CYBER RISK ASSESSMENT IN EDUCATION

UDC: 378.1:[004.056+005.334]
DOI: https://doi.org/10.53486/tids2025.14

VIOLETA BOGDANOVA
"Ion Creanga" State Pedagogical University of Chisinau
bogdanovaleta@gmail.com
ORCID ID: 0000-0003-4140-6317

Abstract. Cyber risk assessment in educational institutions is related to the processes of risk identification, analysis and assessment. The educational environment, as well as other sectors of the economy, is exposed to quite strong digital threats and vulnerabilities. Due to the growing integration of technologies into teaching, learning, administration and communication processes, educational institutions face various cyber risks. Proper risk assessment helps to protect data, ensure compliance and maintain business continuity.

Keywords: cyber security, training, data protection, business processes in education.

JEL Classification: I29.

INTRODUCTION

In the modern world, education is subject to certain requirements related to the demands of a rapidly changing economic environment. Information technologies penetrated all spheres of education from kindergarten to higher education institutions, from engineering to creative specialties.

The development of digital pedagogy, which began to be actively implemented in the Republic of Moldova during the pandemic, is dictated by the requirements of sustainable development of national education at all levels.

Risks related to threats of violations of integrity, confidentiality and availability of information arise when using digital technologies.

The academic environment is quite open. The peculiarity of the university is its openness due to the constant influx of new students, the organization of scientific events, such as conferences.

Cyber threats are realized due to:

– data leaks and unauthorized access;

– ransomware attacks;

– phishing;

– internal threats;

– outdated system vulnerabilities (Liluashvili, G. B., 2021).

An analysis of scientific literature, represented by numerous articles and conference materials, shows that the rapid digitalization of education has significantly increased the security risks of information systems of educational institutions.

Cyber risks in the educational environment are considered in various works from the position of:

– educational process security (features of online learning, difficulties in monitoring students' knowledge, etc.);

– student security (leakage of students' personal data, easy access to the Internet and AI technologies in the process of studying and assessing knowledge, use of unreliable and dangerous information, cyber resistance to information and psychological influence, etc.);

– financial and economic risks (availability of licensed software and timely updates, availability of sufficient material and technical base in terms of information protection and countering threats, insufficient equipment with auxiliary digital technologies and training of teachers in their use, etc.);

– legal aspects, etc.

Analysis and assessment of cyber risks in the educational environment are presented in the works of the authors: Burov, O. Yu. (2024), Ulven, J. B., & Wangen, G. (2021). Bandara, I., Ioras, F., & Maher, K. (2014). And many others. The increase in cyber attacks on educational institutions is mentioned in the works (Vajpayee, P., & Hossain, G. 2024).

The wide interest in this topic is caused by the fact that Industrial Revolution 4.0 has had a significant impact on education due to the expansion of the use of new digital technologies. The issues of ensuring the safety, integrity, authenticity and confidentiality of information, the safety and operability of university information systems, the confidentiality and integrity of information resources are becoming increasingly relevant.

The purpose of this article is to consider cyber risks in the educational activities of a university from the perspective of the business processes being implemented.

To achieve the goal, the following tasks were solved:

1) the goals of the university were formulated taking into account the modern challenges facing the education system;

2) the main business processes of the university were examined in detail;

3) recommendations were presented for training employees and students to reduce the likelihood of cybersecurity threats.

MAIN CONTENT

Informatization affects all the main, auxiliary and management business processes in the university. A business process is a repeating chain of actions that creates value for an educational organization, students, parents, the labor market, and the state. Value is usually understood as products and services, money, and information.

From the point of view of an educational system, which is a non-profit structure, value can be the achievement of specific results that allow an educational institution to increase efficiency, reduce training costs, and improve the quality of educational services. The goal of an educational institution cannot be formulated, as in a commercial one, in the form of a single position. If we consider in detail the process of goal setting in the educational system, the goal itself becomes a subsystem containing various directions, such as: optimization of the university's work, cost reduction, quality improvement, increasing transparency and control, flexibility and scalability, increasing student satisfaction.

In the implementation of the goal "Optimization of the University's work" it is implied:

- a set of measures aimed at improving the learning process and its quality;
- automation of processes;
- use of analytics systems;
- optimization of the class schedule;
- creation of comfortable conditions for independent work of students;
- use of individual approaches to learning;

- introduction of new technologies in learning;
- use of modern methods of knowledge assessment.

Such a goal as "Cost reduction" for a university is always relevant, since higher education needs additional funding to purchase new equipment, materials for laboratories and much more. To achieve this goal, the following usually occurs:

- transfer of information sources and document flow to electronic form;
- optimization of technical support for the university's activities;
- use of financial assistance.

The sphere of higher education is a highly competitive environment. Therefore, the goal of "Quality Improvement" is permanent for any university

- improving the educational process;
- creating conditions for motivating students;
- improving material and technical support;
- supporting an individual approach;
- implementing a quality management system;
- regular monitoring.

The implementation of the goal "Increasing transparency and control" is dictated by the requirements of the environment in the form of control from the state, the interest of the business environment in the quality of graduates, parents of students. To achieve this goal, it is necessary:

- creation of an information platform for interaction with society;
- development of social network communications of the university;
- implementation of the principle of openness and accountability;
- conducting an open audit of financial activities;
- involvement of the academic staff in decision-making processes.

In today's rapidly changing world, the goal of "Flexibility and Scalability" is aimed at promptly making changes and adapting it to changes in the external and internal environment of the university by:

- ensuring flexibility in planning and implementing programs;
- building programs on a modular principle;
- increasing international student mobility;
- implementing access control systems to educational resources.

No less important is the goal of "Increasing student satisfaction". According to the author's observations, the number of people in the Republic of Moldova who want to obtain higher education is currently decreasing. This is due to both demographic problems and changes in the value system of the younger generation. In order to attract more students to the system of higher professional education, it is necessary to:

- update curricula;
- improve and timely update information on academic disciplines;
- uninterrupted connection to electronic library systems;
- support educational and industrial practices;
- participation in grant activities;
- involvement of students in scientific activities;
- timely and high-quality response to all requests.

Each specific university, depending on its operating conditions, sets specific goals for itself.

The main business processes of the university can be divided into:

– educational activities;

– research activities.

. Many universities provide additional education services, so we will classify it as a main business process.

Table 1 presents the main business processes in the university.

Table 1 Structure of the main business processes in the university

Educational process	Research activities	Additional education
– admission and enrollment of students; – development of curricula; – conducting classes and practical training; – current monitoring and assessment of knowledge; – intermediate monitoring of students' knowledge; – final monitoring of students' knowledge. – issuance of educational documents	– preparation and implementation of scientific projects; – organization of conferences and other scientific and scientific-practical events; – participation in grant research; – interaction with the business environment within the framework of scientific research activities; – work of postgraduate schools; – work of scientific research laboratories	– organizing advanced training courses; – organizing professional retraining; – conducting courses, trainings, master classes for the teaching community and business environment

Source: *developed by the author*

Most of the above core business processes can be targeted for financial gain or reputational damage to a higher education institution.

Data leaks can occur for accidental or deliberate reasons. Data leaks usually occur when unauthorized persons gain access to confidential information. This can happen as a result of cyber attacks or security vulnerabilities. Legal consequences, reputational and financial losses for the university are inevitable.

Cases of ransomware being used in cyber attacks have become more frequent. Most often, the university's information system is blocked, the data is encrypted. The attacker demands payment for restoring access to resources.

Since higher education institutions do not have sufficient financial resources, the data is partially or completely destroyed, the university suffers reputational losses and legal risks.

Phishing is becoming an increasingly common cybersecurity problem. Attackers disguise messages in such a way that deceived university employees voluntarily or involuntarily provide access to confidential information. Phishing messages are used to introduce various malicious software into the university's information system, including ransomware. Fake letters and messages encourage employees to follow suspicious links, enter passwords and other important information. Internal threats are especially dangerous, since employees, due to insufficient qualifications or deliberately steal or destroy the university's information system. The actions of employees can lead

to data leaks, unauthorized access by unauthorized persons. At the same time, system vulnerabilities can remain unnoticed for quite a long time.

Universities lack resources for advanced security. Antivirus software and firewalls alone are not enough to counter fraudulent attacks. In addition to classic malware, university security services face social engineering, zero-day exploits, compromised accounts, Living off the Land (LotL) attacks, and the like.

According to cybersecurity companies Arcticwolf and Asimily, a table of cyber threats faced by universities and colleges from USA in 2020 - 2023 has been compiled (Table 2).

Table 2. Cyber threats faced by US universities in 2020-2023

Year	University/College	Attack Type	Impact/Details
2020	University of California, San Francisco	NetWalker ransomware	Paid $1.14 million ransom to recover encrypted research data
2021	Howard University	Ransomware	Forced cancellation of online/hybrid classes; campus Wi-Fi shut down
2022	Mount Saint Mary College	Ransomware	Data stolen and published on the dark web after refusing ransom
2023	University of Michigan	Data breach	230,000 records stolen; included financial, health, and personal data
2023	Stanford University (Dept. of Public Safety)	Ransomware	430GB of confidential data claimed stolen by Akira ransomware gang
2023	University of Manchester	Ransomware	1.1 million people affected; health records and PII exfiltrated via VPN exploit

Source: *Extracted from official sites of. Arcticwolf and Asimily*

As you can see from the table, most often large universities faced financial extortion `by ransomware attack.

The education system stores a large amount of personal data of students, their parents, guardians, teachers and staff. Attackers encrypt such data for financial gain. The universities presented in Table 2 are only the tip of the iceberg. These educational institutions reported attacks and their consequences. It is obvious to assume that even more educational institutions did not inform the public about such incidents.

Attackers are also aware of the lack of cybersecurity specialists in the university, software and hardware. This allows attackers to use social engineering methods more often and more effectively.

CONCLUSIONS

In the work, cyber risks will be considered within the framework of various university processes.

A modern university faces a wide range of threats. The implementation of cyber threats can lead to financial and reputational losses. To minimize risks, the university must apply reliable access

restrictions and regularly audit the information security system. The implementation of information security standards will be effective: NIST SP 800-171, Cybersecurity Maturity Model Certification (CMMC) 2.0, GDPR etc.

REFERENCES

1. 4 Cyberattacks that Shook Universities and Colleges in the Last Year. Available at: https://asimily.com/blog/4-cyberattacks-universities-and-colleges/ [Accessed 01.05.2025].
2. 10 Cybercrimes Against Colleges and K-12 Schools, and How To Prevent Them Available at: https://arcticwolf.com/resources/blog/cyber-attacks-against-schools-and-colleges/ [Accessed 01.05.2025].
3. Gremalschi A., (2021) Lecția Pandemiei: de la simpla alfabetizare digitală la o pedagogie digital autentică, Univers Pedagogic, Nr. 6 (748), p.3
4. Jomir, E., Belostecinic, G. (2022) Educația şi cercetarea universitară ca factor de ameliorare a securităţii naţionale. In: The Collection. : Economic security in the context of sustenable development, 17 decembrie 2021, Chisinau. Chişinău: Departamentul Editorial-Poligrafic al ASEM, 2022, 2, pp. 45-50.
5. Liluashvili, G. B., (2021) Cyber risk mitigation in higher education. Law & World, 17, 15.
6. Vajpayee, P., & Hossain, G. (2024, October). Cybersecurity Education in High School: Exploring Cyber Assets, Cyber Value at Risk, and Authentic Assessment. In 2024 IEEE Frontiers in Education Conference (FIE) (pp. 1-9). IEEE.
7. Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. Future Internet, 13(2), 39.
8. Bandara, I., Ioras, F., & Maher, K. (2014). Cyber security concerns in e-learning education. In ICERI2014 Proceedings (pp. 728-734). IATED.
9. Chiriac L., Bogdanova V. (2024) Modeling of information system security by fuzzy logic methods. In CAIM 2024. Proceedings of the 31th Conference on Applied and Industrial Mathematics, 2024, Bucharest: MATRIX ROM, p. 24-27.
10. Буров, О.Ю., Литвинова, С.Г. Пінчук, О.П. (2024) Cybersecurity in the digital educational environment: external and internal risks. ІЦО НАПН України, м. Київ, Україна, pp. 64-74.
11. Буров, О.Ю. (2021) Cyber risks and the use of artificial intelligence in networking In: Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку. Черкаський національний університет імені Богдана Хмельницького, м. Черкаси, Україна, pp. 60-62.