

# Regarding cybersecurity in Bulgarian educational institutions at the K–12 level

Marieta Hristova<sup>1</sup>, Diana Netova<sup>1</sup>, Nikolay Netov<sup>1</sup>  
Sofia University "St. Kliment Ohridski"<sup>1</sup>

marietaivanova@feb.uni-sofia.bg, dianah@feb.uni-sofia.bg, nnetoff@feb.uni-sofia.bg

**Abstract:** Cybersecurity studies increasingly prioritize empirical methodologies to understand and alleviate security risks arising from human behavior, organizational practices, and the advancement of technologies used to perform cyberattacks. This research paper explores how the school management and key educators in Bulgarian K-12 schools comprehend cybersecurity within the academic framework of the Bulgarian education system. Our survey of 927 Bulgarian K–12 educational institutions revealed that a very small number of them assess their level of cybersecurity as extremely low. Respondents see cybersecurity training as essential for ensuring information security within their institutions. Our findings indicate that only 25% of K-12 employees are able to incorporate this training into their qualification programs.

**KEYWORDS:** HUMAN FACTOR IN SECURITY, K-12 EDUCATION, BULGARIA

## 1. Introduction

Cybersecurity establishes policies, procedures, and technical methods to protect, detect, correct, and defend against harm, illegal use or modification, or exploitation of information and communication systems and the data they contain. The rapid speed of technical progress and innovation, along with the rapidly developing nature of cyber threats, exacerbates the situation, [1].

The European Union underlines the significance of the science and research sector, categorizing it as a vital infrastructure sector subject to distinct cybersecurity rules. The NIS 2 Directive (EU 2022/2555) establishes a revised framework for cybersecurity inside the European Union, superseding the original NIS Directive (2016). It aims to improve cybersecurity within the European Union by creating a uniform high standard of security for network and information systems. While K–12 level educational institutions are not covered by NIS 2 Directive, their cybersecurity must not be overlooked. The rapid growth of digital educational infrastructures, combined with the rise of cloud computing, is introducing new risks that established security frameworks are struggling to manage.

A recent article from 2024 delineates and elucidates the primary elements of cybersecurity protection in Bulgaria. The rules for adopting and implementing effective measures to avoid cybercrime are substantiated based on the ideas of "information security," "cyber security," and "cyber resilience." An analysis has been conducted on the principal administrative documents and legal instruments pertaining to national cyber security protection. A legal analysis was performed for the purpose of examining potential vulnerabilities, dangers, and risks to cybersecurity in Bulgaria, [2].

A study conducted in Bulgaria presents findings from a survey of Cybersecurity Experts aimed at collecting and synthesizing extensive information about the challenges of ensuring cybersecurity in the country, with particular emphasis on the critical role of human factors (HF) in this field. The survey was executed as a component of a project funded by the Bulgarian Institute of Public Administration in 2019. The survey inquiries relate to three specific sectors: public administration, academia, and the business sector, each of which supports the functioning of e-government in Bulgaria. The study results corroborated the prevailing consensus among experts that the human element may represent the 'weakest link' in cybersecurity as a socio-technical system. Therefore, experts believe that the majority of cybersecurity breaches are attributable to human error or other HF vulnerabilities. The predominant issues associated with successful assaults are spam and ransomware. Nonetheless, authors observed a propensity among SMEs to regard HF as a potentially robust method for identifying and alleviating cyber hazards. Consequently, they deem it essential to focus on the significance of the human element in the realm of cybersecurity in Bulgaria. Simultaneously, authors highlighted the competency level and inadequate capacity (knowledge and skills) of IT personnel as the primary issue. The research indicates that, despite the acknowledged significance of HF in cybersecurity, the training remains inadequate, [3].

## 2. The Research Backgrounds

The educational institutions at the K–12 level are frequently targeted by cyber threats. K-12 schools and districts are confronting numerous formidable risks as contemporary cyber-attacks get increasingly sophisticated and astute. A suitable starting point for our analysis can be found in [4]. An analysis of the Cybersecurity and Infrastructure Security Agency of the U.S. Department of Homeland Security indicates that K–12 organizations require simplicity, prioritization, and resources tailored to their unique needs. [4] aims to advance the response to this call by offering clear recommendations and resources to assist K–12 organizations in effectively mitigating their evolving cybersecurity risks. The report's key findings and recommendations are summarized as follows:

**Table 1:** Key findings and recommendations, Source[2]

	FINDING	RECOMMENDATION
1	With finite resources, K–12 institutions can take a small number of steps to significantly reduce cybersecurity risk.	Invest in the most impactful security measures and build a mature cybersecurity plan by taking these three steps: <ul style="list-style-type: none"> <li>• Implement highest priority security controls.</li> <li>• Prioritize further near-term investments in alignment with the full list of CISA's Cross-Sector Cybersecurity Performance Goals (CPGs).</li> <li>• Over the long-term, develop a unique cybersecurity plan that leverages the NIST Cybersecurity Framework (CSF).</li> </ul>
2	Many school districts struggle with insufficient IT resources and cybersecurity capacity.	Recognize and actively address resource constraints: Work with the state planning committee to leverage the State and Local Cybersecurity Grant Program (SLCGP). <ul style="list-style-type: none"> <li>• Utilize free or low-cost services to make near-term improvements in resource-constrained environments.</li> <li>• Expect and call for technology providers to enable strong security controls by default for no additional charge.</li> <li>• Minimize the burden of security by migrating IT services to more secure cloud versions.</li> </ul>
3	No K–12 entity can singlehandedly identify and prioritize emerging threats, vulnerabilities, and risks.	Focus on collaboration and information sharing: <ul style="list-style-type: none"> <li>• Join relevant collaboration groups, such as MS-ISAC and K12 SIX.</li> <li>• Work with other information-sharing organizations, such as fusion centers, state school safety centers, other state and regional agencies, and associations.</li> <li>• Build a strong and enduring relationship with CISA and FBI regional cybersecurity personnel.</li> </ul>

Alongside cybersecurity issues, the proliferation of digital content and the ever-improving access to it have heightened pupils' vulnerability to a broader spectrum of online dangers and unsuitable material. Consequently, the necessity for cybersecurity and school child cybersecurity has become imperative. Given the evolving digital landscape, it is crucial to implement safeguards to protect kids from online risks, including cyberbullying, improper content, sexting, sextortion, and online predation. In this context [5]

proposes a novel education-specific K-12 Cyber Protection Framework (CPF) that provides industry-led cybersecurity and cybersecurity standards.

Other current thorough research analyzes the fundamental principles and procedures involved in the formulation and execution of information security management policies inside educational institutions, with a particular focus on "Dr. Ivan Bogorov" Vocational High School of Economics in Varna. The development of an information security policy within the framework of rules and international standards is discussed. The research presents an overview of the primary steps for implementing information security policies in educational settings, specifically within "Dr. Ivan Bogorov" Vocational High School of Economics, [6].

An intriguing study was undertaken from April 2024 to September 2024 with the participation of 56 Bulgarian citizens employed in higher education. The study aimed to evaluate the state of information security in higher education institutions by collecting the views, attitudes, and perceptions of professionals in the field. The queries were classified according to three fundamental principles: demographic characteristics, occupational features, and individual viewpoints. The main finding is that respondents feel secure regarding the performance of their work duties and the protection of personal data in an information security environment, [7].

### 3. Data and Methodology

In order to have a better knowledge of how to enhance security and make schools more resistant to cyber-attacks, the first logical step is to investigate the comprehension of individuals in educational institutions with regards to cybersecurity.

The survey was conducted online from March 31, 2024, to May 3, 2025, involving a poll of 927 school principals, teaching staff, administrative and other staff from Bulgarian K-12 institutions. This study aimed to compare individual differences, evaluate the availability of systematic cybersecurity training, analyze decision-making styles, and assess behavioral intentions related to cybersecurity for the protection of educational and administrative platforms, software, hardware, and computer networks, along with proactive awareness and knowledge enhancement. The survey was designed and distributed via Microsoft Forms within the internal Microsoft 365 environment of the Bulgarian Ministry of Education.

The survey consisted of 22 questions designed to assess individuals' understanding of cybersecurity within their K-12 educational institutions and to gather their viewpoints on the impact of cybersecurity risks on their daily tasks. No incentives were given out, and participation was completely voluntary and anonymous.

Table 2, Table 3 and Table 4 illustrate the structure of the schools involved in the study.

**Table 2:** Distribution of survey-participating schools by type and kind of ownership.

type and kind of ownership	In numbers	percentage of respondents
State	317	34.20%
Municipal	592	63.86%
Private	4	0.43%
(blank)	14.00	1.51%

**Table 3:** Distribution of survey-participating schools by category.

School category	In numbers	percentage of respondents
Gymnasiums	14	2%
Primary school	31	3%
Integrated school	20	2%
Basic school	321	35%
Profiled gymnasiums	114	12%
Vocational gymnasiums	22	2%
Secondary school	400	43%
(blank)	5	1%

**Table 4:** Distribution of survey-participating schools by size.

School size	In numbers	percentage of respondents
With up to 50 students	23	2%
Between 50 and 100 students	98	11%
Between 100 and 200 students	134	14%
Between 200 and 500 students	329	35%
Over 500	332	36%
(blank)	11	1%

This structure of the schools involved in the study gives us reason to believe that the results obtained from our survey are representative only of the different types and sizes of public K-12 schools. Only four private schools participated in the study, rendering the data unrepresentative of this group of K-12 institutions.

Table 5 illustrates the distribution of survey participants by position.

**Table 5:** Distribution of survey participants by position.

Participants' position	In numbers	percentage of respondents
Teaching staff	750	80.91%
Director	103	11.11%
Deputy director	43	4.64%
Administrative and other staff	27	2.91%
(blank)	4	0.43%

The distribution of survey participants by their positions suggests that the results are indicative of the many roles within K-12 institutions.

Table 6 illustrates the distribution of survey participants by age.

**Table 6:** Distribution of survey participants by years old.

Participants' age (years old)	In numbers	percentage of respondents
Up to 25 years old	23	2.48%
Between 24 and 40 years old	210	22.65%
Between 40 and 60 years old	611	65.91%
Over 60	79	8.52%
(blank)	4	0.43%

The age distribution of survey participants corroborates the trend of an aging teaching workforce in Bulgarian K-12 institutions.

### 4. Key Results

Based on the assessments of the K-12 educational institutions surveyed, only 3.34% indicate that they have faced cybersecurity incidents in the past five years. The results are presented in Table 7.

**Table 7:** Has your school had any cybersecurity incidents in the past five years?

Answer	In numbers	percentage of respondents
Yes	31	3.34%
No	884	95.36%
(blank)	12	1.29%

For comparison, according to data from the USA, [8], 82% of K-12 organizations experienced cyber incidents, nearly 14,000 security events were observed, over 9,300 are confirmed incidents. Cyber threat actors target human behavior 45% more often than technical vulnerabilities. We believe that the significant difference in reported cybersecurity incidents between our data and the US data comes from the absence of established and easy-to-follow procedures for reporting every cybersecurity incident in K-12 educational institutions. In many cases, prevalent cybersecurity incidents like spam, phishing and ransomware often go unreported.

This observation is corroborated by our survey data, which reveals a significant lack of personnel accountable for cybersecurity in K-12 schools. Only 5.39% of the respondents who participated in the survey indicated that their school had personnel accountable for cybersecurity, (See Table 8).

**Table 8:** Do you think it is necessary to have a separate position for cybersecurity activities in your school?

Answer	In numbers	percentage of respondents
There is a position in the school that handles cybersecurity activities.	50	5.39%
Yes, it is important to have such a position.	235	25.35%
I can't say.	361	38.94%
Not really	215	23.19%
Definitely NOT.	50	5.39%
(blank)	16	1.73%

At the same time, the majority of respondents, (48.87%), are unable to assess the state of cybersecurity at their institution, (See Table 9). The positive aspect was that a very small percentage of answers identified significant cybersecurity deficiencies in their K-12 institutions.

**Table 9:** What do you thinking about the level of cybersecurity at your school?

Answer	In numbers	percentage of respondents
Very low	16	1.73%
Relatively low	100	10.79%
Can't tell	453	48.87%
Relatively high	293	31.61%
Very high	61	6.58%
(blank)	4	0.43%

A considerable number of respondents in our poll indicated substantial resources and personnel challenges. The most commonly identified essential components of cybersecurity in K-12 schools are cybersecurity training (staff training, selected by 24.77% of respondents, student training, selected by 20.43% of respondents, parent training, selected by 15.61% of respondents), and technological tools and software, selected by 26% of respondents, (See Table 10). At the same time, a very small percentage of respondents ( 8.00%) refer to the presence of regulations governing cybersecurity as a significant factor.

**Table 10:** In your experience, what are the most crucial parts of cybersecurity in your school?

Answer	In numbers	percentage of respondents*
Technical tools and software for cybersecurity	480	26.02%
Staff training	457	24.77%
Student training	377	20.43%
Parent training	288	15.61%
Regulations	148	8.02%
Other	95	5.15%
(blank)	37	3.99%

\* The cumulative percentages surpass 100% as participants were permitted to select several answers.

Despite the recognition of cybersecurity training as a critical element, only 35% responded positively to the question, "Have you participated in any cybersecurity-related training in the past five years?". Additionally, merely 12.73% of respondents confirmed that their K-12 institutions provide annual cybersecurity training, and 11.76% of respondents confirmed that their K-12 institutions provide a rather general cybersecurity training, (See Table 11).

**Table 11:** Do you expect that your qualification plans will include cybersecurity and computer security training?

Answer	In numbers	percentage of respondents*
Not planned	143	15.43%
Somewhat unlikely	127	13.70%
Can't tell	368	39.70%
Somewhat likely	109	11.76%
Annually	118	12.73%
(blank)	62	6.69%

## 5. Conclusions

Our survey of 927 Bulgarian K–12 educational institutions indicates that a insignificant number of workers employed within, define the level of cybersecurity in their institutions as very low. They believe that cybersecurity training, technological instruments, and software are essential components for maintaining information security within their institutions. Simultaneously, our research indicates that fewer than ¼ of those employed in K-12 institutions can rely on such training as an integral component of their qualification plans. We deem it necessary to do further our investigation into the remarkably low number of cybersecurity events observed in our study.

## References

- R. Kaur, D. Gabrijelčić, T. Klobučar, "Artificial intelligence 1] for cybersecurity: Literature review and future research directions," *Information Fusion*, vol. 97, p. 101804, (2023).
- R. Yanev, "Cyber security protection in Bulgaria," *Yearbook 2] - Higher School of Security and Economics*, no. 21, pp. 47-55, (2025).
- Y. Yanakiev, D. Polimirova, "Exploring the Role of the 3] Human Factor in Cybersecurity: Results from an Expert Survey in Bulgaria," *Information & Security: An International Journal*, vol. 44, pp. 39-50, (2020).
- "Protecting our future: partnering to safeguard k–12 4] organizations from cybersecurity threat," Cybersecurity and infrastructure security agency, U.S. department of homeland security, (2023).
- M. Kamaludeen., S. Ismaeel., S. Asiri., T. Allen , C. Scarfo, 5] "A Framework for Cyber Protection (FCP) in K-12 Education Sector," in *IET Conference Proceedings*, (2020).
- D. Vasilev, "Information security management in 6] educational institutions: policies, procedures and good practices," in *Conferences of the department Informatics*, Varna, (2024).
- E. Angelova, "Information Security in Higher Education 7] Institutions," in *Knowledge, Science, Innovation, Technology*, (2024).
- Center for Internet Security, Inc.®(CIS) and Multi-State 8] Information Sharing and Analysis Center® (MS-ISAC®), "An 18-Month, Retrospective Study of Cyber Threat Trends and Defensive Impact in K-12 Education," Center for Internet Security, in partnership with Consortium for School Networking, (2025).