listed, this approach cannot effectively be used on estimations of financial damage caused to SMEs. This metric proved misleading even in the case of large organizations which, trying not to lose value and reputation, underreport cyberattacks (Dinkova et al., 2024).

Furthermore, according to the research (Dinkova et al., 2024), no relation between profitability of the organization and cybersecurity measures and investments was indicated. The indicated facts support the argument of financial figures being detached from the state of cybersecurity measures in an organization rather than influencing them fundamentally.

Research Methods

The research methods used in the article consisted primarily of a survey which partly included quantitatively (closed questions) and qualitatively processed answers (open questions). The answers were statistically refined and interpreted by confirmation or refutation of established hypotheses.

Survey Creation

The sample ensured diversity across organizational sizes, sectors, and countries, targeting various professionals (e.g., IT, management, and administration). Unlike previous narrow, laboratory-based studies (Chaudhary et al., 2023), our robust questionnaire collected authentic, real-world data and was refined through expert and academic consultations. Relying on respondents' evidence-based experience with actual incidents, the survey assessed cyberattack prevalence using established typologies (Chaudhary et al., 2023; Uwizeyemungu et al., 2019) while accounting for sector-specific variances (Yulianto et al., 2025). Additionally, the instrument evaluated predefined implementation barriers and cyberattack impacts (Alanazi, 2023). Recognizing that technology cannot fully eliminate human error (Tariq et al., 2014), the survey also addressed human factors critical to security behavior, such as motivation, attitude (Mayer et al., 2017), and psychological ownership (Yoo et al., 2018; Chaudhary et al., 2023).

Research Framework

This framework explores whether organizational size or sectoral affiliation is more strongly associated with key cybersecurity dimensions: investments, perceived threats, implementation barriers, and incident impacts. Understanding these associations is crucial for tailoring cybersecurity policies and resource allocation. The study therefore hypothesizes

that an organization's cybersecurity posture varies more significantly by its size than by its sector.

RQ1: Which factor has a greater association with cybersecurity-related investment, perceived threats, barriers, and incident impacts: organizational size or sectoral affiliation?

H1: Organizations vary in cybersecurity investment, perceived threats, barriers, and incident impacts by organizational size more than by sector affiliation.

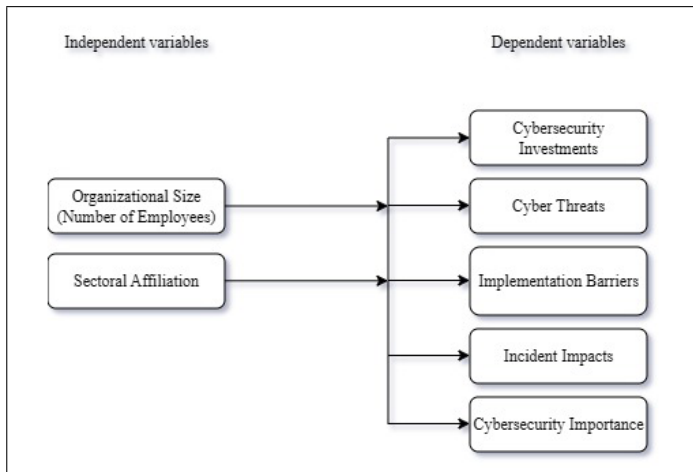
H1a: Perceived cyber threats are more influenced by the size of an organization than its sector.

H1b: Organizations of different sizes face different barriers to implementing security measures, more than just sector affiliation.

H1c: The impacts of cyber incidents vary more significantly by organization size than by sector.

To provide a clear overview of the study's design and to explicitly map the investigated variables, the relationships proposed in the hypotheses are visualized in the conceptual framework below (Figure 1). The model illustrates how the two independent variables are expected to influence the five dependent dimensions of organizational cybersecurity.

Figure 1: Conceptual framework of the study mapping independent and dependent variables



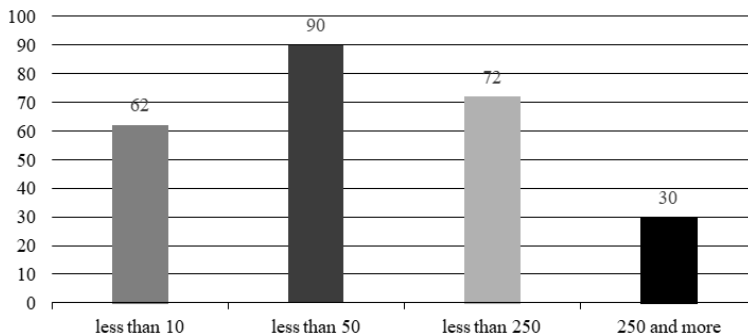
Source: Authors' own design

II. Main Text

Data Sample

A total of 254 organizations participated. SMEs (10–250 employees) demonstrated high interest and were represented above average (Figure 2).

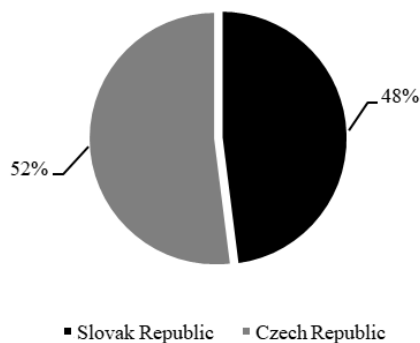
Figure 2: Organizations in the sample analyzed by number of employees



Source: Authors' own elaboration

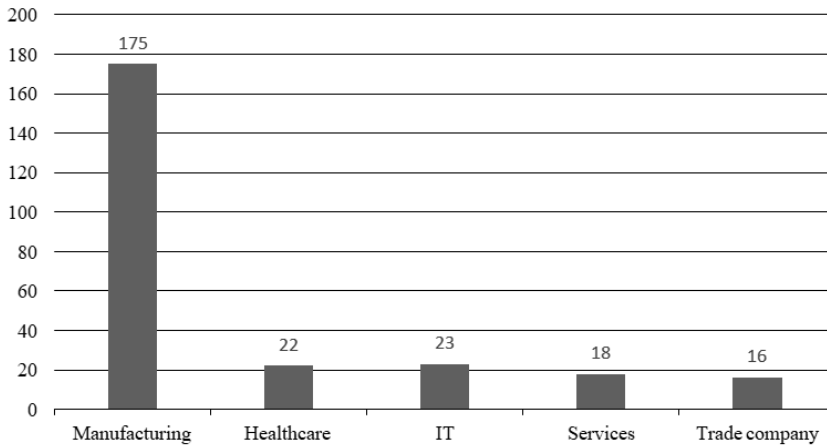
Figure 3 illustrates the percentage of organizations based in the Czech and Slovak Republic. The slight predominance of Czech organizations reflects the country's larger population.

Figure 3: Organizations in the sample analyzed by country



Source: Authors' own elaboration

A significant majority of respondents belong to the manufacturing sector, while other sectors are evenly represented (Figure 4).

Figure 4: Organizations in the sample analyzed by sector affiliation

Source: Authors' own elaboration

Cybersecurity Investments

To examine associations between investments and organizational characteristics, Spearman's rho was conducted (Table 1).

Table 1: Correlation between cybersecurity investments components and organizational characteristics using Spearman's rho

	Number of Employees	Wages	Software	Hardware	Implementation	Sector
Number of Employees	1.000					
Wages	.127*	1.000				
Software	.240**	.015	1.000			
Hardware	.228**	.017	.572**	1.000		
Implementation	.158*	.134*	.373**	.403**	1.000	
Sector	-.126*	.099	.066	.015	-.014	1.000

Source: Authors' own elaboration

Note: $N = 254$

* correlation is significant at the .05 level (2-tailed)

** correlation is significant at the .01 level (2-tailed)

As shown in Table 1, the number of employees positively correlates with investments in software, hardware, and implementation (all $p < .05$). Strong inter-correlations exist among these investment types, indicating that organizations investing heavily in one area likely invest in others. Sector showed no significant correlations with expenditure categories, implying investment patterns are tied more to size than sector.

Table 2 presents correlations regarding threat prevalence.

Table 2: Correlation between perceived cyber threats severity and organizational characteristics using Spearman's rho

	Sector	Number of Employees	Ransomware	Phishing	Data Theft	Social Engineering	DDoS	Insider Threat	Industrial Espionage
Sector	1.000								
Number of Employees	-.126*	1.000							
Ransomware	.004	.207**	1.000						
Phishing	.052	.211**	.252**	1.000					
Data Theft	.024	.214**	.250**	.254**	1.000				
Social Engineering	-.006	.120	.248**	.234**	.389**	1.000			
DDoS	.048	.578**	.343**	.208**	.313**	.222**	1.000		
Insider Threat	.052	.204**	.339**	.259**	.314**	.247**	.300**	1.000	
Industrial Espionage	.006	.383**	.227**	.407**	.407**	.375**	.305**	.327**	1.000

Source: Authors' own elaboration

Note: $N = 254$

* correlation is significant at the .05 level (2-tailed)

** correlation is significant at the .01 level (2-tailed)

While the sector showed a weak negative correlation with organization size, it was not significantly associated with any specific cyber threat. In contrast, organizational size positively correlated with ransomware, phishing, and insider threats (all $p < .01$). This suggests larger organizations perceive these threats more frequently, likely due to broader attack surfaces and better detection mechanisms. Strong inter-correlations among threats were also observed.

Perceived Barriers in Developing Organizational Cybersecurity

Spearman's rank-order correlation was used to assess the relationship between organizational characteristics (sector and size) and perceived barriers to implementing security measures. The results are presented in Table 3.

Table 3 shows that organizational size significantly correlates with resistance to change. Insufficient funding correlates positively with a lack of management support, which in turn correlates with resistance to change, suggesting a systemic pattern of internal barriers. Sector affiliation did not significantly correlate with any perceived barriers, indicating these challenges are structural rather than sector-specific.

Table 3: Organizational characteristics and perceived barriers in developing cybersecurity

	Sector	Number of employees	Insufficient funding	Management support	Shortage of Experts	Reluctance to change
Sector	1.000					
Number of Employees	-.126*	1.000				
Insufficient Funding	-.050	.002	1.000			
Management Support	.056	.068	.210**	1.000		
Shortage of Experts	-.035	.123	-.111	.046	1.000	
Reluctance to Change	-.121*	.251**	-.105	.124*	-.018	1.000

Source: Authors' own elaboration

Note: N = 254

* correlation is significant at the .05 level (2-tailed)

** correlation is significant at the .01 level (2-tailed)

Impacts of Perceived Cybersecurity Threats

Table 4 summarizes the associations between organizational characteristics and the consequences of perceived cybersecurity impacts.

Table 4: Correlation between barriers to cybersecurity investment and organizational characteristics using Spearman's rho

	Sector	Number of Employees	Reputation Loss	Data Loss	Property Damage	Contractual Penalties	Financial Loss	Know-how loss
Sector	1							
Number of Employees	-.126*	1						
Reputation Loss	-.153*	.064	1					
Data Loss	-.127*	.154*	.342**	1				
Property Damage	-.042	.164**	.276**	.442**	1			
Contractual Penalties	-.197**	.166**	.506**	.454**	.479**	1		
Financial Loss	-.026	0.057	.422**	.500**	.546**	.515**	1	
Know-how Loss	-.051	.132*	.358**	.392**	.510**	.467**	.456**	1

Source: Authors' own elaboration

Note: N = 254

* correlation is significant at the .05 level (2-tailed)

** correlation is significant at the .01 level (2-tailed)

Table 4 indicates that the sector is negatively correlated with reputational damage, data loss, and contractual penalties. Conversely, organizational size positively correlates with data loss, property damage, contractual penalties, and loss of know-how. Strong positive correlations among incident consequences suggest a clustering effect, particularly between tangible physical damages and financial losses ($\rho = .546, p < .001$).

Table 5: Correlation between organizational characteristics and cyber incident impact severity

	Impacts	Sector	Number of Employees
Impacts	1.000		
Sector	.000	1.000	
Number of Employees	.088	-.126*	1.000

Source: Authors' own elaboration

Note: $N = 254$

* correlation is significant at the .05 level (2-tailed)

As shown in Table 5, the overall reported severity of damage (measured on a 0–4 scale) showed no statistically significant relationship with either sector or size. This highlights the unpredictable nature of cyber incident severity across the sample.

Cybersecurity Importance

As detailed in Table 6, organizational size positively correlates with the perceived importance of cybersecurity, whereas sectoral affiliation shows a negative correlation.

Table 6: Correlation between organizational characteristics and cybersecurity importance

	Sector	Number of Employees	Cybersecurity Importance
Sector	1.000		–0.275**
Number of Employees	-.126*	1.000	0.369**

Source: Authors' own elaboration

Note: $N = 254$

* correlation is significant at the .05 level (2-tailed)

** correlation is significant at the .01 level (2-tailed)

A Kruskal-Wallis test was conducted to determine whether there were statistically significant differences in how organizations across different sectors perceive the importance of cybersecurity. The perceived importance of cybersecurity was set as the dependent variable, measured on an ordinal scale from 0 (low importance) to 4 (critical importance). The independent variable was the sector in which the organization operates.

The Kruskal-Wallis test revealed a statistically significant difference across sectors, $H(4) = 20.323, p < .001$. This indicates that the variable under investigation – perceived importance of cybersecurity – varies significantly depending on the sectoral affiliation. This supports the idea that sector context plays a role in shaping cybersecurity attitudes or investments.

Table 7: Kruskal Wallis independence test for cybersecurity importance across organizational sectors

Total N	254
Test Statistic	20.323
Degree of Freedom	4
Asymptotic Sig. (2-sided test)	<.001

Source: Authors' own elaboration

Table 8: Post-hoc pairwise comparisons using Dunn's test with Bonferroni correction

Sample 1-Sample 2	Test Statistic	Std. Error	Std. Test Statistic	Sig.	Adj. Sig.^a
Trade-Services	11.413	23.489	0.486	.627	1.000
Trade-Manufacturing	28.710	17.855	1.608	.108	1.000
Trade-IT	71.088	22.256	3.194	.001	.014
Trade-Healthcare	71.491	22.462	3.183	.001	.015
Services-Manufacturing	17.297	16.922	1.022	.307	1.000
Services-IT	59.675	21.514	2.774	.006	.055
Services-Healthcare	60.078	21.728	2.765	.006	.057
Manufacturing-IT	42.378	15.163	2.795	.005	.052
Manufacturing-Healthcare	42.781	15.464	2.766	.006	.057
IT-Healthcare	0.403	20.387	0.020	.984	1.000

Source: Authors' own elaboration

Post-hoc Dunn's tests (Table 8) revealed that the IT sector rated cybersecurity as significantly more important compared to the trade (adjusted $p = .014$) and healthcare sectors (adjusted $p = .015$). Marginal differences also suggest technology-oriented sectors emphasize cybersecurity more strongly.

III. Conclusion

The study investigated the relative association of organizational size and sectoral affiliation with key dimensions of cybersecurity: investment patterns, perceived cyber threats, barriers to implementing security measures, and the perceived negative impacts of cyberattacks. The analysis provides empirical support for the central hypothesis (H1) that organizational size is more strongly associated with an organization's cybersecurity posture than sectoral affiliation, though in the context of the research's limitations (such as bivariate correlations and an uneven sample distribution).

Cybersecurity Investments and Organizational Size

The findings show weak to moderate positive correlations between the number of employees and cybersecurity-related investment on software ($\rho = .240$; $p < .001$), hardware ($\rho = .228$; $p < .001$), and implementation activities ($\rho = .158$; $p = .012$). These

results suggest that larger organizations allocate more resources to both technical and procedural components of cybersecurity which is in compliance with Heidt et al. (2019). This observation also aligns with prior research (Chaudhary et al., 2023), which emphasizes that larger organizations tend to increase cybersecurity investments following externally exposed incidents.

Perceived Threats and Cyberattack Exposure

Supporting the hypothesis H1a, the data indicate that larger organizations face higher exposure to specific types of cyber threats. Statistically significant correlations were observed between organizational size and ransomware attacks ($\rho = .207$; $p < .01$), phishing attempts ($\rho = .211$; $p < .01$), and insider threats ($\rho = .204$; $p < .01$). These findings may reflect both the expanded digital surface and increased detection capabilities of larger entities. Sectoral affiliation, by contrast, was not significantly related to the frequency of the attack types. Previous research (Sarabi et al., 2016) is also in compliance with the approach of considering not only the sector (though in some correlations proved significant), but also other aspects of the organizations.

Barriers to Implementation

The analysis supports the hypothesis H1b, showing that barriers to implementing cybersecurity measures are more strongly associated with organizational size than its sector. Resistance to change was positively correlated with size ($\rho = .251$; $p < .001$), indicating that larger organizations may encounter more institutional inertia when adopting new security protocols. Moreover, significant associations were found between lack of leadership support and both lack of resources ($\rho = .210$; $p = .001$) and resistance to change ($\rho = .124$; $p = .048$), suggesting a systemic pattern of internal barriers. Interestingly, lack of cybersecurity experts which is mentioned by authors in (Puławska et al., 2022) did not show significant associations with any other variables, implying that this issue may be uniformly distributed across sizes and sectors.

Cyber Threats Severity

Supporting the hypothesis H1c, organizational size was positively correlated with several types of perceived cybersecurity threats, including data loss ($\rho = .154$; $p = .014$), asset damage ($\rho = .164$; $p = .009$), contractual penalties ($\rho = .166$; $p = .008$), and loss of know-how ($\rho = .132$; $p = .035$). These findings imply that larger organizations may perceive and suffer greater tangible losses from cyberattacks, potentially due to their more complex infrastructures and greater asset exposure. This finding is in compliance with (Biener et al., 2015) where empirical research in the context of cyber risk insurance demonstrated that organization losses depend on its size (suggesting that larger firms have higher exposure). Sectoral affiliation, in contrast, exhibited only weak negative correlations with reputational damage ($\rho = -.153$; $p = .014$), data loss ($\rho = -.127$; $p = .043$), and contractual sanctions ($\rho = -.197$; $p = .002$), suggesting that some sectors may either better manage or underscore potential cybersecurity risks.

However, when examining the overall perceived severity of cybersecurity impacts (measured on a 0–4 scale), neither organizational size ($\rho = .088$; $p = .161$) nor sector ($\rho = .000$; $p = .994$) showed a statistically significant relationship. This may suggest that while specific perceived threats differ by organizational size, the overall perceived severity of potential cybersecurity cyberattack impacts is uniformly distributed across different types of organizations. This finding is different from Biener et al. (2015) where their empirical research demonstrated that losses from cyberattacks depend on the sector (meaning that financial firms have higher exposure).

Perceived Importance of Cybersecurity

Organizational size also exhibited a strong positive correlation with the perceived importance of cybersecurity ($\rho = .369$; $p < .001$), whereas sectoral affiliation was negatively correlated ($\rho = -.275$; $p < .001$). These results further support the argument that size is a stronger correlate of cybersecurity awareness and prioritization. Kruskal-Wallis testing confirmed statistically significant differences in cybersecurity importance across sectors $\chi^2(4, N = 254) = 20.32$, $p < .001$, and post-hoc Dunn's tests revealed that the IT sector assigns significantly more importance to cybersecurity compared to the trade (adjusted $p = .014$) and healthcare (adjusted $p = .015$) sectors. As suggested by previous studies (Leirimo, 2024), differences among sectors related to this area still prevail.

Overall, the findings provide consistent evidence that organizational size is a more influential factor than sector in terms of its association with cybersecurity expenditures, perceived threats, implementation barriers, and cyberattack impacts. This has important implications for policy and practice. Rather than adopting one-size-fits-all approaches based on sectoral norms, cybersecurity strategies and support mechanisms should be more carefully tailored to organizational scale. Especially for small and medium-sized enterprises (SMEs), which made up the majority of the survey sample, targeted support in overcoming internal barriers and increasing awareness could significantly strengthen their cybersecurity resilience.

Based on the analysis conducted, organization size may appear as a stronger and more significant factor associated with specific cybersecurity aspects such as investments, the occurrence of incidents, perceived barriers, and cyberattack impacts than the sector in which the organization operates. The findings indicate that as the number of employees increases, organizations are more likely to invest in security software, hardware, and implementation. At the same time, larger organizations also perceive higher severity and diversity of cyber threats and are more likely to perceive resistance to change as a key barrier.

Moreover, the consequences of potential attacks – such as data loss, contractual penalties, and loss of know-how – show a stronger correlation with organization size than with sector. Among all else, larger organizations may experience stronger internal resistance to changes related to cybersecurity. The resistance is also closely related to management support. At the same time, the impacts of cyberattacks were proved to demonstrate themselves in a broader range rather than separately, especially among larger organizations.

In contrast, the sector shows only limited statistical association with the studied variables, with its primary significance found in the perception of the importance of cybersecurity. This distinction can likely be attributed to the varying degrees of digital dependency across sectors – organizations in the IT sector typically prioritize cybersecurity more than those in sectors like trade or healthcare. Furthermore, a factor that prevails within all sectors and sizes is the lack of cybersecurity experts.

In conclusion, cybersecurity strategies and policies of organizations are slightly recommended to primarily take into account the size of the organization as a critical factor, rather than relying on sector-based assumptions.

Acknowledgements

The research was funded by Brno University of Technology junior specific internal grant no. FP-J-24-8504 and FP-S-26-9013.

References

- Alanazi, A. T. (2023). Clinicians' Perspectives on Healthcare Cybersecurity and Cyber Threats. *Cureus*, 15(10): e47026. <https://doi.org/10.7759/cureus.47026>.
- Antoniuk, D. (January 10th, 2025). *Slovakia's land registry hit by biggest cyberattack in country's history, minister says*. The Record. Retrieved March 5, 2025, from <https://the-record.media/slovakia-registry-cyberattack-land-agriculture>.
- Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, 38, 304–312. <https://doi.org/10.1016/j.chb.2014.05.046>.
- Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of Cyber Risk: An Empirical Analysis. *The Geneva Papers on Risk and Insurance – Issues and Practice*, 40(1), 131–158. <https://doi.org/10.1057/gpp.2014.19>.
- Chaudhary, S., Gkioulos, V., & Katsikas, S. (2023). A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises. *Computer Science Review*, 50, 1–20. <https://doi.org/10.1016/j.cosrev.2023.100592>.
- Dinkova, M., El-Dardiry, R., & Overvest, B. (2024). Should firms invest more in cybersecurity? *Small Business Economics*, 63(1), 21–50. <https://doi.org/10.1007/s11187-023-00803-0>.
- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), 2022 § (2022).

Dvoulletý, O., Jirásek, M., Giglio, C., & Liguori, E. (2025). Artificial intelligence, digitalization, and new technologies in shaping business and management research. *Cogent Business & Management*, 12(1). <https://doi.org/10.1080/23311975.2025.2580126>.

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems*, 86, 13–23. <https://doi.org/10.1016/j.dss.2016.02.012>.

Ghernaouti-Helie, S. (2012). Going Digital – Rethinking Cybersecurity and Confidence in a Connected World: A Challenge for Society. *2012 Third International Conference on Emerging Security Technologies*, 8–11. <https://doi.org/10.1109/EST.2012.16>.

Heidt, M., Gerlach, J. P., & Buxmann, P. (2019). Investigating the Security Divide between SME and Large Companies: How SME Characteristics Influence Organizational IT Security Investments. *Information Systems Frontiers*, 21(6), 1285–1305. <https://doi.org/10.1007/s10796-019-09959-1>.

Hundreds of schools paralysed by a bomb threat sent from an alleged Russian email. (2024 7). The Slovak Spectator. Retrieved March 5, 2025, from <https://spectator.sme.sk/politics-and-society/c/hundreds-of-schools-paralysed-by-a-bomb-threat-sent-from-an-alleged-russian-email>.

Hyk, V., Vysochan, O., & Vysochan, O. (2026). Cyber Security in Terms of Ensuring the Digital Transformation of European Economies: Empirical Evidence. *DANUBE*, 17(1), 21–35. <https://doi.org/10.2478/danb-2026-0002>.

Kauffman, R. J., & Sougstad, R. (2014). Risk Management of Contract Portfolios in IT Services: The Profit-at-Risk Approach. *Journal of Management Information Systems*, 25(1), 17–48. <https://doi.org/10.2753/MIS0742-1222250102>.

Kearney, W. D., & Kruger, H. A. (2016). Can perceptual differences account for enigmatic information security behaviour in an organisation? *Computers & Security*, 61, 46–58. <https://doi.org/10.1016/j.cose.2016.05.006>.

Kliuchnyk, A., Shyshpanova, N., Sokolik, V., Ostapenko, A., & Kryvko, O. (2025). Digitalisation of Public Administration Processes in Shaping the Investment Environment of Territorial Communities. *DANUBE*, 16(3), 264–276. <https://doi.org/10.2478/danb-2025-0013>.

Knopová, M., & Knopová, E. (2014). The Third World War? In The Cyberspace. Cyber Warfare in the Middle East. *Acta Informatica Pragensia*, 3(1), 23–32. <https://doi.org/10.18267/j.aip.33>.

Leirmo, J. L. (2024). Cybersecurity Awareness in Critical Sectors – a Systematic Literature Review. *Flexible Automation and Intelligent Manufacturing: Manufacturing Innovation and Preparedness for the Changing World Order*, 125–132. https://doi.org/10.1007/978-3-031-74482-2_15.

- 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*, 1–10. <https://doi.org/10.1145/3098954.3098986>.
- Moody's. (2024). Orbis Europe. Retrieved January 22, 2025, from <https://orbiseurope-r1.bvdinfo.com/version-20241204-4-0/Orbis4Europe/1/Companies/Search>.
- Noor, M., Abbas, H., & Shahid, W. B. (2018). Countering cyber threats for industrial applications: An automated approach for malware evasion detection and analysis. *Journal of Network and Computer Applications*, 103, 249–261. <https://doi.org/10.1016/j.jnca.2017.10.004>.
- NÚKIB. (2022 16). *NÚKIB won an award in the Czech At competition*. National Office for Cyber and Information Security. Retrieved May 28, 2025, from <https://nukib.gov.cz/cs/info-servis/aktuality/1836-nukib-ziskal-oceneni-v-soutezi-cesky-zavinac>.
- Puławska, K., Strzelczyk, W., & Orzechowski, A. (2022). Cyber Insurance and Information Sharing As Prevention From Cyber-Attacks – Pilot Study. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4260821>.
- Riek, M., & Böhme, R. (2018). The costs of consumer-facing cybercrime: an empirical exploration of measurement issues and estimates. *Journal of Cybersecurity*, 4(1), 1–16. <https://doi.org/10.1093/cybsec/tyy004>.
- Rocha Flores, W., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security*, 59, 26–44. <https://doi.org/10.1016/j.cose.2016.01.004>.
- Sarabi, A., Naghizadeh, P., Liu, Y., & Liu, M. (2016). Risky business: Fine-grained data breach prediction using business profiles. *Journal of Cybersecurity*, 2(1), 15–28. <https://doi.org/10.1093/cybsec/tyw004>.
- Tariq, M. A., Brynielsson, J., & Artman, H. (2014). The security awareness paradox: A case study. *2014 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2014)*, 704–711. <https://doi.org/10.1109/ASONAM.2014.6921663>.
- Uwizeyemungu, S., Poba-Nzaou, P., & Cantinotti, M. (2019). European Hospitals' Transition Toward Fully Electronic-Based Systems: Do Information Technology Security and Privacy Practices Follow? *JMIR Medical Informatics*, 7(1). <https://doi.org/10.2196/11211>.
- Wilson, M., & McDonald, S. (2024). One size does not fit all: exploring the cybersecurity perspectives and engagement preferences of UK-Based small businesses: exploring the cybersecurity perspectives and engagement preferences of UK-Based small businesses. *Information Security Journal: A Global Perspective*, 1–35. <https://doi.org/10.1080/19393555.2024.2357310>.

Yoo, C. W., Sanders, G. L., & Cervený, R. P. (2018). Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance. *Decision Support Systems*, 108, 107–118. <https://doi.org/10.1016/j.dss.2018.02.009>.

Yulianto, S., Soewito, B., Gaol, F. L., & Kurniawan, A. (2025). Enhancing cybersecurity resilience through advanced red-teaming exercises and MITRE ATT&CK framework integration: A paradigm shift in cybersecurity assessment. *Cyber Security and Applications*, 3. <https://doi.org/10.1016/j.csa.2024.100077>.