IBIMA Publishing
IBIMA Business Review
https://ibimapublishing.com/articles/IBIMABR/2025/620687/
Vol. 2025 (2025), Article ID 620687, 12 pages, ISSEN: 1947-3788
https://doi.org/10.5171/2025.620687

Research Article

Assessing Employees' Knowledge and Skills in Cybersecurity: Quantitative Research in Slovakia

Benita BELANOVA, Anna HAMRANOVA and Aniko TOROKOVA

Bratislava University of Economics and Business, Bratislava, Slovak Republic
benita.belanova@euba.sk

Received date:3 April 2025; Accepted date :8 July 2025; Published date: 19 August 2025

Abstract

The motive behind the study: The study aims to contribute to cybersecurity research by examining the views of managers of companies operating in Slovakia on the level of knowledge and skills of employees in cybersecurity. It focuses on identifying the most lacking and most valued competencies to enhance cybersecurity measures and address the growing concerns of managers globally. The void in literature that makes this study important: Despite the extensive research of literature on cybersecurity, there is a notable gap in understanding the specific knowledge and skills deficits among employees in Slovak companies. While many studies emphasize the human factor in cybersecurity, few focus on the detailed competencies that are most lacking and most valued by managers. This study aims to fill this gap by providing empirical data on these critical aspects, thereby contributing to more targeted and effective cybersecurity training and development. Methodology: The research involved a questionnaire survey conducted from January to June 2024, with 357 managers participating. Data were analyzed using statistical methods, including descriptive statistics and the Kruskal-Wallis test. Summary of the findings: The study found that flexibility, problem-solving, and effective communication are the most lacking yet most valued skills in cybersecurity. No significant differences were found based on company size, ownership, or number of computers. Regular training on soft skills is recommended.

Keywords: cybersecurity, knowledge and skills of employees, the most lacking and most valued knowledge and skills

Introduction

Cybersecurity is an important aspect of the modern digital world that protects sensitive information from unauthorized access and cyber-attacks. Given the growing number of online threats, it is imperative that organizations and individuals invest in robust security measures. Ensuring cybersecurity helps prevent financial loss, protect privacy and maintain credibility. The importance of cybersecurity assurance is underscored by the fact that cybersecurity has become a focus of concern for responsible managers across the globe, both at the level of supranational and national governing bodies and institutions.

Cite this Article as: Benita BELANOVA, Anna HAMRANOVA and Aniko TOROKOVA (2025)," Assessing Employees' Knowledge and Skills in Cybersecurity: Quantitative Research in Slovakia ", IBIMA Business Review, Vol. 2025 (2025), Article ID 620687, https://doi.org/10.5171/2025.620687

In 2020, the European Union presented 2020, a new EU cybersecurity strategy from which a number of regulations and rules have emerged. These include the updated Network and Information Systems Security Directive (NIS2 Directive), which was adopted in 2023 and aims to strengthen cyber resilience and harmonize regulations across member states (World Economic Forum, 2024). Member states were tasked with fully transposing and implementing the NIS2 Directive by 18 October 2024. However, the Directive only applies to companies with more than 50 employees, with a turnover greater than 10 mi. €10 million, providing services in selected critical infrastructure sectors. Other regulations according to the European Commission (2024) and Kost (2025) are the Cyber Resilience Act (mandatory cybersecurity requirements for all products connected directly or indirectly to another device or network) and the GDPR (General Data Protection Regulation).

In the Slovak Republic, the implementation of regulations related to cybersecurity is carried out through the amended Act on Cybersecurity 69/2018 Coll. 18/2018 Coll.) and the Electronic Communications Act (No. 351/2011 Coll.) (CMS, 2025).

In companies and organizations, cybersecurity means protecting information systems, networks and data from cyber threats and attacks (MIRRI, 2025). This process includes various activities and strategies e.g. for prevention, detection, response to cyber incidents, incident recovery, access control (strong password policies), securing cloud services, creating a culture of security in the company.

The issue of cybersecurity is also widely developed in the field of science and research. The intention of our paper is to contribute to cybersecurity research by examining the views of managers of companies operating in Slovakia on the level of knowledge and skills of employees in the field of cybersecurity. We will focus in more detail on the knowledge and skills that employees lack most in the area of cybersecurity, compare them with the knowledge and skills that are most valued in companies and identify the parameters in which the opinions on the examined knowledge and skills differ.

Literature Review

To ensure cybersecurity in a company, various activities and measures need to be implemented. This fact is also reflected in the professional and scientific literature, where a large number of scientific articles have been published that examine cybersecurity from different perspectives. For example, there are currently 25 252 scientific articles published in the Web of Science database under the heading 'cybersecurity'. In most of the publications, among other aspects of cybersecurity, the influence of the human factor, which is also the focus of our paper, is present. We are inspired by the research studies of Reddy & Rao (2016), Suryotrisongko & Muhashi (2019), Wu & Zhang (2019), Lee & Kim (2023), Perala & Lehto (2024), Fatoki et al. (2024).

In addition, many electronic resources (electronic publications, websites, possibly blogs) dealing with cybersecurity and emphasizing the importance of the human factor are available (cybercompetence (2025), O2 Business Services (2025), MIRRI (2024), H&P Magazine (2025) ...).

The complexity of cybersecurity issues and the importance of systematically examining them has been published by Suryotrisongko & Muhashi (2019), who developed a taxonomy of cybersecurity research, where they created 8 areas, namely: (1) Applied cybersecurity, (2) Cybersecurity data science, (3) Cybersecurity education and training, (4) Cybersecurity incidents, (5) Cybersecurity management and policy, (6) Cybersecurity technology, (7) Human and social cybersecurity and (8) Theories in cybersecurity. The focus on the human factor was evident in two areas, namely (3) Cybersecurity education and training and (7) Human and social cybersecurity. The taxonomy developed by the authors underlines the interdisciplinary nature of cybersecurity, i.e. it is not only technical cybersecurity, but also data,

systems/technology and human/societal cybersecurity.

Reddy & Rao (2016) investigated user behaviour in the area of cyber security. They assumed that knowledge of cybersecurity issues is one of the predictors of adherence to security policies and procedures. The authors examined the impact of cybersecurity knowledge and skills on compliance, and, as a result, they argued that cybersecurity knowledge and skills can be a moderating factor in the relationship between awareness and compliance.

Lee & Kim (2023) also dealt with a similar issue, as well as Reddy & Rao (2016) explored an important task, namely the knowledge of cybersecurity issues. They conducted the study with respondents of multiple age groups and found that knowledge of cybersecurity issues and cybersecurity risks is positively related to cybersecurity behavior. In the multi-group analysis, the effect of cybersecurity risk on cybersecurity behavior was statistically significant.

Wu & Zhang (2019) focused on cybersecurity in companies and organizations where an important aspect is the employees themselves. The authors highlight the critical importance for the success of regular training programs and increasing cybersecurity awareness in organizations, identify best practices and provide actionable insights (linking cyber awareness to employees' personal lives). They recommend regular cybersecurity training to help employees recognize threats (such as phishing attacks) and respond appropriately. The result of working with employees is the creation of a culture of security, which means that every employee understands their role in protecting data and information systems.

A study by Fatoki et al. (2024) examines the relationship between employees' personal dispositions and their cybersecurity behaviors in companies and organizations. It examines how optimism bias influences attitudes (opinions) towards cybersecurity and consequently affects individuals' behavior. In addition, it examines the moderating role of cognition (knowledge and skills) about cybersecurity in shaping the relationship between attitudes and risk-taking behavior in the domain under study.

Research Framework and Methodology

According to the research plan, the main objective of the paper is to investigate the opinions of managers of companies operating in Slovakia on the level of knowledge and skills of employees in the field of cyber security, to focus in more detail on the knowledge and skills that employees lack most in the field of cyber security, to compare them with the knowledge and skills that are most valued in companies and to identify the parameters in which the opinions on the examined knowledge and skills differ.

Research Hypotheses

For our research, 4 research hypotheses formulated as null (H_0) alternative hypotheses (H_1) were proposed:

$1H_0$: The assessment of the level of the most lacking and most valued knowledge and skills of employees does not differ statistically significantly depending on the size of the companies.
$1H_1$: The assessment of the level of the most lacking and most valued knowledge and skills of employees differs statistically significantly depending on the size of companies.

$2H_0$: The assessment of the level of the most lacking and most valued knowledge and skills of employees does not differ statistically significantly by company´s ownership.
$2H_1$: The assessment of the level of employees' most lacking and most valued knowledge and skills differs statistically significantly by company´s ownership.

$3H_0$: The assessment of the level of the most lacking and most valued knowledge and skills of employees does not differ

statistically significantly according to the number of computers in the company.
$3H_1$: The assessment of the level of the most lacking and most valued knowledge and skills of employees differs statistically significantly according to the number of computers in the company.

$4H_0$: The assessment of the level of the most lacking and most valued knowledge and skills of employees does not differ statistically significantly according to the person responsible for cyber security in the company.
$4H_1$: The assessment of the level of the most lacking and most valued knowledge and skills of employees differs statistically significantly by the person responsible for cybersecurity in the company.

Research Model

The research was conducted in 3 main stages (Figure 1). In Stage 1, we focused on the study of scientific and professional literature with a focus on cybersecurity. In stage 2, the research hypotheses were formulated. At the same time, a research model (research variables model) was created to verify them. Stage 3 represented the statistical verification of the hypotheses and the formulation of conclusions.

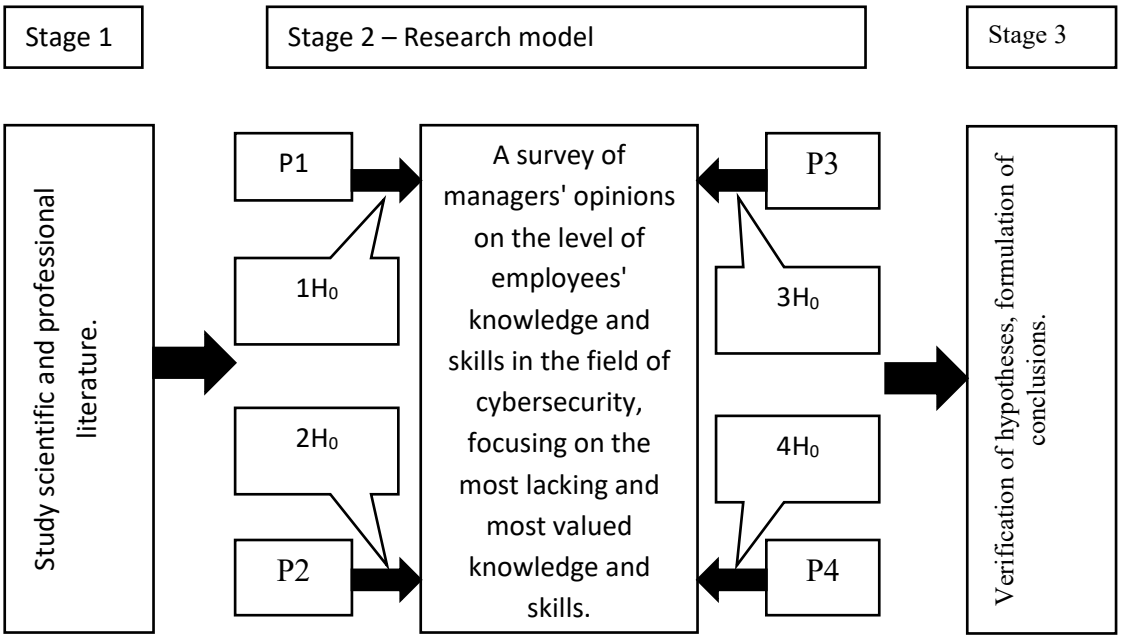

Fig 1. Research framework

(Source: prepared by authors)

In addition to the standard methods of scientific work (analysis, synthesis, comparison), other methods were used in the paper, namely the method of data collection and the method of evaluation of results. The source data were obtained from a questionnaire survey conducted in the months of January to June 2024 in companies operating in Slovakia. The questionnaire was conducted in electronic form, and the respondents were managers of companies whose competence included the area of cybersecurity. A total of 357 respondents were involved in the survey, divided into groups according to the size of the company,

its ownership, number of computers and the person responsible for cybersecurity.

Methods of evaluation of research variables: data were processed in Excel and statistical verification of hypotheses in Jamovi. These were the following statistical tests, tools and coefficients: descriptive statistics, Cronbach's α and McDonald's ω, Shapiro Wilk's test of normality and Levene's test of homogeneity of the research sample, and the non-parametric alternative of the ANOVA test (Kruskal - Wallis test).

Results and Discussion

This chapter presents the results of the questionnaire survey in the following structure: the reliability of the research tool, the research sample, the results of the evaluation of individual indicators according to the research model and the results of the statistical verification of the hypotheses.

Reliability of the research tool

The scale reliability of the A1 and A2 groups of variables reached α = 0.929, ω = 0.930 (overall). Reliability of individual variables reached α values ranging from 0.924 to 0.928, ω ranging from 0.925 to 0.929.

Although the above reliability values of our research instrument meet the required values of Cronbach's α > 0.7 (Hanak (2016), Kolarcik (2013), Marko (2016)), nevertheless, the calculation was supplemented with the McDonald's ω coefficient, whose values confirm sufficient internal consistency of the questionnaire used in the survey (Ullah, 2018; Marko, 2016).

Results of the questionnaire survey – research sample

The research sample was characterized based on the size of the company (P1), ownership (P2), total number of computers in the company (P3), and the person responsible for cybersecurity in the company (P4). The structure of the research sample is detailed in Table 1.

Table 1: Research sample

Parameters		No.	% share
P1 – company size	Small (min 10 - 49 employees)	168	47,06%
	Medium (50 - 249 employees)	89	24,93%
	Large (250+ employees)	100	28,01%
P2 – ownership	100% state ownership	25	7,00%
	Dominant domestic owner	46	12,89%
	Dominant foreign owner	43	12,04%
	Solely domestic owner	158	44,26%
	Solely foreign owner	85	23,81%
P3 – number of computers	1 - 10	57	15,97%
	11 - 50	165	46,22%
	51 - 100	31	8,68%
	101 - 500	67	18,77%
	>501	37	10,36%
P4 – person responsible for cybersecurity	Independent IS/IT department	182	50,98%
	Internal IS/IT specialist	25	7,00%
	External IS/IT specialist (outsourcing)	88	24,65%
	Director/ Security manager	62	17,37%

(Source: prepared by authors)

Results of the evaluation of the examined variables

Respondents' opinions were measured by two groups of variables. Both groups were rated on a 5-point Likert scale ranging from 0 to 4, with 0 meaning disagree not at all and 4 meaning agree completely. The first group consisted of variables A1.1, A1. 2.. A1.11, which characterized the knowledge and skills of employees in the field of cybersecurity that the company lacks most. The second group were variables A2.1, A2. 2...A2.11, which characterized the knowledge and skills in this area that the company values most. The variables of both groups had the same textual description that characterized their importance.

Table 2: Meaning of variables

Variables	Meaning of variables
A1.1, A2.1	IS/IT technological knowledge
A1.2, A2.2	Subject matter knowledge of the organization's operations
A1.3, A2.3	Subject matter knowledge of cybersecurity issues
A1.4, A2.4	Knowledge of financial management and budgeting
A1.5, A2.5	Knowledge of a foreign language
A1.6, A2.6	Ability to manage projects
A1.7, A2.7	Analytical skills
A1.8, A2.8	Flexibility and constructive approach to problem solving
A1.9, A2.9	Ability to communicate effectively with senior management
A1.10, A2.10	Presentation skills
A1.11, A2.11	Management skills

(Source: prepared by authors)

Table 3: Percentages of A1 variable group scores

Variable	Score					Mean	STDEV	Mode	Median
	0 (%)	1 (%)	2 (%)	3 (%)	4 (%)				
A1.1	4.20	14.29	26.89	31.09	23.53	2.55	1.12	3	3
A1.2	2.24	8.40	23.25	38.66	27.45	2.81	1.01	3	3
A1.3	4.76	16.53	27.45	26.05	25.21	2.50	1.17	2	3
A1.4	3.92	12.61	24.93	34.17	24.37	2.62	1.10	3	3
A1.5	3.36	10.92	21.57	30.25	33.89	2.80	1.12	4	3
A1.6	2.52	13.17	19.05	35.29	29.97	2.77	1.09	3	3
A1.7	3.36	10.36	22.13	34.45	29.69	2.77	1.09	3	3
A1.8	2.80	7.56	21.57	37.82	30.25	2.85	1.03	3	3
A1.9	3.36	10.08	16.53	38.10	31.93	2.85	1.08	3	3
A1.10	4.48	11.48	23.25	34.17	26.61	2.67	1.12	3	3
A1.11	3.64	8.96	20.73	36.13	30.53	2.81	1.08	3	3

(Source: prepared by authors)

Table 3 shows that the variables rated with the highest percentages (indicating that it is cybersecurity knowledge and skills that the company is most lacking) include:

- *Flexibility and Constructive Approach to Problem Solving* (A1.8), mean 2.85, with 68.07% of the ratings being at level 3 or 4, indicating that the majority of respondents are aware of a deficiency in this area.

- *Ability to communicate effectively with management* (A1.9), mean 2.85, with 70.03% of the ratings being at levels 3 or 4. This indicates the importance and relatively low level of this skill.
- *Management Skills* (A1.11), mean 2.81, with 66.66% of the assessments at level 3 or 4, indicating some difficulty.

The variables rated with the lowest percentages, the knowledge and skills that respondents rated as least lacking, were:

- *IS/IT Technology Knowledge* (A1.1), mean 2.55. Only 54.62% gave them a high rating of 3 or 4, the lowest of all variables. The highest percentage rating of 1 (14.29%) means that a large proportion of respondents are satisfied with their level.
- *Subject matter knowledge of cybersecurity issues* (A1.3), mean 2.50. The lowest mode (2) means that a rating of 2 was most common, indicating that more respondents identified these skills as least lacking.

Table 4: Percentages of A2 variable group scores

Variable	Score					Mean	STDEV	Mode	Median
	0 (%)	1 (%)	2 (%)	3 (%)	4 (%)				
A2.1	3.08	8.68	15.69	22.13	50.42	3.08	1.13	4	4
A2.2	1.68	7.84	18.21	34.45	37.82	2.99	1.01	4	3
A2.3	2.52	8.96	1.96	25.21	43.70	2.99	1.11	4	3
A2.4	5.88	11.48	22.97	33.61	26.05	2.62	1.16	3	3
A2.5	3.64	8.12	23.53	29.13	35.57	2.85	1.11	4	3
A2.6	3.36	7.28	17.65	39.78	31.93	2.90	1.04	3	3
A2.7	2.24	7.84	17.93	32.49	39.50	2.99	1.05	4	3
A2.8	1.40	5.04	15.97	29.69	47.90	3.18	0.97	4	3
A2.9	3.36	4.20	16.25	34.17	42.02	3.07	1.03	4	3
A2.10	3.92	8.12	24.09	35.85	28.01	2.76	1.07	3	3
A2.11	4.48	9.52	20.17	29.41	36.41	2.84	1.15	4	3

(Source: prepared by authors)

Table 4 shows the cybersecurity knowledge and skills that are most valued in companies. Variable A2.8 – *Flexibility and constructive approach to problem solving* had the highest mean score of 3.18, with 47.90% of respondents giving the highest score of 4 and only 1.40% giving a score of 0. This was followed by *IS/IT Technological Knowledge* (A2.1), which achieved an average value of 3.08. At the same time, up to more than 50% of the respondents reported the highest score of 4 followed by A2.9 – *Ability to communicate effectively with the management*, with an average of 3.07, 76.19% of the respondents reported ratings of 4 and 3, indicating that the respondents attach great importance to effective communication in the companies.

The lowest ratings, i.e. the knowledge and skills that respondents consider least valued, are given for A2.4 – *Knowledge of financial management and budgeting* (lowest mean of 2.62), followed by A2.10 – *Presentation skills* (mean of 2.76) and A2.11 – *Managerial skills* (mean of 2.84). Although these scores are the lowest, they are all above average.

Table 5: Comparison of evaluation results

Variables	Meaning of variables	Most lacking knowledge (A1)	Actual knowledge	Most valued knowledge (A2)	Difference (valued - actual)
A1.1, A2.1	IS/IT technological knowledge	2.55	1.45	3.08	1.63
A1.2, A2.2	Subject matter knowledge of the organization's operations	2.81	1.19	2.99	1.80
A1.3, A2.3	Subject matter knowledge of cybersecurity issues	2.5	1.50	2.99	1.49
A1.4, A2.4	Knowledge of financial management and budgeting	2.62	1.38	2.62	1.24
A1.5, A2.5	Knowledge of a foreign language	2.8	1.20	2.85	1.65
A1.6, A2.6	Ability to manage projects	2.77	1.23	2.9	1.67
A1.7, A2.7	Analytical skills	2.77	1.23	2.99	1.76
A1.8, A2.8	Flexibility and constructive approach to problem solving	2.85	1.15	3.18	2.03
A1.9, A2.9	Ability to communicate effectively with senior management	2.85	1.15	3.07	1.92
A1.10, A2.10	Presentation skills	2.67	1.33	2.76	1.43
A1.11, A2.11	Management skills	2.81	1.19	2.84	1.65

(Source: prepared by authors)

Table 5 contains comparisons of the variables under study A1 (most lacking knowledge and skills), A2 (most valued knowledge and skills), calculated actual knowledge and skills (based on a set maximum score), and the difference between the most valued and actual knowledge and skills, which determines the gap between what is valued and what employees actually possess.

The largest difference between valued and actual knowledge and skills was for the variables A1.8, A2.8 *Flexibility and constructive approach to problem solving* (difference of 2.03), with a value of 1.15 for actual knowledge being very low, despite the valued knowledge value of 3.18 being the highest in the table. We conclude that employees do not feel sufficiently prepared to solve problems and adapt to change.

Another pair of variables with a high difference between valued and actual knowledge and skills is *Ability to communicate effectively with management* (A1.9, A2.9), where the difference is 1.92, actual knowledge 1.15, valued knowledge 3.07. This difference may indicate the fact that employees lack the ability to effectively present and argue their propositions to the company management.

The third pair of variables in order is *Subject matter knowledge of the organization's operations* (A1.2, A2.2), the difference of valued and actual knowledge and skills is 1.80, actual knowledge 1.19, valued knowledge 2.99. This means that employees do not know the processes and structure of the organization well enough, which can cause problems in the coordination of teams.

Results of statistical significance of the hypotheses

Statistical verification of relationships between ordinal variables (P1, P2, P3, P4) and scale-type variables (A1, A2) was conducted using the ANOVA statistical test. To verify the assumptions for using the ANOVA test, two tests were used: the

Shapiro-Wilk test (to verify the normality of the research sample) and Levene's test (to verify the homogeneity of the research sample). Since normality and homogeneity of the research sample were not confirmed, we used the non-parametric Kruskal-Wallis test for testing. The results of the verification are presented in Tables 6 to 9. Statistically significant values of the Kruskal-Wallis test are marked with an asterisk (*).

Testing the statistical significance of hypothesis 1

Table 6: Results of statistical verification of the difference of variable A1 according to P1

	Shapiro Wilk Normality Test		Levene´s Test of Homogeneity				Kruskal Wallis Test			
	W	p	F	df1	df2	p	χ^2	df	p	ε^2
A1.1	0.9619	<.00001	4.00	2	354	0.0191	14.78	2	0.0006**	0.0415
A1.2	0.9192	<.00001	5.60	2	354	0.0044	2.39	2	0.2600	0.0076
A1.3	0.9609	<.00001	0.12	2	354	0.8864	17.47	2	0.0002**	0.0491
A1.4	0.9266	<.00001	2.98	2	354	0.0757	4.96	2	0.1142	0.0122
A1.5	0.9186	<.00001	3.66	2	354	0.0397	7.27	2	0.0252*	0.0207
A1.6	0.9112	<.00001	7.06	2	354	0.0010	2.46	2	0.3081	0.0066
A1.7	0.9424	<.00001	12.92	2	354	< .0001	12.00	2	0.0025*	0.0337
A1.8	0.9168	<.00001	5.15	2	354	0.0042	4.90	2	0.1103	0.0124
A1.9	0.8841	<.00001	8.02	2	354	0.0004	0.60	2	0.7427	0.0017
A1.10	0.9409	<.00001	8.13	2	354	0.0004	7.68	2	0.0226*	0.0213
A1.11	0.9236	<.00001	2.03	2	354	0.0742	8.06	2	0.0154*	0.0235

*Note: p values of the Kruskal Wallis test *p<0.05 **p<0.001 ***p<0.0001*
(Source: prepared by authors)

Table 7: Results of statistical verification of the difference of variable A2 according to P1

	Shapiro Wilk Normality Test		Levene´s Test of Homogeneity				Kruskal Wallis Test			
	W	p	F	df1	df2	p	χ^2	df	p	ε^2
A2.1	0.8846	<.00001	8.77	2	354	0.0002	22.23	2	< .0001***	0.0624
A2.2	0.8886	<.00001	2.63	2	354	0.1127	3.08	2	0.1628	0.0102
A2.3	0.9151	<.00001	3.10	2	354	0.0462	29.41	2	< .0001***	0.0826
A2.4	0.9173	<.00001	0.68	2	354	0.5055	4.13	2	0.1135	0.0122
A2.5	0.9128	<.00001	0.63	2	354	0.5350	7.20	2	0.0228*	0.0212
A2.6	0.8934	<.00001	0.80	2	354	0.4510	7.31	2	0.0214*	0.0216
A2.7	0.9166	<.00001	2.12	2	354	0.1218	21.32	2	< .0001***	0.0599
A2.8	0.8579	<.00001	0.32	2	354	0.7229	8.02	2	0.0181*	0.0225
A2.9	0.8547	<.00001	1.87	2	354	0.1469	4.25	2	0.0957	0.0132
A2.10	0.9243	<.00001	4.37	2	354	0.0137	7.47	2	0.0191*	0.0222
A2.11	0.9005	<.00001	0.69	2	354	0.5044	7.69	2	0.0201*	0.0220

*Note: p values of the Kruskal Wallis test *p<0.05 **p<0.001 ***p<0.0001*
(Source: prepared by authors

Testing the statistical significance of hypothesis 2

Table 8: Results of statistical verification of the difference of variable A1 according to P2

	Shapiro Wilk Normality Test		Levene´s Test of Homogeneity				Kruskal Wallis Test			
	W	p	F	df1	df2	p	χ^2	df	p	ε^2
A1.1	0.9559	<.00001	4.46	4	352	0.0015	15.32	4	0.0041*	0.0430
A1.2	0.9129	<.00001	4.15	4	352	0.0018	1.28	4	0.7536	0.0053
A1.3	0.9592	<.00001	3.17	4	352	0.0142	15.18	4	0.0044*	0.0426
A1.4	0.9373	<.00001	4.08	4	352	0.0030	4.68	4	0.3574	0.0123
A1.5	0.9261	<.00001	2.93	4	352	0.0424	9.06	4	0.0597	0.0254
A1.6	0.9335	<.00001	3.19	4	352	0.0049	9.15	4	0.0575	0.0257
A1.7	0.9312	<.00001	4.50	4	352	0.0013	7.80	4	0.0954	0.0222
A1.8	0.8988	<.00001	0.97	4	352	0.4242	2.02	4	0.7318	0.0057
A1.9	0.8801	<.00001	1.17	4	352	0.3236	1.25	4	0.8626	0.0036
A1.10	0.9381	<.00001	2.44	4	352	0.0486	6.35	4	0.1524	0.0188
A1.11	0.9312	<.00001	2.62	4	352	0.0339	15.77	4	0.0033*	0.0443

*Note: p values of the Kruskal Wallis test *p<0.05 **p<0.001 ***p<0.0001*
(Source: prepared by authors)

Table 9: Results of statistical verification of the difference of variable A2 according to P2

	Shapiro Wilk Normality Test		Levene´s Test of Homogeneity				Kruskal Wallis Test			
	W	p	F	df1	df2	p	χ^2	df	p	ε^2
A2.1	0.8826	<.00001	4.70	4	352	0.0017	19.99	4	0.0005**	0.0562
A2.2	0.8970	<.00001	1.12	4	352	0.1425	5.01	4	0.2616	0.0148
A2.3	0.9162	<.00001	2.24	4	352	0.0662	32.55	4	<.0001***	0.0914
A2.4	0.9237	<.00001	1.28	4	352	0.1147	3.13	4	0.5370	0.0088
A2.5	0.9291	<.00001	2.05	4	352	0.0281	18.91	4	0.0008**	0.0531
A2.6	0.8890	<.00001	1.67	4	352	0.2279	6.79	4	0.1587	0.0185
A2.7	0.8883	<.00001	0.78	4	352	0.5417	8.18	4	0.0852	0.0230
A2.8	0.8737	<.00001	0.57	4	352	0.6814	12.72	4	0.0144*	0.0349
A2.9	0.8544	<.00001	1.04	4	352	0.3855	5.06	4	0.2811	0.0142
A2.10	0.9433	<.00001	1.09	4	352	0.2044	16.86	4	0.0021**	0.0474
A2.11	0.9183	<.00001	2.36	4	352	0.0237	9.01	4	0.0418*	0.0279

*Note: p values of the Kruskal Wallis test *p<0.05 **p<0.001 ***p<0.0001*
(Source: prepared by authors)

The other two hypotheses were tested in the same way. In the case of hypothesis 3 (difference of variable A1, A2 according to P3), 6 out of 11 sub-variables for variable A1 and 7 out of 11 sub-variables for variable A2 were statistically significant.

A similar situation occurred in the verification of hypothesis 4 (difference of

variable A1, A2 according to P4). In this case, 5 out of 11 sub-variables (for A1) and 4 out of 11 (for A2) were statistically significant.

In neither case was significance shown for all the sub-variables, but only for some of them, so we have to reject the alternative hypotheses $1H_1$, $2H_1$, $3H_1$ a $4H_1$ and accept the null hypotheses $1H_0$, $2H_0$, $3H_0$ a $4H_0$.

Conclusion

The main objective of the paper was to examine the opinions of managers of companies operating in Slovakia on the level of knowledge and skills of employees in the field of cybersecurity. To focus in more detail on the knowledge and skills that employees lack most in the field of cybersecurity, to compare them with the knowledge and skills that are most valued in companies and to identify the parameters in which the assessments of each group of respondents on the surveyed knowledge and skills differ. The results are detailed in the text of the paper and in Tables 3 to 5. Interestingly, however, the most lacking and at the same time the most valued knowledge and skills are *Flexibility and constructive approach to problem solving* and *Ability to communicate effectively with the management of the company*. In contrast, *IS/IT technology skills*, which are also among the most valued, were ranked as the least lacking by respondents.

No statistical significance could be shown for the differences in responses by size of the company, structure of owners, total number of computers in the company, or by the person responsible for cyber security, although several of the sub-variables are statistically significant.

The analyzed literature as well as our results show that companies should conduct regular training aimed at improving employees' soft skills (e.g. effective communication) in addition to learning about cyber security issues and their development. In order to achieve the goal of creating a culture of security in the company, the personal dispositions and characteristics of the employees should not be forgotten.

Suggestions for further research are seen in a repeated survey on either the same sample of companies or an extension of the research sample.

Acknowledgment

The paper was elaborated within VEGA No. 1/0662/23 - Digital transformation of companies and their readiness to integrate the elements of Industry 5.0 – proportion 50 % and VEGA No. 1/0520/24 - Aspects of building an ambient enterprise ecosystem – proportion 50 %.

References

- CMS. (2025.) 'Data protection and cybersecurity laws in Slovakia', [Online], [Retrieved February 15, 2025] https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/slovakia.
- Cybercompetence. (2025). 'Cyber security competence and certification centre. Courses and workshops', [Online], [Retrieved February 20, 2025] https://cybercompetence.sk/kurzy-a-workshopy/.
- European Commission. (2024). 'A safer digital future: new cyber rules become law ', [Online], [Retrieved February 05, 2025] https://commission.europa.eu/news/safer-digital-future-new-cyber-rules-become-law-2024-12-10_en.
- Fatoki, J. G., Shen, Z., & Mora-Monge, C. A. (2024). 'Optimism amid risk: How non-IT employees' beliefs affect cybersecurity behavior', *Computers & Security, 141, 103812*.
- H&P Magazine. (2025). 'Cybersecurity obligations extend to a wider range of companies', [Online], [Retrieved February 21, 2025] https://magazin.havelpartners.cz/2025-01/bezpecne-a-podla-pravidiel.html.
- Hanak, R. (2016). *'Data analysis for the social sciences'*. Bratislava: Ekonóm.

[Online], [Retrieved February 20, 2025] https://statistikapspp.sk/ucebnica/datova-analyza-pre-socialne-vedy/.

- He, W. & Zhang, Z. (2019). 'Enterprise cybersecurity training and awareness programs: Recommendations for success', *Journal of Organizational Computing and Electronic Commerce, 29(4), 249-257.*
- Kolarcik, P. (2013). 'Statistical data processing', [Online], [Retrieved February 20, 2025] http://sodezz.upol.cz/soubory/2013_kvantita/sodezzkvantita2_zamcene.pdf.
- Kost, E. (2025) 'Ultimate Guide to Cybersecurity Reports in 2025', [Online], [Retrieved February 05, 2025] https://www.upguard.com/blog/cyber-security-reports .
- Lee, C. S. & Kim, D. (2023). 'Pathways to cybersecurity awareness and protection behaviors in South Korea'. *Journal of Computer Information Systems,* 63(1), 94-106.
- Marko, M. (2016). The use and misuse of Cronbach's alpha in the evaluation of psychodiagnostic instruments', *Testfórum, (7), 99-107.*
- MIRRI. (2024). 'Central Cyber Security Portal. Acquisition, development and maintenance: Key aspects of cyber security', [Online], [Retrieved February 18, 2025] https://kyberportal.slovensko.sk/aktuality/akvizicia-vyvoj-a-udrzba-klucove-aspekty-kybernetickej-bezpecnosti/.
- MIRRI. (2025). 'Central Cyber Security Portal. Basic information', [Online], [Retrieved February 20, 2025] https://kyberportal.slovensko.sk/znalostna-baza/zakladne-informacie/.
- O2 Business Services .(2025). '5 tips on how to train your employees in cybersecurity', [Online], [Retrieved February 20, 2025] https://business.o2.sk/blog/5-tipov-ako-skolit-vasich-zamestnancov-v-oblasti-kyberbezpecnosti.
- Reddy, D., & Rao, V. (2016). 'Cybersecurity skills: The moderating role in the relationship between cybersecurity awareness and compliance'.
- Suryotrisongko, H. & Musashi, Y. (2019). 'Review of cybersecurity research topics, taxonomy and challenges: Interdisciplinary perspective', *In 2019 IEEE 12th conference on service-oriented computing and applications (SOCA) (pp. 162-167). IEEE.*
- Ullah, I. M. (2018). 'Cronbach's Alpha Reliability Analysis of Measurement Scales', [Online], [Retrieved February 14, 2025] https://itfeature.com/stat-soft/spss/cronbachs-alpha-reliability/.
- World Economic Forum. (2024). 'Cybersecurity rules saw big changes in 2024. Here's what to know ' ,[Online], [Retrieved February 10, 2025] https://www.weforum.org/stories/2024/10/cybersecurity-regulation-changes-nis2-eu-2024/