CYBERSECURITY READINESS IN SLOVAK SCHOOLS: SURVEY ANALYSIS AND RECOMMENDATIONS

Milan KUBINA – Nikola ŠTAFFENOVÁ – Adam TÍŽIK

University of Žilina, Faculty of Management Science and Informatics, Slovak Republic

e-mail: nikola.staffenova@fri.uniza.sk

Abstract

Cybersecurity has become a critical concern for educational institutions worldwide, as schools increasingly rely on digital technologies for teaching, administration, and student learning. Cybersecurity readiness refers to an organization's ability to effectively identify threats, prevent attacks, and respond to incidents in cyberspace. In essence, being "cyber ready" means being fully prepared to defend against cyberattacks and mitigate their impact. For schools, cybersecurity readiness encompasses not only technical defenses (like secure networks and up-to-date software) but also organizational measures such as staff training, clear policies, and incident response planning.

Keywords**:** *becoming aware, size effects, imitation effects, initial benefit, optimization*

1 INTRODUCTION

In recent years, schools have faced a surge in cyber threats ranging from data breaches and ransomware attacks to online harassment and email hoaxes. Globally, K-12 schools and districts are identified as soft targets for cybercriminals, often due to limited IT security budgets and expertise. A 2025 international survey of over 600 schools revealed persistent security gaps: for example, only 37% of schools had a dedicated cyber incident response plan, and merely 46% implemented multi-factor authentication (MFA) on all devices. Such findings underscore that many schools remain ill-prepared, increasing their vulnerability to disruptive cyber incidents.[4,8,7]

Slovak schools are no exception to these challenges. In Slovakia, the integration of cybersecurity into the education system has historically been fragmented and insufficient. Official reports acknowledge that *"education in information security and cybersecurity in primary and secondary schools is not grasped strategically at all"*, with no unified curriculum or standards in place. This lack of systematic cybersecurity education has resulted in a generation of students, teachers, and school administrators

with uneven awareness of safe online practices. At the same time, Slovakia has witnessed real threats targeting schools. For instance, there was a notable increase in hybrid attacks combining physical threats (like bomb hoaxes) with cyber and information warfare tactics, causing school evacuations and highlighting security weaknesses. Research focusing on Slovak university students found high perceived risks in areas such as cyber espionage and IT infrastructure disruption in schools, reinforcing the need for robust cybersecurity measures and a culture of vigilance in the education sector.[1,3,9,10,11]

Given this context, this article aims to evaluate the current state of cybersecurity readiness in Slovak primary and secondary schools. We do so by analyzing the results of a survey conducted among school staff. The survey covers key areas of cybersecurity readiness, from policy and governance to technical controls and user awareness, providing a multifaceted picture of how prepared schools are to prevent and handle cyber incidents. We discuss these findings in light of national strategies and international best practices, and we propose recommendations to enhance the cybersecurity posture of schools in Slovakia. [4,7,8,9,10]

2 THEORETICAL BACKGROUND

The theoretical background provides an overview of key concepts and existing knowledge related to cybersecurity in educational institutions.

2.1 Cybersecurity Challenges in School Environments

Schools today face a range of cybersecurity threats like those confronting businesses and individuals – but often with far fewer resources to counter them. Common threats include phishing attacks targeting staff or student email accounts, malware and ransomware infecting school networks, data theft from student information systems, and disruptions of online learning platforms. Notably, the education sector has seen an uptick in ransomware incidents, where attackers encrypt school data to demand payment, leading to school shutdowns or loss of student records in various countries. Attackers are drawn to schools due to a combination of valuable personal data and potentially weaker security postures. According to a 2025 Secure Schools report, ongoing security gaps leave schools vulnerable: fewer than half of schools surveyed had policies for promptly disabling former staff access to IT systems, and only 15% performed regular data backups on a termly basis. These shortcomings can amplify the impact of any breach or malware outbreak, as schools may struggle to recover data or prevent unauthorized access when employees depart. [4,7,8,9,10]

Beyond malware, cyberbullying and online harassment are prevalent security and safety issues in schools. While not attacks by external hackers, these incidents underscore the need for strong digital policies and awareness among students and staff. The human factor (students clicking on malicious links, teachers using weak passwords, etc.) is a critical vulnerability. With many schools rapidly adopting educational technology (devices for students, e-learning services, cloud-based gradebooks), the attack surface has expanded, often without commensurate training in cybersecurity for

educators. A lack of specialized IT personnel in schools (especially smaller or rural schools) further exacerbates these risks. [7,8,9,10]

2.2 Importance of Cybersecurity Readiness in Schools

Achieving cybersecurity readiness in schools is crucial for several reasons. Firstly, schools hold sensitive personal data (student identities, health records, family contacts) that must be protected under laws and regulations (including GDPR in the EU). A breach can lead to identity theft or other harms to students and staff, eroding trust in the school's ability to safeguard information. Secondly, cyber incidents can disrupt the educational mission – for example, a ransomware attack might render school computers unusable or take down e-learning platforms, directly impeding instruction. In 2020, when education globally shifted online due to COVID-19, many schools discovered they were ill-prepared to secure remote learning environments, leading to incidents like "Zoom-bombing" and increased phishing attempts targeting teachers. Being cyber ready ensures that learning can continue with minimal interruptions even in the face of attacks. [5,8,9]

Additionally, schools play a formative role in shaping students' digital habits. If cybersecurity and digital ethics are modeled well (through school policies and practices), students gain practical lessons in staying safe online. Conversely, if a school falls victim to a major cyber incident, it can undermine the sense of safety among students and parents. In the worst cases, such incidents may incur financial costs (for recovery, fines, or ransom payments) that strain school budgets already stretched thin. Cybersecurity readiness, therefore, is part of overall risk management and resilience for schools**,** similiar to preparedness for fires or natural disasters. [5,9]

From a governance perspective, international frameworks like the NIST Cybersecurity Framework and regional standards encourage even public sector organizations (schools included) to adopt a cycle of *"identify, protect, detec t, respond, recover"*. For schools, this translates to measures such as: identifying critical digital assets (e.g. student databases), protecting them with controls (access restrictions, backups), detecting incidents (through monitoring or user reports), responding (having an incident response plan), and recovering (data restoration and lessons learned). Unfortunately, many schools have not formally adopted such frameworks**.** Studies indicate that a majority of school IT leaders are not confident in their institution's security posture**.** To improve this, readiness must be approached as a collective responsibility: school leadership must prioritize it, IT staff need support and training, teachers should follow best practices, and students should be engaged in basic cyber hygiene. [6,8,10]

In Slovakia, the importance of readiness is further emphasized by national strategy goals to integrate safety into digital skill development at all education levels. Simply put, building cybersecurity readiness in schools will not only protect the institutions themselves but also contribute to a more cyber secure society by educating young citizens. The following sections describe how our survey was used to gauge where Slovak schools currently stand on this readiness spectrum. [3,5,9,10,11]

3 METHODOLOGY

To assess cybersecurity readiness in Slovak schools, we conducted a structured questionnaire survey targeting school administrators or IT staff responsible for technology and security. This section outlines the survey design, distribution, and analysis approach.

3.1 Questionnaire Survey

A structured online questionnaire was designed to assess cybersecurity readiness in Slovak schools. The questionnaire consisted of 10 thematic sections covering governance, policy, infrastructure, technical safeguards, user awareness, incident handling, and perceived risks.

The survey targeted staff members responsible for digital technologies in schools, including ICT coordinators, deputy school directors, and teachers who manage IT infrastructure as part of their role.

The data were collected between May and September 2025 via an online form (Google Forms). Respondents were approached through school mailing lists, professional teacher groups, and direct communication with school management.

The questionnaire was distributed and administered by the author of this study as part of an academic research project. Participation was voluntary and anonymous. Each respondent completed the questionnaire individually, without external guidance, ensuring that the final data reflect genuine perceptions and real practices within schools.

The research employed a quantitative questionnaire-based approach complemented by qualitative interpretation of selected open-ended responses. The aim was to assess the level of cybersecurity awareness among secondary school students and to analyze their gaming habits, which may influence their exposure to digital risks. The survey was designed as an online self-administered form using Google Forms.

4 RESULTS

The survey results (though partially qualitative due to data unavailability) provide a snapshot of the cybersecurity readiness of Slovak primary and secondary schools. In this section, we interpret these findings in a broader context, compare them with both international data and national objectives, and identify key areas that require attention.

4.1 Key Weaknesses

The survey results expose a pattern of systemic vulnerabilities across Slovak schools' cybersecurity ecosystems. Although some institutions demonstrate commendable progress, particularly those with dedicated IT coordinators or participation in national digital initiatives, the majority operate without the governance, infrastructure, or human capacity needed to meet modern security standards. Three dominant weaknesses emerge: the absence of formal cybersecurity management structures, insufficient implementation of advanced technical safeguards, and inconsistent awareness or training among educators and students. These weaknesses are

interlinked: without clear governance, there is no accountability for maintaining security controls or organizing staff education; without training, even existing safeguards are underused or misconfigured. The consequence is a reactive security posture—schools respond to threats only after damage occurs, rather than preventing incidents proactively. This triad of deficiencies collectively undermines readiness and resilience, leaving many schools exposed to preventable cyber risks.

4.1.1 Lack of Formal Structure

Many schools do not have a designated cybersecurity lead or comprehensive security policies. This absence of governance structure means cybersecurity is handled ad-hoc. Without clear responsibility, important tasks (like regular risk assessments or updating policies) may be neglected. This finding echoes what has been noted at the national level – that cybersecurity in education isn't strategically managed. It's a fundamental issue because governance is the backbone of readiness; everything from budgeting to incident response depends on someone being in charge and guidelines being in place.

4.1.2 Insufficient Technical Safeguards

While basic protections (e.g., antivirus) are present, more robust measures (firewalls, MFA, rigorous patching) are often missing. Notably, the near absence of multi-factor authentication is a concern, as stolen passwords (via phishing or leaks) remain a primary attack vector. With only an estimated handful of schools using MFA, the education sector lags behind corporate practices where MFA adoption is growing to mitigate account compromises. Similarly, infrequent backups (with possibly less than 20% doing them monthly or more) put schools at risk of severe data loss in ransomware scenarios. These technical gaps indicate that the *"Protect"* function in the NIST framework is underdeveloped in schools.

4.1.3 Human Factor and Awareness

The survey suggests that staff training is sporadic and limited. This is problematic since even the best technical controls can be undermined by human error. Phishing, for example, is often successful because an untrained user is tricked – and schools have many potential targets (teachers, administrators, even older students). The lack of systematic cybersecurity education for students is a double concern: it not only leaves students more vulnerable to personal cyber risks (like cyberbullying or scams) but also means they might inadvertently introduce threats into the school network. The national strategy's emphasis on integrating basic safety into digital skills education is directly aimed at this issue, yet our findings show that integration hasn't happened at scale yet.

4.1.4 Incident Preparedness is Low

Perhaps the most alarming insight is that schools are generally ill-prepared to handle a cyber incident. The near lack of incident response plans means when (not if) an incident occurs, response will be slow and improvised. This can turn manageable incidents into crises. For example, a malware infection on one machine, if not contained

and responded to properly, could spread to an entire lab of computers or compromise the school's grading system. The fact that a decent fraction of schools have experienced some incident, but a much smaller fraction have a plan, points to a reactive rather than proactive stance. The consequence is extended downtime – recall that on average it took 280 days to identify and contain a breach in 2020 globally; a school without plan could easily become part of such statistics if a breach is not caught early.

4.2 Comparison with International Benchmarks:

How do Slovak schools compare to international trends? The Secure Schools 2025 report from the UK (and other global sources) provides some benchmarks: e.g., ~37% have incident response plans, ~46% MFA, ~47% have offboarding policies, 15% do regular backups It's likely that Slovak schools are *below* these percentages on most counts, given less funding and attention historically. For instance, if only ~10% of Slovak schools (hypothetically) have IR plans versus 37% globally, that's a significant gap. One area where Slovak schools might be on par is basic antivirus usage – which is nearly universal everywhere now. Another area is perhaps content filtering, since many countries mandate filters in schools (Slovakia does not mandate but provides some). In terms of awareness, anecdotal evidence suggests Slovak teachers have similar challenges as their counterparts elsewhere – many know the basics, but few are well-versed in evolving threats. So overall, Slovak schools' cybersecurity readiness can be characterized as lagging behind best practices, reinforcing the need for concerted improvement efforts.

4.3 Alignment with National Initiatives

The findings hold up a mirror to the goals of Slovakia's national cybersecurity strategies and educational digitization plans. The strategy for 2021-2025 clearly wants to inject cybersecurity into education at all levels. Our analysis shows schools need exactly that injection – in the form of curriculum content for students and training for staff. Additionally, the establishment of a National Center for Digital Technologies in Education (as noted in educational plans) could play a big role: such a center might develop and disseminate security guidelines, offer training modules, and maybe even provide managed cybersecurity services to schools (like centralized monitoring or incident response assistance). The survey results underscore the urgency of these measures. One can argue that the *Recovery and Resilience Plan* investment in digitizing education (Component 17) should explicitly include funding for cybersecurity infrastructure – e.g., ensuring every school gets a next-gen firewall and secure network configuration, along with training.

The Ministry of Education's recent steps, like banning mobile phones in schools to curb distractions and cyberbullying, show awareness of digital risks. However, cybersecurity readiness in the infrastructure and organizational sense needs similar bold measures (albeit not bans, but implementations). There is a role for the National Security Authority (NBU) and its cyber arm (SK-CERT) to perhaps create a specialized outreach to schools, maybe adapting the concept of Cyber Hygiene training (which NBU offers

to government employees) to the school context. The survey results could serve as baseline data to track improvements year over year if such programs are put in place.

4.4 Consequences of Inaction:

Discussing the implications, if the current state does not improve, Slovak schools could face increasing incidents: ransomware outbreaks that halt school operations for days, sensitive data leaks leading to privacy violations, or even manipulation of school IT systems (e.g., changing grades or exam answers) by malicious actors. Additionally, if students are not educated in cybersecurity, they graduate without essential life skills for the digital era – which is a lost opportunity in building a cyber-resilient society. The findings highlight that cybersecurity readiness is not just an IT issue, but a fundamental component of providing safe and uninterrupted education. Modern schools are intertwined with technology; thus, neglecting cybersecurity could undermine educational quality and trust.

In conclusion, the discussion confirms that the survey's revelations, albeit limited by data availability, align closely with known challenges and policy aims. They provide concrete direction on what to fix: assign responsibility, formalize security processes, invest in technical defenses, educate users, and plan for incidents. The next section provides targeted recommendations to address these points.

5 DISCUSSION AND CONCLUSION

The findings of this study demonstrate that cybersecurity readiness in Slovak schools remains fragmented and inconsistent across different regions and school types. Although many schools show awareness of basic cybersecurity practices, the overall level of preparedness is significantly below what is considered standard in international education systems. The results align with previous work stressing that cybersecurity in Slovak schools is not addressed in a systematic way and lacks strategic coordination at the national level [3,9,10].

The most visible weaknesses observed in the survey relate to governance, technical safeguards and human factors. First, a considerable number of schools do not have formalised cybersecurity policies or a designated person responsible for security management. This reflects national findings indicating that Slovak schools often operate without strategic leadership in digital safety [9]. Without defined responsibilities, tasks such as updating guidelines, coordinating training or preparing incident response procedures may be neglected or postponed indefinitely.

Second, the technical foundations of cybersecurity in many schools remain insufficient. While the majority of respondents report the use of antivirus software and regular updates, advanced measures such as network level firewalls, backup routines or multi factor authentication are not consistently implemented. International studies highlight the importance of these safeguards for educational institutions, especially given the rising number of phishing attempts and ransomware incidents targeting schools [4,7,8]. The low frequency of systematic backups observed in the survey contradicts

recommendations for maintaining operational continuity, and increases vulnerability in the event of data loss.

Third, the survey confirms a significant gap in cybersecurity awareness among teachers and students. Many respondents perceive staff knowledge as average or below average, and student understanding as even lower. This gap supports previous research showing that Slovak schools lack unified curricula and structured education aimed at building digital resilience among young people [9]. Training is often infrequent, reactive or limited to basic topics. As a result, users remain a key weak point, particularly given that phishing and user error were consistently identified as major risks by respondents.

Incident response readiness is also limited. Very few schools have a formal incident response plan, and many handle incidents only informally. This reactive posture can prolong recovery time and increase the impact of attacks. International frameworks such as the NIST Cybersecurity Framework emphasize incident planning as a core component of organisational readiness. The absence of such planning suggests that Slovak schools have not yet translated national cybersecurity priorities into practical processes at the institutional level [6].

When compared with international benchmarks, Slovak schools appear to lag behind in several essential areas. For instance, the share of schools that reported having an incident response plan or advanced security controls is lower than global averages reported in the Secure Schools 2025 report [4]. This gap highlights resource constraints and limited expertise, which were also widely mentioned in open ended responses, with schools calling for more funding, stronger technical support and dedicated IT staff. These challenges are consistent with previous evaluations of the Slovak cybersecurity environment [10,11].

At the same time, the survey results reveal strengths that can serve as a foundation for future improvements. The majority of respondents update software regularly and implement antivirus protection. Many schools also express a willingness to improve their cybersecurity posture and acknowledge training as a priority. Several schools demonstrate proactive attitudes by monitoring network activity, conducting regular backups or integrating cybersecurity topics into teaching.

Overall, the discussion shows that improving cybersecurity readiness in Slovak schools requires action at multiple levels. Schools need clear governance structures, technical investment, regular training and practical risk management processes. National authorities can support these efforts through strategic coordination, development of unified educational content, provision of expert services and targeted funding for cybersecurity tools and staff development.

5.1 Conclusion

The study provides the first comprehensive look at cybersecurity readiness in Slovak primary and secondary schools based on direct feedback from those responsible for school digital infrastructures. The results demonstrate that although basic protective measures exist, the overall level of preparedness is insufficient to address modern cyber

threats. The main shortcomings relate to weak governance, insufficient technical protections and low user awareness. These findings align with national and international analyses which highlight similar vulnerabilities in the education sector.

To strengthen cybersecurity readiness, Slovak schools should focus on several priority areas. Establishing formal cybersecurity roles and policies would improve coordination and accountability. Enhancing technical safeguards such as firewalls, multi factor authentication and systematic backups would significantly reduce exposure to common attacks. Regular training for teachers, students and administrators is essential for building a culture of digital safety. Finally, developing and implementing incident response plans would ensure faster and more effective management of security incidents.

Addressing these challenges will require collaboration between schools, regional authorities and national institutions. Strategic guidance, financial support and shared resources can help educational institutions meet modern cybersecurity demands. Strengthening the digital resilience of schools will not only protect their own systems but will also contribute to preparing future generations to navigate the digital world safely and responsibly.

Acknowledgement: Funded by the EU NextGenerationEU through the Recovery and Resilience Plan for Slovakia under the project No. 09I05-03-V02-00010.

REFERENCES

[1] FRANTIŠEK VRÁB (2024). *Cyber Security and Bomb Threats in Schools: A Case Study of Slovakia.* International Journal of Advanced Natural Sciences and Engineering Researches, 8(9)

[2] NATIONAL SECURITY AUTHORITY OF SLOVAKIA (2022). *Report on Cybersecurity of the Slovak Republic in 2021.* https://www.nbu.gov.sk/data/att/3431.pdf

[3] MINISTRY OF INVESTMENT, REGIONAL DEVELOPMENT AND INFORMATIZATION (MIRRI SR) & MINISTRY OF EDUCATION (SLOVAKIA) (2021). *National Cyber Security Strategy of the Slovak Republic for 2021–2025.*

[4] SECURE SCHOOLS (2025). *The State of School Cybersecurity Report 2025.* – (Global survey of over 600 schools) https://www.secureschools.com/

[5] EDUCATION POLICY PROFILE: SLOVAKIA (2025). *Technology in Education – Slovakia.* UNESCO Education Profiles. https://education-profiles.org/europe-and-northern-america/slovakia/~technology

[6] POTOMAC INSTITUTE & GLOBSEC (2019). *Slovak Republic Cyber Readiness at a Glance (CRI 2.0 Profile).*

[7] İSTANBULLU, A., DELIALIOĞLU, Ö., & AKKURT, O. (2025). Determining the digital resilience profiles of classroom teachers. In *INTED2025 Proceedings* (pp. 7029–7036). Valencia, Spain. ISBN 978-84-09-70107-0. ISSN 2340-1079. https://doi.org/10.21125/inted.2025.1815

[8] MALASOWE, B. O., AGHWARE, F. O., OKPOR, M. D., EDIM, E. B., AKO, R. E., & OJUGO, A. A. (2024). Techniques and best practices for handling cybersecurity risks in educational technology environment (EdTech). *NIPES – Journal of Science and Technology Research*, 6(2). https://doi.org/10.5281/zenodo.12617068

[9] HRUŠECKÝ, R., KALAŠ, I., & DVORSKÁ, K. (2024). Safety in the digital age: A conception of education in primary and secondary schools in Slovakia. In *EDULEARN24 Proceedings* (pp. 9286–9294). Palma, Spain. ISBN 978-84-09-62938-1. ISSN 2340-1117. https://doi.org/10.21125/edulearn.2024.2237

[10] KAMPOVÁ, K., MADLEŇÁK, M., & DOLNÁK, I. (2024). Addressing cybersecurity challenges in Slovakia from the education perspective. In *INTED2024 Proceedings* (pp. 5423–5426). Valencia, Spain. ISBN 978-84-09-59215-9. ISSN 2340-1079. https://doi.org/10.21125/inted.2024.1399

[11] HATHAWAY, M., SPIDALIERI, F., & KAUSHIK, A. (2019). Slovak Republic: Cyber Readiness at a Glance. Potomac Institute for Policy Studies and GLOBSEC.