DOI: 10.55643/fcaptp.4.69.2026.5291

CONVINCED BUT UNPREPARED: A PILOT MEASUREMENT OF CYBERSECURITY PREPAREDNESS IN SLOVAK SMES

Jakub Sopko
PhD in Economics, Assistant Professor of the Department of Banking and Investment, Faculty of Economics, Technical University of Košice, Košice, Slovakia;
e-mail: jakub.sopko@tuke.sk
ORCID: 0000-0002-7314-828X
(Corresponding author)

Leoš Šafár
PhD in Economics, Assistant Professor of the Department of Banking and Investment, Faculty of Economics, Technical University of Košice, Košice, Slovakia;
ORCID: 0000-0001-8466-0644

ABSTRACT

Small and medium-sized enterprises (SMEs) are increasingly becoming targets of cyberattacks. Their preparedness in Slovakia, however, is rarely measured. This study develops and pilots a survey instrument for assessing the cybersecurity preparedness of SMEs. The questionnaire has six parts. Four of them contain an attitudinal scale and form the measured dimensions of preparedness: technological preparedness and compatibility, process preparedness and response management, the perceived benefit of cybersecurity technologies for employees, and strategic and development orientation. The pilot survey was completed by 25 Slovak SMEs. We verified the data using Cronbach's alpha, corrected item-total correlations, and principal component analysis with Varimax rotation, together with the Kaiser-Meyer-Olkin measure and Bartlett's test of sphericity. All four dimensions show acceptable internal consistency (alpha 0.673 to 0.886), and three exceed the 0.7 threshold. The technological dimension is unidimensional and explains 60.27 per cent of response variance. One problematic item was identified in the employee dimension; its removal raises alpha from 0.673 to 0.779. The rotated component matrix indicates that the strategic-financial dimension splits into two subscales: economic awareness and strategic-innovation orientation. Descriptive findings reveal a consistent gap between implementation and verification. Basic technical controls are widespread, while measures that verify their effectiveness lag behind. Regular backups are performed by 19 of the 25 firms, but only 11 test whether data can be restored. The study delivers a revised measurement framework ready for data collection on a large representative sample. It thus provides a methodological basis for the systematic data collection of cybersecurity preparedness of Slovak SMEs.

Keywords: cybersecurity, small and medium-sized enterprises, preparedness, survey, Slovakia

JEL Classification: M15, G32, D81, L26, C83

INTRODUCTION

Digital transformation has brought new opportunities for businesses, but also new risks. According to the Allianz Risk Barometer survey, cyber incidents were the biggest global business risk for 2025 (Allianz Commercial, 2025). The World Economic Forum (2026) ranks cyber insecurity among the six most significant risks over a two-year horizon, and the Allianz Risk Barometer (2026) identifies cyber incidents as the top global business risk for the fifth consecutive year. The main cause of insurance claims is ransomware, and the pressure from attackers on sensitive data is also growing. A cyber attack is no longer just a technical complication. For a small or medium-sized enterprise (SME), it represents a traumatic event that can threaten its turnover, reputation and business continuity, and in extreme cases even its very solvency (Renaud and Weir, 2016).

The significance of this topic is highlighted by the macroeconomic importance of the SME sector. Small and medium-sized enterprises (SMEs) account for approximately 90 per cent of businesses worldwide and more than half of global employment. In the European Union, they represent over 99 per cent of all businesses (Arroyabe et al., 2024b). SMEs also form the backbone of the Slovak economy, so their resilience to cyber threats is a question of economic stability rather than a purely technical concern.

Received: 01/07/2026
Accepted: 19/08/2026
Published: 31/08/2026

At the same time, SMEs are more vulnerable than large enterprises, and attackers increasingly target them as the weakest point of supply chains. The economic case for protecting this segment therefore rests on two questions. Firstly, how large the losses from cyber incidents are, and secondly, how much effective defence costs. In Slovakia, small and medium-sized enterprises account for 99.9 per cent of all businesses, employ approximately 74 per cent of the business workforce, and generate 55 per cent of added value, with 97 percent of them being micro-enterprises with fewer than ten employees (SBA, 2026). The resilience of this segment is therefore a macroeconomic question for a small open economy.

The financial losses involved are substantial. The average cost of cybercrime for an affected organisation rose from USD 11.7 million to USD 13 million between 2017 and 2018 (Accenture, 2019). Industry reporting places the average cost of a data breach at USD 4.45 million and of a ransomware attack at USD 1.85 million per incident, including ransom payments and system restoration expenses (Fotis, 2024). Firm-level evidence nevertheless cautions against reading these averages as typical. Romanosky (2016) estimates the cost of a typical cyber incident at below USD 200,000, or about 0.4 per cent of annual revenue, which is less than routine losses from fraud or theft. The distribution of losses, however, has a heavy tail. Vidović and Beriša (2025) report median direct losses of about USD 0.4 million across 31 documented incidents, with extremes reaching billions of dollars, in some cases 2 to 2.5 per cent of national GDP. Indirect and hidden costs, such as reputational damage, legal liabilities and lost customer trust, often exceed the direct costs and can persist for five years or more after the incident (Tahmasebi, 2024; Vidović and Beriša, 2025). For an SME with thin liquidity buffers, even a below-average loss can therefore be existential. A substantial part of this damage falls on the intangible component of business value. Reputation, brand and customer loyalty constitute goodwill, which is increasingly important for firm value yet remains inadequately recognised and disclosed in financial reporting, so losses of this kind are rarely visible in the accounts (Semenova et al., 2024).

Firms and governments respond to this exposure with rapidly growing spending on cyber defence. Global spending on cybersecurity grew from USD 75.6 billion in 2015 to USD 124 billion in 2020 and was projected to reach USD 133.8 billion in 2022 (Lee, 2021). The global cybersecurity market as a whole is expected to expand from USD 89.72 billion in 2017 to USD 271.90 billion in 2029, a compound annual growth rate of 9.68 per cent (Lakhtionova, 2025). The spending stands against estimated global losses approaching one trillion dollars, which suggests that the economy as a whole is still under-spending on protection and that the key question is not only how much to spend, but how effectively (Wirth, 2017). Among organisations covered by the EU NIS framework, cybersecurity absorbs about 9 per cent of IT budgets (ENISA, 2025). For SMEs, the picture is less favourable. Threat exposure in Europe has grown faster than their defensive expenditure (Porkoláb-Angyalos and Szilágyi, 2026). Protection is economically feasible precisely because prevention is cheaper at the margin than the expected loss it averts. The practical task is to allocate limited budgets to the controls with the highest loss-reducing effect (Lee, 2021).

Regulatory pressure on the sector is also rising. The NIS2 Directive extends cybersecurity obligations to a far wider range of entities than its predecessor, including many medium-sized firms previously outside its scope. Documenting a firm's own preparedness is therefore becoming a practical requirement. Slovakia achieves a good rating at the national level in the Global Cybersecurity Index (ITU, 2024). At the business level, however, the picture is different. According to a survey by the National Security Authority, as many as 60.5 per cent of Slovak SMEs do not provide any training in cybersecurity, and almost half consider their employees' digital skills to be inadequate (NSA, 2023b).

Improving preparedness first requires the ability to measure it. However, the literature repeatedly highlights a lack of quantitative research focusing specifically on the cybersecurity of SMEs (Chidukwani et al., 2022; Tam et al., 2021), and the Slovak context lacks a validated and cost-effective measurement tool that would cover technologies, processes, people and finances simultaneously. This article addresses this gap. We present a questionnaire tool developed on the basis of international literature and cyber insurance practice, and are pilot-testing it on a sample of 25 Slovak SMEs. We place emphasis on the validation of the scales, the internal consistency of the question scales, and their dimensionality. We regard the pilot validation as a first step. Its output is a refined set of items that can be deployed in the forthcoming data collection from a large sample of enterprises. The economic dimension of preparedness, that is, losses, spending, insurance and the willingness to invest, is measured even less often than the technical one. The survey presented here therefore includes a separate financial dimension.

LITERATURE REVIEW

Cyber risk is an interdisciplinary phenomenon. It brings together information technology, finance and economics, and can be defined as the operational risk associated with information and technology assets, with implications for the confidentiality, availability and integrity of information (Pacelli, 2025). Threats are constantly evolving, and their impacts include

DOI: 10.55643/fcaptp.4.69.2026.5291

both financial losses and reputational damage (Darem et al., 2023). The economic perspective on information security has a solid theoretical foundation. Anderson and Moore (2009) demonstrate that security failures often arise not from technical but from economic causes, such as moral hazard, externalities, and misperceptions of risk. Empirical estimates of damages are, however, uncertain. Anderson et al. (2013) highlight methodological weaknesses in measuring the costs of cybercrime, while Riek and Böhme (2018) demonstrate that many published estimates lack scientific rigour. Event studies in capital markets find only a limited direct impact of incidents on firm value, depending on the type of incident (Campbell et al., 2003; Kamiya et al., 2021), whereas Amir et al. (2018) document that firms systematically under-report incidents associated with a significant decline in value. These findings explain why measuring preparedness at the firm level is necessary, yet methodologically challenging.

Heidt et al. (2019) document the security gap between SMEs and large enterprises in the form of limited budgets, a lack of specialised roles and a different logic underpinning investment decisions. ENISA data confirm a significant difference in resources, with only 5 per cent of SMEs surveyed in the EU having cyber insurance, compared with 39 per cent of large enterprises (ENISA, 2022). Kabanda et al. (2018) show that SMEs' security practices are shaped by resource constraints and management attitudes. Osborn and Simpson (2018) describe informal risk decision-making in small organisations, while Paulsen (2016) points out that standard frameworks are difficult for small businesses to grasp. At the same time, review studies note that, despite the sector's importance, research into SME cybersecurity remains scarce (Chidukwani et al., 2022; Tam et al., 2021). Attackers exploit SMEs as a gateway into the supply chains of larger organisations, so the consequences of their failure extend beyond the boundaries of the enterprise itself (Lloyd, 2020; Sawik, 2022). For the firm itself, an attack can threaten turnover, reputation, business continuity and, in extreme cases, solvency (Renaud and Weir, 2016). Overconfidence contributes to this exposure. Benz and Chatterjee (2020) report that up to 95 per cent of IT leaders in SMEs consider their security to be above average, even though more than half of these businesses have no up-to-date cyber risk management strategy. Alahmari and Duncan (2020) reach a similar conclusion: SME management systematically underestimates cyber threats, which raises vulnerabilities both for the firms themselves and for the parties connected to them.

Chidukwani et al. (2024) studied SMEs in Western Australia using a convenience sample of 36 businesses, considering a response valid if at least half of the questions had been answered. They identified a lack of funding and a lack of knowledge about where to start with security as the greatest barriers; businesses were unfamiliar with frameworks such as the NIST CSF and obtained information mainly through internet searches and from IT suppliers. The authors also document the discrepancy between stated responsibilities and actual practice, and draw particular attention to the gap between backup procedures and testing the recoverability of backups. They describe preparedness in terms of the proportion of measures implemented and the distribution of attitudinal responses, without inferential testing, precisely in view of the scope and method of sample selection. We follow the same logic in our paper. Valli et al. (2014) previously focused on the Australian population and found a low level of security awareness despite the widespread use of basic technical tools. Franke and Wernberg (2020) document a systematic preference for technical measures, such as updates and backups, and an under-representation of soft organisational and personnel measures in Swedish manufacturing firms. Renaud and Ophoff (2021) address the question of where SMEs seek security advice and why they often fail to find it. Bada and Nurse (2019) follow this up with proposals on how to design training programmes for SMEs in such a way that they lead to verifiable skills. Papathanasiou et al. (2025) respond to these barriers with a practical framework for SMEs that combines technical measures, employee training and regulatory compliance, and stress that the human factor remains the cheapest point of intervention. Regulatory awareness shows the same pattern as security awareness. For example, in a European survey on the Cyber Resilience Act, 66 per cent of SME respondents had heard of the regulation, yet few understood its requirements, and financial support was among the most frequently requested forms of assistance (ENISA, 2026c).

Hasani et al. (2023) applied the technology–organisation–environment framework (TOE; DePietro et al., 1990). They demonstrated that the adoption of cybersecurity technologies is significantly influenced by compatibility, perceived usefulness and ease of use, organisational flexibility, and support from senior management, with adoption subsequently enhancing both financial and non-financial performance. Our survey section on technological readiness and compatibility ties in directly with the technological context of this framework. Benz and Chatterjee (2020) address the complexity of comprehensive frameworks and have simplified the NIST CSF into a practical assessment tool for SMEs, and the Cyber Resilience Review methodology (CISA, 2020) follows the same principle of simplicity. Fielder et al. (2016) model the optimal allocation of a limited security budget as a decision-making problem. Dinkova et al. (2024) construct a cyber maturity indicator by linking a representative survey with tax data from Dutch firms, and find an inverted U-shaped relationship between maturity and the probability of a reported incident. Based on their results, basic measures primarily improve incident detection, while more advanced measures prevent them. However, they do not confirm a relationship between maturity and profitability. This implies an important methodological lesson for surveys. The number of reported incidents is a function not

only of exposure but also of a company's ability to detect incidents in the first place. Risk transfer is a separate issue. Cyber insurance plays a dual role in the SME sector because it covers residual risk and, at the same time, through the underwriting process, creates pressure to meet a minimum-security standard. However, its penetration in the SME sector remains low (ENISA, 2022; Lloyd, 2020).

Arroyabe et al. (2024b) analyse data from 12,863 European SMEs and identify four business profiles. Concern about cybercrime is higher among firms with more intensive online activities and previous cyber incidents. The impact of past incidents also affects perceived cyber risk. Some firms respond by restricting their online activities, which can reduce their business activity. Wells et al. (2014) had previously pointed out that attacks in industry threaten both product integrity and human safety, and therefore training the workforce is critical. Zimmermann and Renaud (2019) propose a shift from viewing people as the problem to viewing them as part of the solution, which shifts the focus from technical controls to building competencies and a safety culture.

A separate stream of literature examines the economics of cyber losses and security investment, and it frames the financial dimension of our survey. Estimates of cyber losses vary considerably. A typical incident costs less than USD 200,000 (Romanosky, 2016), while extreme events can result in losses of billions (Vidović and Beriša, 2025). Some costs also persist for years after the incident (Tahmasebi, 2024). Evidence from listed firms is less clear. Celeny et al. (2024) find that the stock-market reaction becomes statistically weak after correcting standard errors. Data breaches, however, remain the most damaging type of incident. This weak market discipline matters for SMEs. If even listed firms face limited external pressure, unlisted small firms face almost none. On the investment side, SMEs should invest up to the point where the marginal cost of defence equals the marginal reduction in expected loss (Lee, 2021; Fielder et al., 2016). Applying this rule presupposes that a firm can quantify its exposure, which SMEs typically cannot. Approaches such as real cyber value at risk (RCVaR) therefore estimate attack costs from industry data (Franco et al., 2024). Empirically, the return on compliance-driven security investment differs sharply across sectors, and inexpensive controls such as multi-factor authentication and zero-trust architectures are among the strongest predictors of breach resilience (Mayeke, 2025). Reviews consolidating this evidence link security capability to profitability and business continuity (Liu and Babar, 2026; Al Aamer and Hamdan, 2023). Arroyabe et al. (2024a) offer a structural explanation for why SMEs nevertheless do not invest more in cyber defence. Cybersecurity behaves as a merit good under market failure, marked by information asymmetry and managerial myopia, so that neither incidents nor their impacts reliably trigger implementation. Macro-level evidence points in the same direction. The threat exposure of European SMEs grew faster than their defensive spending between 2015 and 2020, and the NIS2 Directive acts as a regulatory shock that lifts spending in the short run without guaranteeing long-term convergence (Porkoláb-Angyalos and Szilágyi, 2026). EU-level monitoring of sector maturity has expanded accordingly (ENISA, 2024, 2026a).

The literature review reveals two gaps. Firstly, existing tools are designed for different institutional contexts and have not been validated in the Slovak context. Secondly, few studies explicitly document the reliability of the scales used, even though this is a prerequisite for the comparability of results over time and across countries, with the exception of studies that report threshold values for Cronbach's alpha and convergent validity (Hasani et al., 2023). We have deliberately drawn our theoretical and methodological foundations from the global literature. International findings cannot be automatically applied to Slovak SMEs. The institutional framework, sector structure, and regulatory environment vary between countries, which limits direct comparability. Slovakia lacks a comparable enterprise-level data set. What is available consists primarily of institutional overviews without a measurement tool of documented reliability (NSA, 2023a, 2023b). The economic evidence itself is concentrated on large firms, while enterprise-level instruments rarely connect preparedness with its financial dimension, that is, with losses, spending and risk transfer. Our survey addresses this by measuring a strategic-financial dimension alongside the technical, process, and human ones.

AIMS AND OBJECTIVES

The main objective of this article is to conduct a pilot test of a questionnaire tool designed to measure the preparedness of Slovak SMEs for cyber threats. We pursue this through three sub-objectives:

1. We aim to verify the internal consistency of the four proposed dimensions using Cronbach's alpha and item analysis.
2. We assess the dimensionality of the scales using principal component analysis.
3. We identify problematic items and propose a revised structure for the tool for the planned data collection from a large sample of enterprises.

DOI: 10.55643/fcaptp.4.69.2026.5291

4. We provide an economic and financial interpretation of the pilot results, relating the observed preparedness patterns to the economics of security investment.
5. We formulate a set of economic proposals for SMEs on the implementation of cyber defence, derived from the gaps identified in the pilot.

MEHODS

We designed the tool by combining several sources. The starting point was the Cyber Resilience Review questionnaire (CISA, 2020), which is based on the CERT resilience management model. The second source was cyber insurance underwriting questionnaires from Colonnade Insurance S.A., which reflect insurers' information needs when assessing risk. The third source comprised threat perceptions and technical measures according to Chidukwani et al. (2024) and Arroyabe et al. (2024b). We followed the technological and organisational context of cybersecurity adoption according to Hasani et al. (2023) and a simplified assessment framework based on NIST, in line with the tool developed by Benz and Chatterjee (2020).

The questionnaire comprised six sections: general information, systems and security, response plans and incident management, staff and training, finance and future developments, and cyber insurance. The sections differ in the type of questions they contain. The first part records the characteristics of the respondent and the firm. The sixth part contains a binary question on insurance together with supplementary reasons. Parts two to five each contain, alongside factual questions, one attitudinal battery rated on a seven-point Likert scale (1 = strongly disagree, 7 = strongly agree). Hasani et al. (2023) used the same scale format. These four sections represent the dimensions of preparedness examined in the validation analysis. The first and sixth sections do not contain scale items. They are used for descriptive purposes. Table 1 links the structure of the questionnaire to the validated dimensions.

Table 1. Link between the questionnaire structure and the validated dimensions. Note: Item wording was recoded into short labels for presentation purposes (TECH1 to TECH7, PROC1 to PROC3, EMP1 to EMP3, FIN1 to FIN7). Full item wording is available from the authors.

Part	Questionnaire part	Items		Measured dimension
1	General information	–	–	Descriptive characteristics
2	Systems and security	TECH	TECH1 to TECH7	Technological preparedness and compatibility
3	Response planning and incident management	PROC	PROC1 to PROC3	Process preparedness and response management
4	Employees and training	EMP	EMP1 to EMP3	Perceived benefit of technologies for employees
5	Finance and future development	FIN	FIN1 to FIN7	Strategic and development orientation
6	Cyber insurance	–	–	Binary question and reasons

Data were collected between 5 March 2026 and 10 April 2026 using Google Forms. Participation was anonymous and voluntary. Invitations were sent to 288 SMEs identified in the Finstat.sk database. This database was selected because it is the only publicly available Slovak database that allows firms to be filtered simultaneously by headcount, turnover, region, and industry, that is, by the criteria of the applicable SME definition (MIRRI SR, 2025). A total of 29 responses were received. Two respondents declined to participate, and two firms were excluded for exceeding the limit of 250 employees. The final sample comprises 25 firms, corresponding to a response rate of 8.7 per cent. The questionnaire was completed predominantly by owners and managing directors. Nineteen respondents were male, and the largest age group was 26 to 35 years. Small firms (10 to 49 employees) predominated in the sample, as did the limited liability company legal form (21 firms) and firms operating for more than ten years. Manufacturing and industry were the dominant sector (10 firms). The Košice and Prešov regions were the most represented (8 firms each).

To assess the structure of the pilot sample, we compared it with the 2023 survey of Slovak SMEs conducted for the National Security Authority and the Cyber Security Competence and Certification Centre (NSA, 2023b) and with the analysis of the Slovak Business Agency (SBA, 2026). SBA (2026) stated that, for 2025 in Slovakia, there are more than 97 per cent of Micro firms, about 2 per cent of small firms, and below 1 per cent of medium-sized enterprises. Comparing with our pilot sample, the structure is 7 micro firms (28 per cent), 14 small firms (56 per cent) and 4 medium firms (16 per cent). The survey by NSA (2023b) included small and medium-sized firms, but not micro firms. Among the 18 comparable non-micro firms in our pilot, 14 were small (77.8 per cent) and four were medium-sized (22.2 per cent). The corresponding shares in the national benchmark were 82.5 per cent and 17.5 per cent. The size composition is therefore reasonably close within the comparable part of the pilot. Sector composition is less similar. Manufacturing and industry account for 10 of the 25

pilot firms, compared with 24.5 per cent in the national benchmark. Regional concentration is stronger, where 16 of the 25 firms are located in the Košice or Prešov regions, while the Trnava and Trenčín regions are absent. The pilot should therefore not be treated as regionally or sectorally representative.

The size of the sample is consistent with the character of a pilot study. Johanson and Brooks (2010) treat approximately 30 respondents as a reasonable minimum for piloting an instrument, and Hertzog (2008) accepts samples of 10 to 40 units for initial pilot phases. The present sample lies within this range. The 25 observations are therefore used to examine item behaviour, feasibility and internal consistency. They are not used to estimate national prevalence or to establish a final factor structure. Comparable constraints are common in this field of research. Chidukwani et al. (2024) worked with a convenience sample of 36 firms and rejected probability sampling precisely because of the expected reluctance of SMEs to participate in research on a sensitive topic. Low willingness to answer questions about a firm's own security is therefore a systematic feature of this research field, and not solely a limitation of the present data collection.

Internal consistency was assessed using Cronbach's alpha (Warrens, 2015). De Vaus (2002) treats values above 0.7 as desirable, notes that values above 0.9 may indicate item redundancy, and accepts values between 0.6 and 0.7 for scales with few items. Corrected item-total correlations (CITC) were analysed, with 0.3 as the conventional lower bound, together with alpha if the item was deleted. Principal component analysis (PCA) was used only as a secondary exploratory diagnostic. Components with eigenvalues above 1 were inspected. Sampling adequacy was screened using the Kaiser-Meyer-Olkin measure (KMO) and Bartlett's test of sphericity, with 0.5 treated as the minimum acceptable KMO value (Kaiser, 1974). Communalities and the variance explained by the first component were also examined. Varimax rotation with Kaiser normalisation was applied to dimensions with heterogeneous content (de Vaus, 2002). Confirmatory factor analysis was deliberately not performed, given the size of the sample, and is left for the large-scale data collection. Calculations were performed in IBM SPSS Statistics v. 25. Descriptive processing and data recoding were carried out in RStudio and MS Excel.

RESULTS

Table 2 summarises the reliability of the four dimensions and the assumptions of the component analysis. Three dimensions exceed the 0.7 threshold for alpha. The dimension of perceived benefit for employees falls within the 0.6 to 0.7 range. No dimension exceeds 0.9. Bartlett's test of sphericity is statistically significant in all dimensions. KMO exceeds the 0.5 threshold in all of them. Values of 0.821 and 0.747 were obtained for the seven-item dimensions, and values of 0.554 and 0.586 for the three-item dimensions. Our four dimensions correspond to distinct parameters of cyber risk. The technological dimension captures the capacity to prevent losses, and the process dimension the ability to contain the severity of a loss once an incident occurs. The employee dimension captures the exposure arising from the human factor, and the financial dimension captures the firm's stance on security investment. The dimensions thus measure the determinants of expected loss together with the firm's investment response, which is in line with Lee (2021).

Table 2. Descriptive statistics of the preparedness dimensions. Note: KMO = Kaiser-Meyer-Olkin measure of sampling adequacy; α (std.) = alpha based on standardised items.

Dimension	Items	Cronbach's α	α (std.)	KMO	Bartlett χ^2 (df); p	PCA variance	Recommendation
A – Technological preparedness (TECH)	7	0.886	0.888	0.821	89.87 (21); < 0.001	60.27 %	Retain all items
B – Process preparedness (PROC)	3	0.728	0.728	0.554	18.64 (3); < 0.001	65.33 %	Retain; monitor PROC1
C – Perceived benefit for employees (EMP)	3	0.673	0.672	0.586	13.99 (3); 0.003	61.30 %	Move EMP3 to a separate set of items
D – Strategic orientation (FIN)	7	0.835	0.820	0.747	76.56 (21); < 0.001	69.00 % (2 comp.)	Split into two subscales

The technological preparedness dimension (seven items) reaches an alpha of 0.886 (Table 2). Item means range from 4.48 to 5.68 (Table 3). The highest proportion of agreement was recorded for TECH4 (76 per cent) and TECH5 (72 per cent). All CITC values fall between 0.543 and 0.788, and deleting any item would reduce alpha. All communalities exceed 0.3, and the first component explains 60.27 per cent of response variance. Based on this, the firms perceive security

DOI: 10.55643/fcaptp.4.69.2026.5291

primarily as protection of operational continuity and market credibility, that is, as a revenue-protecting asset rather than a pure cost item (Lloyd, 2020). The high score for compatibility (TECH7) also matters economically, because compatible technologies lower the adoption and integration costs of further security investment (Hasani et al., 2023).

Table 3. Item analysis of the technological preparedness dimension (TECH). Note: CITC = corrected item-total correlation; α if deleted = Cronbach's alpha with the item removed; communality = principal component extraction. Top 3 / Bottom 3 = proportion of responses of 5 to 7 and 1 to 3, respectively, on the seven-point scale.

Code	Item (abbreviated)	Mean	SD	Top 3	Bottom 3	CITC	α if deleted	Communality
TECH1	IT services designed to operate independently	4.48	1.66	40 %	28 %	0.704	0.865	0.634
TECH2	Systems communicate via common interfaces	4.88	1.88	60 %	16 %	0.685	0.869	0.625
TECH3	Technologies are flexible and interoperable	4.48	1.56	48 %	28 %	0.773	0.858	0.720
TECH4	Data protection improves process stability	5.68	1.57	76 %	8 %	0.690	0.867	0.611
TECH5	Security improves credibility in the market	5.44	1.69	72 %	12 %	0.788	0.855	0.730
TECH6	Cybersecurity is a condition of survival	5.40	1.92	72 %	20 %	0.594	0.882	0.488
TECH7	Compatible with existing technologies	5.20	1.19	64 %	4 %	0.543	0.885	0.410

The process preparedness dimension (three items) reaches an alpha of 0.728 (Table 4). This is the lowest-rated area. Item PROC1 has a mean of 3.84 and 36 per cent agreement. All CITC values exceed 0.3. Deleting PROC1 would raise alpha to 0.780 and increase the variance explained by the first component from 65.33 per cent to 81.96 per cent. The severity of a loss is driven largely by downtime and by indirect costs, which response capability is meant to contain (Tahmasebi, 2024; Vidović and Beriša, 2025). Weak response processes therefore raise the expected loss per incident even where preventive controls are in place.

Table 4. Item analysis of the process preparedness dimension (PROC). Note: column labels as in Table 3.

Code	Item (abbreviated)	Mean	SD	Top 3	Bottom 3	CITC	α if deleted	Communality
PROC1	Processes set up for rapid response to attacks	3.84	1.93	36 %	40 %	0.430	0.780	0.497
PROC2	Clear procedures for secure handling of data	4.52	1.90	52 %	40 %	0.724	0.417	0.826
PROC3	Security controls improve operational efficiency	4.20	1.87	40 %	44 %	0.517	0.679	0.637

The dimension covering perceived benefit for employees (three items) reaches an alpha of 0.673 (Table 5). Items EMP1 and EMP2 both attract 64 per cent agreement. Item EMP3 has a mean of 3.36 and 52 per cent of responses in the lower third of the response scale. EMP3 shows the lowest CITC (0.321) and the lowest communality (0.356) in the dimension. Its removal would raise alpha to 0.779 and increase explained variance from 61.30 to 81.88 per cent. The low score for EMP3 signals underinvestment in human capital. Employee training is among the cheapest controls with a strong marginal effect on breach resilience, so the unused potential here represents a low-cost, high-return investment opportunity (Papathanasiou et al., 2025; Al Aamer and Hamdan, 2023).

Table 5. Item analysis of the perceived benefit for employees' dimension (EMP). Note: column labels are as in Table 3.

Code	Item (abbreviated)	Mean	SD	Top 3	Bottom 3	CITC	α if deleted	Communality
EMP1	Technologies improve reliability of information exchange	4.76	1.94	64 %	24 %	0.571	0.460	0.736
EMP2	Technologies improve employee work efficiency	4.64	1.91	64 %	28 %	0.587	0.440	0.747
EMP3	The firm motivates employees to learn about threats	3.36	1.91	32 %	52 %	0.321	0.779	0.356

The strategic and development orientation dimension (seven items) reaches an alpha of 0.835 (Table 6). The highest means were recorded for FIN1 (6.24; 88 per cent agreement) and FIN2 (5.80; 80 per cent agreement). The lowest means were recorded for FIN6 (4.04) and FIN5 (4.20). Item FIN1 has a CITC of 0.170, below the 0.3 threshold, and its removal would raise alpha to 0.861. The individual measure of sampling adequacy for this item is 0.398, the only value in the dimension below 0.5. The almost unanimous alignment with FIN1 indicates that firms perceive a positive expected net benefit from prevention, which is precisely the same estimate that follows from the reported costs of security breaches

(Fotis, 2024). The much lower scores for investment items suggest that this perceived benefit does not overcome the internal barrier to capital budgeting, a pattern consistent with the analysis of benefits and market failure in the area of cybersecurity for small and medium-sized enterprises (Arroyabe et al., 2024a) and the weak link between security maturity and profitability (Dinkova et al., 2024).

Table 6. Item analysis of the strategic and development orientation dimension (FIN). Note: column labels are as in Table 3.

Code	Item (abbreviated)	Mean	SD	Top 3	Bottom 3	CITC	α if deleted
FIN1	Investment is cheaper than the consequences of an attack	6.24	1.23	88 %	4 %	0.170	0.861
FIN2	Uninterrupted operation protects revenue	5.80	1.16	80 %	4 %	0.414	0.836
FIN3	The firm actively implements modern technologies	4.28	1.99	56 %	40 %	0.710	0.790
FIN4	Plan to further expand security capacities	4.72	1.86	52 %	28 %	0.708	0.791
FIN5	Rapid adoption of new security trends	4.20	1.85	48 %	40 %	0.726	0.788
FIN6	Management accepts risks of innovation	4.04	1.84	48 %	44 %	0.518	0.824
FIN7	Cybersecurity as a competitive advantage	4.24	1.90	48 %	44 %	0.810	0.771

Component analysis of the FIN dimension extracted two components with eigenvalues above 1, jointly explaining 69.00 per cent of the variance (51.45 and 17.55 per cent, respectively). The rotated component matrix (Table 7) shows that items FIN1 and FIN2 load on the second component at 0.838 and 0.776. Items FIN3 to FIN7 load on the first component at values between 0.711 and 0.883. Cross-loadings do not exceed 0.290. These two components have clear economic significance. The second component captures the perceived economics of prevention, that is, the calculation of expected losses, while the first captures investment behaviour. Valuing protection and deciding on expenditure on it are economically distinct actions, and the data distinguish between them accordingly (Lee, 2021; Fielder et al., 2016).

Table 7. Rotated component matrix of the FIN dimension (Varimax with Kaiser normalisation). Note: extraction by principal component analysis; rotation converged in 3 iterations.

Code	Item (abbreviated)	Component 1	Component 2
FIN1	Investment is cheaper than the consequences of an attack	–0.039	0.838
FIN2	Uninterrupted operation protects revenue	0.286	0.776
FIN3	The firm actively implements modern technologies	0.798	0.238
FIN4	Plans to further expand security capacities	0.778	0.205
FIN5	Rapid adoption of new security trends	0.883	0.036
FIN6	Management accepts risks of innovation	0.711	–0.090
FIN7	Cybersecurity as a competitive advantage	0.865	0.245

The identified revisions were not applied retrospectively to the pilot data. Table 8 reports the reliability of the proposed subscales calculated from the pilot data, for information on the expected behaviour of the revised instrument. The subscales excluding PROC1 and EMP3 reach alphas of 0.780 and 0.779, respectively. Subscale FIN-B reaches an alpha of 0.877, while subscale FIN-A reaches 0.525 with two items. From a financial perspective, the FIN-A subscale measures precisely the construct that a finance-oriented instrument must capture effectively, namely the implicit assessment of a firm's costs and returns in relation to prevention. The extension of this subscale is therefore not only a validated refinement, but also a prerequisite for modelling investment behaviour in the second wave.

Table 8. Reliability of the proposed subscales of the revised instrument (n = 25). Note: mean r = mean inter-item correlation; PC1 = first principal component. These values serve as a basis for revising the instrument.

Proposed subscale	Items	Cronbach's α	Mean r	PC1 variance
Process preparedness (without PROC1)	PROC2, PROC3	0.780	0.639	81.96 %
Perceived benefit for employees (without EMP3)	EMP1, EMP2	0.779	0.638	81.88 %
FIN-A: economic awareness	FIN1, FIN2	0.525	0.357	67.83 %
FIN-B: strategic-innovation orientation	FIN3 – FIN7	0.877	0.588	67.48 %

DOI: 10.55643/fcaptp.4.69.2026.5291

The reliability and dimensionality findings are complemented by a descriptive overview of the controls and practices in place (Table 9). Proportions are reported against the full sample (n = 25). Responses of "do not know" are included in the denominator but not counted as confirmed controls. Items are ordered by the level of implementation within each area.

Table 9. Controls, processes and practices in place in the pilot sample (n = 25). Note: proportions are calculated against the full sample (n = 25). Indicators with "do not know" responses: testing the recoverability of backups (4), regular improvement based on risks (5), training cybersecurity spending (6), firewall (5). For training for IT specialists, the response category is "not applicable" (5). Incidents refer to more than one occurrence in the preceding 12 months.

Area	Indicator	Count	Share
Technical controls	Operating system and application updates	24	96 %
	Antivirus software	22	88 %
	Strong password policy	20	80 %
	Multi-factor authentication	18	72 %
	Offsite backup	17	68 %
	VPN for external access	16	64 %
	Firewall on the corporate network	15	60 %
	Encryption of stored data	13	52 %
	Regular risk assessments	11	44 %
	IT security assessment methods (testing, review)	10	40 %
Processes and response	Revocation of access after an employee leaves	21	84 %
	Regular full backups of business data	19	76 %
	Knowledge of the incident response procedure	18	72 %
	Regular improvement based on identified risks	12	48 %
	Testing the recoverability of backups	11	44 %
People and training	Designated person responsible for information security	18	72 %
	ICT training for other employees	8	32 %
	Training for IT specialists	7	28 %
Finance and risk transfer	Cybersecurity spending above 1 % of the IT budget	7	28 %
	Cyber insurance	6	24 %
Incidents (12 months)	Malicious software	14	56 %
	Breach of confidential data through unintentional employee action	5	20 %
	Unavailability of IT services due to an external attack	4	16 %

Within the pilot sample of 25 SMEs, basic technical controls were among the most commonly reported cybersecurity measures. System updates were confirmed by 24 firms, antivirus software by 22 firms, and a strong password policy by 20 firms. By contrast, practices focused on the systematic verification of cybersecurity practices were less frequently implemented. Regular risk assessments were reported by 11 firms, while 10 firms used IT security assessment methods such as testing or review. A similar pattern was observed for backup practices. Nineteen firms reported performing regular full backups of business data, and 17 maintained offsite backup copies. However, only 11 firms reported testing backup recoverability. Ten firms indicated that such testing was not performed, while four respondents were unable to confirm whether recoverability testing took place. The findings also indicate differences between the formal assignment of cybersecurity responsibility and the provision of employee training. Eighteen firms reported having a designated person responsible for information security, whereas ICT training for other employees was provided by eight firms and training specifically aimed at IT specialists by seven firms. Cyber insurance was reported by six firms. Regarding cybersecurity incidents experienced during the preceding 12 months, malicious software was the most frequently reported incident type, identified by 14 firms. Only seven out of 25 companies spend more than 1 per cent of their IT budget on cybersecurity, while organisations covered by the EU's NIS Framework allocate approximately 9 per cent of their IT budgets to this area (ENISA, 2025). Even taking into account differences in scale, this points to a significant underinvestment. As only six companies have cyber insurance, the residual risk for the remaining nineteen companies remains entirely on their own balance sheets. The distribution of selected indicators by firm size is reported in Table 10.

Table 10. Selected indicators by firm size (number of firms answering yes). Note: for indicators with a "do not know" option, such responses are not counted as positive. Subgroup counts are small, so these data describe the sample and are not generalised.

Indicator	Micro (1–9)	Small (10–49)	Medium (50–249)
Multi-factor authentication	6 of 7	9 of 14	3 of 4
Regular full backups	3 of 7	12 of 14	4 of 4
Testing the recoverability of backups	0 of 7	9 of 14	2 of 4
Encryption of stored data	1 of 7	8 of 14	4 of 4
Regular risk assessments	2 of 7	5 of 14	4 of 4
IT security assessment	2 of 7	4 of 14	4 of 4
Designated person responsible	3 of 7	11 of 14	4 of 4
Training for IT specialists	0 of 7	4 of 14	3 of 4
ICT training for other employees	1 of 7	5 of 14	2 of 4
Cyber insurance	1 of 7	3 of 14	2 of 4

Across most indicators, the level of implementation increases with firm size. All four medium-sized firms reported regular backups, risk assessments, IT security assessments, and a designated responsible person. None of the seven micro firms reported testing the recoverability of backups or training for IT specialists. Multi-factor authentication runs in the opposite direction, reported by six of the seven micro firms and by nine of the fourteen small firms. The gradient has an economic explanation. Many controls carry fixed costs and indivisibilities, so the unit cost of preparedness falls with firm size, which mirrors the resource-based security divide between smaller and larger firms (Heidt et al., 2019). The exception for multi-factor authentication may be explained by the ambition of micro firms to obtain this control as part of purchased cloud services, substituting a provider's operating expenditure for their own capital expenditure.

DISCUSSION

The technological preparedness dimension is unidimensional and has very good reliability, and the process preparedness dimension is acceptable. Two findings nonetheless call for revision of the instrument. First, the item on employee motivation (EMP3) differs from the items on perceived technological benefit both in content and in statistical behaviour. The difference lies between an attitude towards technology and actual organisational practice. This distinction is well grounded in the literature. Within the TOE framework, perceived usefulness and ease of use belong to the technological context, whereas training and management support belong to the organisational context (Hasani et al., 2023; DePietro et al., 1990). Zimmermann and Renaud (2019) further argue that building employee competencies is a distinct area of management, not a by-product of technology adoption. The empirical separation of the two constructs in the present data is therefore theoretically expected.

Second, the strategic-financial dimension splits into economic awareness and strategic-innovation orientation. The split corresponds to the difference between believing in the value of prevention and being willing to act. Dinkova et al. (2024) show that the relationship between security controls, maturity, and firm outcomes is not linear, and that a declared belief in the value of prevention need not translate into investment or into a lower incidence of incidents. Franke and Wernberg (2020) similarly document a preference for readily available technical controls over systematic change. The revisions proposed here have the status of recommendation.

The substantive findings reveal two related gaps. The first is a gap between declared belief and practice. Firms agree almost unanimously on the financial rationality of prevention (22 of 25 for FIN1), yet items describing actual implementation and innovation orientation reach means of only 4.04 to 4.72. Chidukwani et al. (2024) describe a comparable gap in Western Australia, where firms reported clear security responsibilities without corresponding formalised procedures. Benz and Chatterjee (2020) refer in this context to self-overestimation among SME management, which regards its own position as above average despite the absence of a strategy.

The second and, in the present data, more pronounced gap lies between implementing a control and verifying it. Firms in the sample cover the basic technical layer well. Updates were reported by 24 of the 25 firms, antivirus software by 22, and strong passwords by 20. Controls that verify whether protection actually works lag behind by half. Risk assessments were reported by 11 firms and IT security assessments by 10. The pattern is most pronounced for backups. Backups are performed by 19 firms, but only 11 test their recoverability. An untested backup does not provide a verified recovery

DOI: 10.55643/fcaptp.4.69.2026.5291

capability. It only creates the assumption that recovery is possible. Chidukwani et al. (2024) identify a similar weakness in the recover function of the NIST CSF. The present results show the same problem in the Slovak context. Franke and Wernberg (2020) also note a preference for readily available technical controls over systematic organisational change. Similarly, Valli et al. (2014) show that the adoption of technical tools does not necessarily lead to greater security awareness. This distinction has a practical implication for the questionnaire. Questions asking whether a control is in place should be separated from questions asking whether that control is regularly tested or verified.

The difference may reflect the nature of the two types of control, although the pilot data cannot verify this explanation. Backups, antivirus software, and updates can be purchased as a service and run automatically once configured. Testing backup recovery is different. It requires dedicated time, a recovery scenario, and responsibility assigned to a specific person. These requirements may be more difficult for SMEs with limited resources (Heidt et al., 2019). The results by firm size are consistent with this interpretation. None of the seven micro firms reported testing backup recovery, although three reported performing backups. Among the nineteen firms that perform backups, eleven test recovery. The remaining eight either do not test it or do not know whether testing takes place. If confirmed in a larger sample, this pattern could suggest that controls requiring active human involvement are more difficult for SMEs to maintain than controls that can be automated or outsourced.

One exception to the size gradient deserves attention. Six of the seven micro firms reported using multi-factor authentication, compared with nine of the fourteen small firms. Micro firms performed worse on all other indicators. A possible explanation is that micro firms rely on ready-made cloud services in which the provider enables multi-factor authentication by default or enforces it. The control would then not be the outcome of a security decision by the firm, but a property of the purchased service. This hypothesis cannot be verified on the pilot sample. The instrument for the second wave should therefore include a question on whether the firm implemented a control itself or inherited it from a provider default.

A third finding concerns the imbalance between the organisational anchoring of security and the development of people. A designated person responsible for information security is in place in 18 of the 25 firms, and the same number report knowledge of the incident response procedure. Training for other employees is nonetheless provided by only eight firms and training for IT specialists by seven. Responsibility is therefore assigned, but competencies are not built systematically. The pattern is sharper at the firm level. Of the eighteen firms with a designated responsible person, only seven provide training for IT specialists. Eleven firms have therefore entrusted information security to a specific person without providing for that person's professional development. At the same time, all seven firms that train IT specialists also have a designated responsible person, so organisational anchoring appears to be a precondition for training rather than a substitute for it. The level of training in the sample corresponds to national data indicating that 60.5 per cent of Slovak SMEs provide no training at all (NBU, 2023b). The literature attaches particular importance to this area, since an unprepared employee remains the most common entry point for an attack (Wells et al., 2014; Kabanda et al., 2018). Bada and Nurse (2019) emphasise that the mere existence of training is insufficient. What matters is whether it leads to a verifiable ability to recognise and respond to a threat. Zimmermann and Renaud (2019) add that employees should be understood as part of the solution rather than as a risk to be controlled technically.

The data also reveal an apparent inconsistency in the responses. Eighteen of the 25 respondents agreed that cybersecurity is essential for the firm’s survival. However, only nine reported having processes in place for a rapid response to an attack. This was the lowest count among all attitudinal items. Five firms agreed with the first statement but disagreed with the second. The difference may reflect a gap between awareness and capability rather than contradictory responses. Firms may recognise cyber threats as a serious risk but still lack the capacity to establish formal response procedures. This interpretation is consistent with Chidukwani et al. (2024), who identify limited financial resources and uncertainty about where to start as common barriers for SMEs. Awareness alone should therefore not be treated as evidence of preparedness. The questionnaire should measure awareness and operational capability separately.

The low uptake of cyber insurance (six of the 25 firms) is consistent with European findings on limited insurance penetration in the SME segment (ENISA, 2022). Respondents reported price and limited awareness of the product as the main barriers. These correspond to the two obstacles most frequently identified in the literature, namely budget constraints and uncertainty about where to start (Chidukwani et al., 2024; Kabanda et al., 2018; Osborn and Simpson, 2018). Cyber insurance is also relevant from a financial perspective. The underwriting process may require SMEs to assess and document their security controls (Lloyd, 2020). The low level of awareness observed in the pilot also points to a role for insurers and business support organisations. Chambers of commerce and national cybersecurity authorities may also contribute to improving awareness of available insurance options. The pilot data cannot determine whether cyber insurance improves security maturity or whether more mature firms are simply more likely to purchase it. This relationship should be examined in the second wave.

Placing the pilot results next to evidence from other European Union countries sharpens what is specific to the Slovak sample and what is not. The gap between performing backups and testing their recoverability, which is the most pronounced result reported here, matches the Western Australian evidence of Chidukwani et al. (2024) and the preference for readily available technical controls over systematic organisational change documented by Franke and Wernberg (2020). In a European survey on the Cyber Resilience Act, 66 per cent of SME respondents had heard of the regulation while few understood its requirements, and financial support was among the most frequently requested forms of assistance (ENISA, 2026c), which mirrors the belief-investment gap observed in our data. Two other findings look more country-specific. Cyber insurance is held by six of the 25 firms here, against 5 per cent of SMEs surveyed across the EU (ENISA, 2022). Cybersecurity spending above 1 per cent of the IT budget was reported by only seven firms, whereas organisations covered by the EU NIS framework devote about 9 per cent of their IT budgets to it (ENISA, 2025). Yarovenko et al. (2025), modelling the digital readiness of European countries between 2012 and 2024, find statistically significant positive country effects for Sweden, the Netherlands, Finland, Germany and Denmark and significant negative effects for a group of central and eastern European countries, and conclude that digital indicators become effective only when supported by institutional capacity. Slovakia had to be excluded from their panel altogether for lack of data, which is itself an argument for the enterprise-level measurement proposed in our work.

The economic interpretation of the pilot can be condensed into a set of proposals for SMEs on implementing cyber defence. First, firms should verify existing controls before investing in additional ones. A small share of the security budget can be used to test backups and other controls. This helps firms determine whether existing spending provides effective protection. Second, firms should prioritise the human factor. Training is relatively inexpensive, while measures such as multi-factor authentication can provide substantial security benefits (Mayeke, 2025). Third, SMEs should make deliberate use of security features provided by cloud services. These controls can reduce the need for separate investment. Resources can then be directed towards risks specific to the firm. Fourth, cyber insurance can provide an additional external assessment of security practices. The underwriting process may reveal weaknesses in existing controls and provide an external view of the firm's risk profile (Lloyd, 2020). Fifth, security budgets should be based on a benchmark rather than determined ad hoc. The 9 per cent share of IT budgets reported for EU NIS-regulated organisations provides one possible reference point (ENISA, 2025). For the smallest firms, spending above 1 per cent of the IT budget may serve as a realistic starting point. Sixth, investments should be prioritised according to their expected reduction in losses relative to their cost. This approach is consistent with the marginal principle of security investment (Lee, 2021; Fielder et al., 2016). Ostapets et al. (2026) similarly emphasise the importance of risk assessment in IT investment decisions. Their analysis shows that project-specific risks should be considered before resources are committed. Such assessment can support more prudent investment decisions and reduce the risk of budget overruns.

A methodological implication for the second wave also follows from the results. Dinkova et al. (2024) note that the number of reported incidents depends on the ability of a firm to detect incidents at all, so less mature firms systematically underreport them. Amir et al. (2018) document comparable underreporting among listed firms. Self-reported data on incidents therefore cannot be interpreted as a direct measure of exposure, and the forthcoming collection should complement them with questions on detection capability. These findings also support the decision to measure preparedness through attitudinal and process items rather than through incident counts.

The study has limitations, which are acknowledged openly. The sample of 25 firms is small and self-selected, with an overrepresentation of eastern Slovakia and of manufacturing firms. The response rate of 8.7 per cent is low, although this is not unusual for a sensitive topic such as cybersecurity. Chidukwani et al. (2024) abandoned probability sampling for the same reasons. The data are self-reported and may be subject to social desirability bias. Cronbach's alpha increases with the number of items, so comparisons between dimensions with different item counts are interpreted with caution. Differences between subgroups by firm size are reported as absolute counts and are not tested statistically. The subgroups comprise seven, fourteen and four firms. At this size, significance tests and effect sizes alike would yield confidence intervals too wide for any interpretation. These differences are therefore treated as a description of the sample and as hypotheses for the second wave, not as established relationships. Component analysis at this sample size is treated as indicative, and confirmatory verification of the structure is a task for the large-scale collection. The methodological risks nevertheless remain, and we clearly state them. Two individual values illustrate the limits of the data. KMO reaches only 0.554 and 0.586 for the two three-item dimensions, which is above the threshold, and the individual measure of sampling adequacy for FIN1 is 0.398. Solutions obtained at this sample size can also capitalise on chance, which is why the revisions identified here were not applied retrospectively to the same data. The component structure is therefore treated as a hypothesis to be tested on the larger sample. The interpretation does not rely on the component analysis alone. It is also supported by reliability coefficients, item statistics and the descriptive distribution of responses. The results are therefore not generalised to the population of Slovak SMEs. As participation was voluntary and limited to professionally engaged

DOI: 10.55643/fcaptp.4.69.2026.5291

respondents, the results should not be considered representative of the Slovak SME population. The purpose of the pilot was to refine the measurement instrument, not to estimate population parameters.

CONCLUSIONS

This study presented and piloted a survey instrument for measuring the cybersecurity preparedness of Slovak SMEs. All four dimensions reach acceptable internal consistency, and three exceed the 0.7 threshold; the technological dimension is clearly unidimensional. In line with the principles of instrument development, the identified revisions were not applied retrospectively to the pilot data. They are instead incorporated into the specification of a revised instrument for the second wave of data collection. Five revisions are proposed. Item PROC1 should be retained but monitored. Item EMP3 should be moved to a separate set of items on training practices. The strategic-financial dimension should be split into subscales of economic awareness and strategic-innovation orientation. The economic awareness subscale should be expanded with additional items, since two items are insufficient for reliable measurement. Questions on the implementation of controls should be separated from questions on their verification. This last revision follows from the most consistent substantive finding of the pilot. Basic technical controls are widespread, whereas controls that verify whether protection actually works lag behind by half. Backups are performed by 19 of the 25 firms, but only 11 test whether data can be restored.

The study also responds to the second gap identified in the literature. Reliability coefficients, item statistics, sampling adequacy measures and the component structure are reported in full for every dimension, so the measurement profile of the instrument is documented rather than assumed. This is what allows the results of the second wave to be compared over time and against studies conducted in other countries.

The results also support an economic interpretation. Most firms in the sample believe that prevention is less costly than the consequences of a cyberattack. This view was shared by 22 of the 25 respondents. However, their reported spending does not fully reflect this belief. Only seven firms allocate more than 1 per cent of their IT budget to cybersecurity, and only six have cyber insurance. In addition, eight of the nineteen firms that perform backups do not know whether the data can be restored. This suggests a gap between perceived importance and actual preparedness. Such a gap is consistent with previous evidence on underinvestment in SME cybersecurity (Arroyabe et al., 2024a). The practical implications concern both firms and policy. For firms, the pilot highlights several low-cost measures, including testing existing controls, training employees, using security features provided by external services, and using insurance underwriting as an external assessment. For policymakers, the gap between awareness and investment supports the role of external incentives and regulatory requirements. These include the NIS2 framework and mechanisms created through the cyber insurance market. The instrument developed in this study may help identify where such support is most needed.

The revised questionnaire is ready for the second phase of the research, namely data collection on a large representative sample of firms. A larger sample will allow confirmatory factor analysis, tests of invariance by firm size and industry, and modelling of the relationships between preparedness, investment and the incidence of incidents, provided that detection capability is measured alongside the incidents themselves. Future research may extend the questionnaire with questions on external service providers, detection capability, incident impacts and sources of information on legislation. The practical contribution of the instrument is that it offers firms a parsimonious mirror of their preparedness across four areas simultaneously: technology, processes, people and finance. For policymakers, it provides a measurable basis for monitoring the resilience of the SME sector in the context of the requirements of the NIS2 Directive. The threat landscape itself will keep shifting, not least with the diffusion of artificial intelligence on both the attack and the defence side (ENISA, 2026b), which strengthens the case for repeated measurement.

ADDITIONAL INFORMATION

AUTHOR CONTRIBUTIONS

Conceptualization: *Jakub Sopko*

Data curation: *Jakub Sopko*

Formal Analysis: *Jakub Sopko, Leoš Šafár*

Software: *Jakub Sopko*

Supervision: *Jakub Sopko*

Validation: *Jakub Sopko*

Visualization: *Jakub Sopko*

Funding acquisition: *Jakub Sopko, Leoš Šafár*

Writing – review & editing: *Leoš Šafár*

Writing – original draft: Jakub Sopko

ACKNOWLEDGMENT

We would like to thank Martina Vlasáková for coordinating the data collection and preparing the dataset, and Marek Pekarčík for his valuable comments and feedback during the development and formulation of the questionnaire items.

FUNDING

This work was supported by the Scientific Grant Agency of the Ministry of Education, Research, Development and Youth of the Slovak Republic and the Slovak Academy of Sciences [VEGA 1/0638/25] and Slovak Research and Development Agency under the Contract no. VV-MVP-24-0272.

CONFLICT OF INTEREST

The Authors declare that there is no conflict of interest.

REFERENCES

1. Accenture. (2019). *At a glance: Ninth annual cost of cybercrime study*. https://www.accenture.com/content/dam/accenture/final/a-com-migration/pdf/pdf-99/accenture-cost-cyber-crime-infographic.pdf
2. Al Aamer, A. K., & Hamdan, A. (2023). Cyber security awareness and SMEs' profitability and continuity: Literature review. *Emerging Trends and Innovation in Business and Finance*, 593–604. Springer. https://doi.org/10.1007/978-981-99-6101-6_43
3. Alahmari, A., & Duncan, B. (2020). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. In *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)* (pp. 1–5). IEEE. https://doi.org/10.1109/CyberSA49311.2020.9139638
4. Allianz Commercial. (2025). *Allianz Risk Barometer: Identifying the major business risks for 2025*. Allianz Global Corporate & Specialty. https://commercial.allianz.com/
5. Allianz Commercial. (2026). *Allianz Risk Barometer: Identifying the major business risks for 2026*. https://commercial.allianz.com/contenat/dam/onemarketing/commercial/commercial/reports/allianz-risk-barometer-2026.pdf
6. Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies, 23*(3), 1177–1206. https://doi.org/10.1007/s11142-018-9452-4
7. Anderson, R., & Moore, T. (2009). Information security: Where computer science, economics and psychology meet. *Philosophical Transactions of the Royal Society A, 367*(1898), 2717–2727. https://doi.org/10.1098/rsta.2009.0027
8. Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J., Levi, M., Moore, T., & Savage, S. (2013). Measuring the cost of cybercrime. In R. Böhme (Ed.), *The economics of information security and privacy* (pp. 265–300). Springer. https://doi.org/10.1007/978-3-642-39498-0_12
9. Arroyabe, M. F., Arranz, C. F., De Arroyabe, I. F., & de Arroyabe, J. C. F. (2024a). Exploring the economic role of cybersecurity in SMEs: A case study of the UK. *Technology in Society, 78*, 102670. https://doi.org/10.1016/j.techsoc.2024.102670
10. Arroyabe, M. F., Arranz, C. F. A., Fernandez de Arroyabe, I., & Fernandez de Arroyabe, J. C. (2024b). Revealing the realities of cybercrime in small and medium enterprises: Understanding fear and taxonomic perspectives. *Computers & Security, 141*, 103826. https://doi.org/10.1016/j.cose.2024.103826
11. Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information and Computer Security, 27*(3), 393–410. https://doi.org/10.1108/ICS-07-2018-0080
12. Benz, M., & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons, 63*(4), 531–540. https://doi.org/10.1016/j.bushor.2020.03.010
13. Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security, 11*(3), 431–448.
14. Celeny, D., Maréchal, L., Rousselot, E., Mermoud, A., & Humbert, M. (2024). Prioritizing investments in cybersecurity: Empirical evidence from an event study on the determinants of cyberattack costs. *arXiv preprint arXiv:2402.04773*. https://doi.org/10.48550/arXiv.2402.04773
15. Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A survey on the cyber security of small-to-medium businesses: Challenges, research focus and recommendations. *IEEE Access, 10*, 85701–85719. https://doi.org/10.1109/ACCESS.2022.3197899

16. Chidukwani, A., Zander, S., & Koutsakis, P. (2024). Cybersecurity preparedness of small-to-medium businesses: A Western Australia study with broader implications. *Computers & Security, 145*, 104026. https://doi.org/10.1016/j.cose.2024.104026

17. Cybersecurity and Infrastructure Security Agency. (2020). *Cyber resilience review (CRR): Question set with guidance*. U.S. Department of Homeland Security. https://www.cisa.gov/

18. Darem, A. A., Alhashmi, A. A., Alkhaldi, T. M., Alashjaee, A. M., Alanazi, S. M., & Ebad, S. A. (2023). Cyber threats classifications and countermeasures in banking and financial sector. *IEEE Access, 11*, 125138–125158. https://doi.org/10.1109/ACCESS.2023.3327016

19. de Vaus, D. (2002). *Analyzing social science data: 50 key problems in data analysis*. SAGE Publications.

20. DePietro, R., Wiarda, E., & Fleischer, M. (1990). The context of change: Organization, technology and environment. In L. G. Tornatzky & M. Fleischer (Eds.), *The processes of technological innovation* (pp. 151–175). Lexington Books.

21. 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

22. European Union Agency for Cybersecurity. (2022). *NIS investments report 2022*. ENISA. https://www.enisa.europa.eu/

23. European Union Agency for Cybersecurity. (2024). *The EU cybersecurity index 2024: EU-level insights and next steps*. ENISA. https://www.enisa.europa.eu/sites/default/files/2025-06/The%20EU%20Cubersecurity%20Index%202024_en_0.pdf

24. European Union Agency for Cybersecurity. (2025). *NIS investments 2025: Main report*. ENISA. https://www.enisa.europa.eu/sites/default/files/2026-02/NIS%20Investments%202025%20-%20Main%20report.pdf

25. European Union Agency for Cybersecurity. (2026a). *ENISA NIS360: Latest insights in the cybersecurity maturity and criticality of NIS sectors of high criticality*. ENISA. https://www.enisa.europa.eu/sites/default/files/2026-05/ENISA%20NIS360%202026.pdf

26. European Union Agency for Cybersecurity. (2026b). *ENISA's view on cybersecurity in the frontier AI era*. ENISA. https://www.enisa.europa.eu/sites/default/files/2026-07/ENISA%20view%20on%20cybersecurity%20in%20the%20frontier%20AI%20era_en_0.pdf

27. European Union Agency for Cybersecurity. (2026c). *SME CRA survey report: Survey results and analysis*. ENISA. https://www.enisa.europa.eu/sites/default/files/2026-06/SME%20CRA%20survey%20report.pdf

28. 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

29. Fotis, F. (2024). Economic impact of cyber attacks and effective cyber risk management strategies: A light literature review and case study analysis. *Procedia Computer Science, 251*, 471–478. https://doi.org/10.1016/j.procs.2024.11.135

30. Franco, M. F., Künzler, F., von der Assen, J., Feng, C., & Stiller, B. (2024). RCVaR: An economic approach to estimate cyberattacks costs using data from industry reports. *Computers & Security, 139*, 103737. https://doi.org/10.1016/j.cose.2024.103737

31. Franke, U., & Wernberg, J. (2020). A survey of cyber security in the Swedish manufacturing industry. In *Proceedings of the International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)* (pp. 1–8). IEEE.

32. Hasani, T., O'Reilly, N., Dehghantanha, A., Rezania, D., & Levallet, N. (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance. *SN Business & Economics, 3*(5), 97. https://doi.org/10.1007/s43546-023-00477-6

33. 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

34. Hertzog, M. A. (2008). Considerations in determining sample size for pilot studies. *Research in Nursing & Health, 31*(2), 180–191. https://doi.org/10.1002/nur.20247

35. International Telecommunication Union. (2024). *Global cybersecurity index 2024* (5th ed.). ITU.

36. Johanson, G. A., & Brooks, G. P. (2010). Initial scale development: Sample size for pilot studies. *Educational and Psychological Measurement, 70*(3), 394–400. https://doi.org/10.1177/0013164409355692

37. Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce, 28*(3), 269–282. https://doi.org/10.1080/10919392.2018.1484598

38. Kaiser, H. F. (1974). An index of factorial simplicity. *Psychometrika, 39*(1), 31–36. https://doi.org/10.1007/BF02291575

39. Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics, 139*(3), 719–749. https://doi.org/10.1016/j.jfineco.2019.05.019

40. Lakhtionova, A. (2025). Global cybersecurity market 2017–2029: Dynamics, structure, challenges and key players. *Society. Economy. Digitalization, 1*(4), 61–75. https://doi.org/10.31379/sed.1.4.2025.38

41. Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons, 64*(5), 659–671. https://doi.org/10.1016/j.bushor.2021.02.022

42. Liu, C., & Babar, M. A. (2026). Corporate cybersecurity risk and data breaches: A systematic review of empirical research. *Australian Journal of Management, 51*(1), 62–92. https://doi.org/10.1177/03128962241293658

43. Lloyd, G. (2020). The business benefits of cyber security for SMEs. *Computer Fraud & Security, 2020*(2), 14–17. https://doi.org/10.1016/S1361-3723(20)30019-1

44. Mayeke, N. R. (2025). Evaluating the cost-benefit dynamics of cybersecurity compliance investments: A multi-sectoral analysis across financial, educational, and ecommerce industries. *Computer Science & IT Research Journal, 6*(4), 266–287. https://doi.org/10.51594/csitrj.v6i4.1914

45. Ministry of Investments, Regional Development and Informatization of the Slovak Republic. (2025). *Methodological guideline No. 18 on the verification of enterprise size (SME)*. MIRRI SR. (In Slovak)

46. NSA—National Security Authority of the Slovak Republic. (2023a). *Report on cybersecurity in the Slovak Republic in 2023*. NBÚ SR. https://www.nbu.gov.sk/sprava-o-kybernetickej-bezpecnosti-v-slovenskej-republike-v-roku-2023/

47. NSA—National Security Authority of the Slovak Republic. (2023b). *Cybersecurity 2023: Results of a telephone survey of small and medium-sized enterprises*. NBÚ SR. https://cybercompetence.sk/wp-content/uploads/dokumenty/na_stiahnutie/letak_KB-prieskum_verejnej_mienky_msp_2023.pdf

48. Osborn, E., & Simpson, A. (2018). Risk and the small-scale cyber security decision making dialogue: A UK case study. *The Computer Journal, 61*(4), 472–495. https://doi.org/10.1093/comjnl/bxx093

49. Pacelli, V. (2025). *Systemic risk and complex networks in modern financial systems*. Springer Nature. https://doi.org/10.1007/978-3-031-64916-5

50. Papathanasiou, A., Liontos, G., Katsouras, A., Liagkou, V., & Glavas, E. (2024). Cybersecurity guide for SMEs: Protecting small and medium-sized enterprises in the digital era. *Journal of Information Security, 16*(1), 1–43. https://doi.org/10.4236/jis.2025.161001

51. Paulsen, C. (2016). Cybersecuring small businesses. *Computer, 49*(8), 92–97. https://doi.org/10.1109/MC.2016.223

52. Porkoláb-Angyalos, Z., & Szilágyi, R. (2026). Cyber maturity among European SMEs: A time-series and cluster-based analysis. *Applied Studies in Agribusiness and Commerce, 20*(1). https://doi.org/10.19041/APSTRACT/2026/1/6

53. Renaud, K., & Ophoff, J. (2021). A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs. *Organizational Cybersecurity Journal, 1*(1), 24–46. https://doi.org/10.1108/OCJ-03-2021-0004

54. Renaud, K., & Weir, G. R. S. (2016). Cybersecurity and the unbearability of uncertainty. In *Proceedings of the Cybersecurity and Cyberforensics Conference (CCC)* (pp. 137–143). IEEE. https://doi.org/10.1109/CCC.2016.29

55. Riek, M., & Böhme, R. (2018). The costs of consumer-facing cybercrime: An empirical exploration of measurement issues and estimates. *Journal of Cybersecurity, 4*(1), tyy004. https://doi.org/10.1093/cybsec/tyy004

56. Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity, 2*(2), 121–135. https://doi.org/10.1093/cybsec/tyw001

57. Sawik, T. (2022). Balancing cybersecurity in a supply chain under direct and indirect cyber risks. *International Journal of Production Research, 60*(2), 766–782. https://doi.org/10.1080/00207543.2021.1914356

58. SBA—Slovak Business Agency. (2026). *Vznik a zánik malých a stredných podnikov na Slovensku v roku 2025*. Analýza. https://www.npc.sk/media/Vznik%20a%20z%C3%A1nik%20mal%C3%BDch%20a%20stredn%C3%BDch%20podnikov%20na%20Slovensku%20v%20roku%202025_FINAL.pdf

59. Semenova, S., Shpyrko, O., Androsenko, O., Afanasieva, I., Kolumbet, O., & Vorchakova, I. (2024). The essence of Goodwill in disclosing the intangible value of business in the context of digital transformation. *Financial and Credit Activity: Problems of Theory and Practice, 4*(57), 98–113. https://doi.org/10.55643/fcaptp.4.57.2024.4449

60. Tahmasebi, M. (2024). Cyberattack ramifications, the hidden cost of a security breach. *Journal of Information Security, 15*(2), 87–105. https://doi.org/10.4236/jis.2024.152007

61. Tam, T., Rao, A., & Hall, J. (2021). The good, the bad and the missing: A narrative review of cyber-security implications for Australian small businesses. *Computers & Security, 109*, 102385. https://doi.org/10.1016/j.cose.2021.102385

62. Valli, C., Martinus, I., & Johnstone, M. (2014). Small to medium enterprise cyber security awareness: An initial survey of Western Australian business. In *Proceedings of the International Conference on Security and Management (SAM)* (pp. 1–5). CSREA Press.

63. Vidović, N., & Beriša, H. (2025). Economic aspects of cyber security: Socio-financial consequences of cyber attacks. *International Journal of Contemporary Security Studies, 1*(2), 105–118. https://doi.org/10.18485/fb_ijcss.2025.1.1.11

64. Warrens, M. J. (2015). On Cronbach's alpha as the mean of all split-half reliabilities. In R. E. Millsap, D. M. Bolt, L. A. van der Ark, & W.-C. Wang (Eds.), *Quantitative psychology research* (pp. 293–300). Springer. https://doi.org/10.1007/978-3-319-07503-7_18

65. Wells, L. J., Camelio, J. A., Williams, C. B., & White, J. (2014). Cyber-physical security challenges in manufacturing systems. *Manufacturing Letters, 2*(2), 74–77. https://doi.org/10.1016/j.mfglet.2014.01.005

66. Wirth, A. (2017). The economics of cybersecurity. *Biomedical Instrumentation & Technology, 51*(s6), 52–59. https://doi.org/10.2345/0899-8205-51.s6.52

67. World Economic Forum. (2022). *Global cybersecurity outlook 2022*. https://www.weforum.org/publications/global-cybersecurity-outlook-2022/

68. World Economic Forum. (2026). *The global risks report 2026*. https://reports.weforum.org/docs/WEF_Global_Risks_Report_2026.pdf

69. Yarovenko, H., Bilovodska, V., Bylbas, R., Pankiv, O., Baghirzade, M., Niemi, O., & Djakons, D. (2025). Digital readiness of European countries to combat corruption and cyber threats: Panel analysis. *Business Ethics and Leadership,*

DOI: 10.55643/fcaptp.4.69.2026.5291

9(2), 238–265. https://doi.org/10.61093/bel.9(2).238-265.2025

70. Zimmermann, V., & Renaud, K. (2019). Moving from a "human-as-problem" to a "human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies, 131*, 169–187. https://doi.org/10.1016/j.ijhcs.2019.05.005

Сопко Я., Шафар Л.

ПЕРЕКОНАНІ, АЛЕ НЕ ГОТОВІ: ПІЛОТНЕ ВИМІРЮВАННЯ ГОТОВНОСТІ ДО КІБЕРБЕЗПЕКИ СЛОВАЦЬКИХ МАЛИХ І СЕРЕДНІХ ПІДПРИЄМСТВ

Малі та середні підприємства (МСП) дедалі частіше стають мішенню кібератак. Однак їхню готовність у Словаччині рідко вимірюють. Це дослідження розробляє та пілотує інструмент для оцінки готовності до кібербезпеки малих і середніх підприємств. Анкета складається з шести частин. Чотири з них містять шкалу ставлення й формують вимірювані виміри готовності: технологічну готовність і сумісність, готовність процесів і управління реагуванням, сприйняту користь кібербезпеки для працівників, а також стратегічну та розвиткову орієнтацію. Пілотне обстеження провели 25 словацьких малих і середніх підприємств. Ми перевіряли дані за допомогою альфа-моделі Кронбаха, коригували кореляції між елементами й загальним аналізом та аналізом головних компонентів за допомогою обертання Varimax, разом із мірою Кайзера-Мейєра-Олкіна та тестом сферичності Бартлетта. Усі чотири виміри мають прийнятну внутрішню послідовність (альфа 0,673 до 0,886), і три перевищують поріг 0,7. Технологічний вимір є одновимірним і пояснює 60,27 % дисперсії відгуків. Один проблемний пункт був виявлений у вимірі працівника; його видалення підвищує альфу з 0,673 до 0,779. Обертована матриця компонентів свідчить, що стратегічно-фінансовий вимір поділяється на дві підшкали: економічну обізнаність і орієнтацію на стратегічні інновації. Описові результати виявляють послідовний розрив між упровадженням і перевіркою. Базові технічні методи контролю дуже поширені, водночас заходи, що підтверджують їхню ефективність, відстають. Регулярні резервні копії виконують 19 із 25 компаній, але лише 11 перевіряють, чи можна відновити дані. Дослідження пропонує оновлену модель вимірювання, готову до збирання даних на великій репрезентативній вибірці. Отож, вона забезпечує методологічну основу для систематичного збирання даних про готовність до кібербезпеки словацьких малих і середніх підприємств.

Ключові слова: кібербезпека, малі та середні підприємства, готовність, опитування, Словаччина

JEL Класифікація: M15, G32, D81, L26, C83