International Journal of Innovative Technologies in Social Science

e-ISSN: 2544-9435

Scholarly Publisher
RS Global Sp. z O.O.
ISNI: 0000 0004 8495 2390

Dolna 17, Warsaw,
Poland 00-773
+48 226 0 227 03
editorial_office@rsglobal.pl

ARTICLE TITLE	A STUDY OF THE LEGAL ENVIRONMENT AND IMPLEMENTATION OF CYBERSECURITY IN MONGOLIA'S EDUCATION SECTOR
DOI	https://doi.org/10.31435/ijitss.3(47).2025.3781
RECEIVED	11 August 2025
ACCEPTED	22 September 2025
PUBLISHED	30 September 2025
LICENSE	The article is licensed under a **Creative Commons Attribution 4.0 International License.**

A STUDY OF THE LEGAL ENVIRONMENT AND IMPLEMENTATION OF CYBERSECURITY IN MONGOLIA'S EDUCATION SECTOR

Munkhtsetseg Erdenebulgan
National Defense University, Ulaanbaatar, Mongolia

Munkhjargal Bayanjargal
Nomad Cyber Defense LLC, Ulaanbaatar, Mongolia

Byambadorj Dondogmegd
University of Science and Technology, Ulaanbaatar, Mongolia

ABSTRACT

Cybersecurity in the education sector is distinct from other sectors, as the primary participants are children and young people who may not fully comprehend cyber threats and risks. Therefore, it is crucial to devise a strategy to mitigate cyber threats and enhance the cybersecurity knowledge and skills of teachers and staff. The aim of the research is to pinpoint the key challenges, opportunities, and future trends in implementing cybersecurity policies and regulations in Mongolia's education sector. This is essential for minimizing risks.

Mongolia's cybersecurity efforts are governed by the 2021 Law on Personal Data Protection and the 2021 Law on Cybersecurity, which establish a system, principles, and legal framework for cybersecurity operations. The legal environment has been in development for years. A study of the legal environment and implementation of cybersecurity in Mongolia's education sector would likely examine how these laws are applied within educational institutions, assess the effectiveness of the current legal framework in protecting data and systems, and identify any challenges in implementing cybersecurity measures in the education sector.

KEYWORDS

Cybersecurity, Cyber-Attacks, Risks, Education Sector, Legal Environment

CITATION

Munkhtsetseg Erdenebulgan, Munkhjargal Bayanjargal, Byambadorj Dondogmegd. (2025). A Study of the Legal Environment and Implementation of Cybersecurity in Mongolia's Education Sector. *International Journal of Innovative Technologies in Social Science*, 3(47). doi: 10.31435/ijitss.3(47).2025.3781

Introduction

The use of e-learning has significantly increased worldwide since the Covid-19 pandemic, with learning activities relying on electronic technology and a vast amount of information being stored and transmitted electronically. This trend has continued in the post Covid-19 years. As educational activities, management, and information exchange in the education sector increasingly rely on new infrastructures and platforms, the risks in the cyber environment, including the number and scale of attacks, are continuously rising. This poses a threat to the information systems and networks of educational institutions, as well as the personal information of teachers and students.

Despite the education sector containing valuable data, there is a relative lack of awareness regarding cyber risks and the widespread distribution of sensitive data, making it a prime target for cyber-attacks, as evidenced by international studies. For instance, a research report from May 2022 indicated a 44% increase in cyber-attacks compared to the previous year.

According to Microsoft's Global Threat Activity Tracker study in April 2023, approximately 80% of the 90 million attacks recorded worldwide were aimed at educational institutions. International research highlights the education sector as one of the high-risk sectors for cyber-attacks.

Nevertheless, Mongolia is confronted with numerous challenges in the present cybersecurity landscape within the education sector. One such challenge is the lack of cybersecurity expertise, manpower, financial resources, and technical capabilities in local schools and primary and secondary educational institutions, which heighten the vulnerability to cyber threats.

While Mongolia has established a legal framework for cybersecurity in the education sector through national laws, strategies, and regulations, there remains a need for a comprehensive long-term plan and a multi-faceted approach to cybersecurity protection. Targeted policies and assistance are crucial for the efficient enforcement of legal regulations in the education sector.

Cybersecurity in The Global Education Sector

There is no industry in the world that is immune to cyberattacks. As a result, the number of attacks continues to grow rapidly. Ransomware attacks targeting the education sector increased by 19% in 2020. This increased by 26% in the first half of 2021. The average cost of these ransomware attacks was $450,000. Two-thirds of the colleges surveyed did not have basic email security measures in place, and 86% of them were victims of botnet attacks.

A 2021 report by the UK's National Cyber Security Centre (NCSC) stated that ransomware attacks targeting the education sector are spreading globally and are increasing rapidly every year, so it is necessary to increase the response to attacks.

According to the 2023 cybersecurity report released by Check Point software technology company, attacks against all sectors are continuously increasing in the data collected for the study, with education and research institutions being the most targeted sectors.

There is an average of 2,314 attacks per organization per week, an increase of more than 40 percent in 2022 compared to 2021.[1]

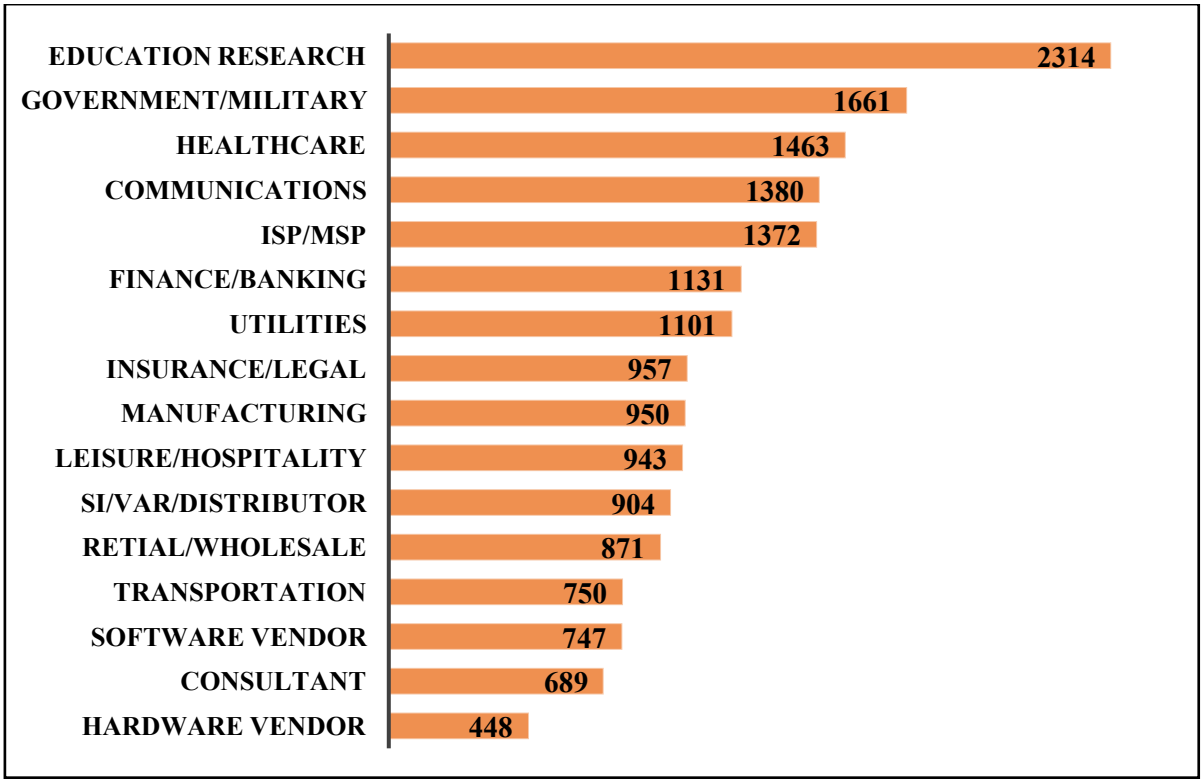

Fig. 1. *The average weekly cybersecurity performance by industry in 2022.*

[1] Check Point Security. (2023). *Security report*.

The statistics show that cyber security research organizations are seeing similar impacts across various sectors, with a notable global focus on the education sector. The report, published by Statista, a prominent global research organization established in Germany, is displayed in the image below.

Table 1. Data from Statista showing the industries impacted by cyberattacks between 2020 and mid-2023.

Characteristic	Jul 2020 – Jun 2021	Jul 2021 – Jun 2022	Jul 2022 – Jun 2023
Education	3%	14%	16%
Government	48%	10%	12%
Think tanks and NGOs	31%	17%	11%
IT	2%	22%	11%
Communications	-	2%	6%
Finance	-	5%	5%
Transportation	-	2%	-
Defense industry	-	-	4%
Energy	1%	-	3%
Manufacturing infrastructure	2%	-	2%
Intergovernmental organizations	3%	2%	-
Media	-	4%	-
Health	1%	2%	-
Other critical infrastructure	-	-	5%

The Current Cyber Security Situation in Mongolia's Education Sector

Globally, ransomware attacks targeting the education sector have seen a steady annual increase, with a 19% rise in 2020 and a further 26% increase in 2021 [8]. A report from the National Cyber Security Center (NCSC) highlights the escalating trend of ransomware attacks on educational institutions worldwide, emphasizing the urgent need for enhanced response measures.

Mongolia is emerging as a potential hotspot in the cyber warfare landscape, particularly amidst the ongoing conflict between Russia and Ukraine. Positioned between the influential powers of China and Russia, Mongolia faces heightened susceptibility to cyber threats. To address these challenges, Mongolia has enacted comprehensive legal frameworks at multiple levels to bolster cybersecurity in the education sector and safeguard information privacy.

These initiatives encompass:

- ***The Cybersecurity Act*** (2021) which outlines the protection of critical information infrastructure, cybersecurity principles, and the responsibilities of organizations;
- ***The Personal Data Protection Act*** (2021) which sets out the procedures, consent principles, security measures, and data breach notification requirements for handling personal data in educational institutions;
- ***The National Cybersecurity Strategy*** (2022) which outlines a phased approach in four key areas: capacity building, standards, technology, and public awareness;
- ***JICA's "Cybersecurity Human Resource Development Project"*** (2023 - 2026) which aims to enhance the skills of IT professionals in educational institutions, develop curricula, and establish professional networks;
- ***The UNESCO/ICDL Digital Competency Program*** (2024) which has introduced an internationally recognized training system to enhance digital literacy and cybersecurity awareness among teachers and students.

Some of the legal and educational initiatives mentioned above serve as the foundation for enhancing cybersecurity in the education sector, mitigating cyber threats, and bolstering professional capabilities. A study conducted in 2024 by the Ministry of Electronic Development and Communications of Mongolia highlighted the insufficient cybersecurity expertise, technical infrastructure, and workforce readiness in local educational establishments, impeding their ability to effectively combat cyber-attacks. The cybersecurity landscape in Mongolia's education sector currently grapples with various obstacles, including inadequate cybersecurity knowledge, human resources, financial support, and technological assets in local schools and primary and secondary educational institutions.

Cybersecurity knowledge gap: The Cybersecurity Capacity Assessment Study of Mongolia found that the level of cyber security knowledge and skills in the country is rated as "beginner to emerging." This suggests that both teachers and students lack adequate digital literacy and awareness of cybersecurity.

Human resource constraints: To address the shortage of cybersecurity professionals, Mongolia has introduced master's level training programs at the Mongolian State University of Information and Communication Technology (SUST) in 2021 and at the Mongolian National University of Information and Communication Technology (NUIS) in 2024. However, these programs are primarily available in the capital city, limiting access to experts in local schools.

Financial and technical resource constraints: The study also emphasized the need for investment in standards and technology to improve cybersecurity. The small cybersecurity market and lack of investment further compound the technical resource limitations in local schools.

Local school conditions: Local schools are particularly vulnerable to cyberattacks due to their limited cybersecurity knowledge, human resources, financial resources, and technical resources. The risk of cyberattacks is heightened by the inadequate security of their information systems and networks, as well as the lack of protection for teachers' and students' personal information. International cybersecurity research organizations conduct annual evaluations of countries based on specific criteria. Table 2 displays Mongolia's performance.

Table 2. Mongolia Cybersecurity Index

No	Name	2017	2018	2020	2021	2022	2023	2024
1	The International Telecommunication Union's CAB Index”	**104**	**85**	**120**				**103**
2	According to the United Nations e-Government Development Index				**92**	**74**		**46**
3	European Union cyber security by status index				**26**			
4	NCSI National Cybersecurity Index						**137**	**137**

In December 2021, Mongolia implemented the Cybersecurity Law, leading to the establishment of various state and non-state entities dedicated to enhancing cybersecurity and raising public awareness. According to the 2024 Global Cybersecurity Index by the International Telecommunication Union, Mongolia was ranked at level 3 ("Strengthening") out of 5 levels. The evaluation highlighted strong performance in law, regulation, and organizational aspects, with Mongolia surpassing the regional average in the Asia-Pacific region. However, the country received lower ratings in technical protection and cooperation.

The Factors That Influence

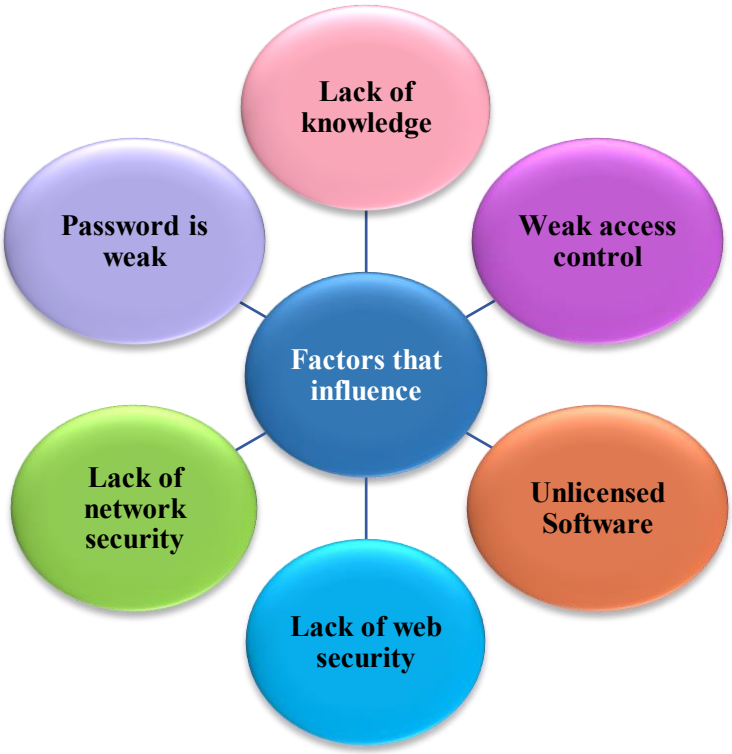

Diagram 1. *The factors influencing cybersecurity.*

The factors that commonly impact cybersecurity also apply to the education sector.

However, unlike other industries, the primary end users in education are students and pupils, who often lack strong data processing and threat-predicting skills. Political issues play a significant role in influencing these factors. For instance, cyberattacks related to the Russia-Ukraine conflict and those exploiting the pandemic have had a notable impact.

With the shift to remote learning prompted by the Covid-19 outbreak in early 2020, educational institutions' networks have expanded significantly. This increased connectivity has made them more vulnerable to cyber threats, leading to a rise in cyberattacks targeting the education sector globally. Diagram 1 illustrates the common factors.

Malicious software is a key threat to cybersecurity, and the detection process differs based on how it is deployed. Malicious software can infiltrate educational information systems, websites, and emails, carrying out activities like copying, deleting, altering, forwarding, and exploiting data. Furthermore, these activities can manipulate the functioning of physical devices (bots), disrupt systems, and potentially halt operations. Cybersecurity malware indicators reveal an increase in phishing and ransomware attacks. Educators, staff, and students in the education sector should prioritize learning basic techniques to safeguard against these threats.

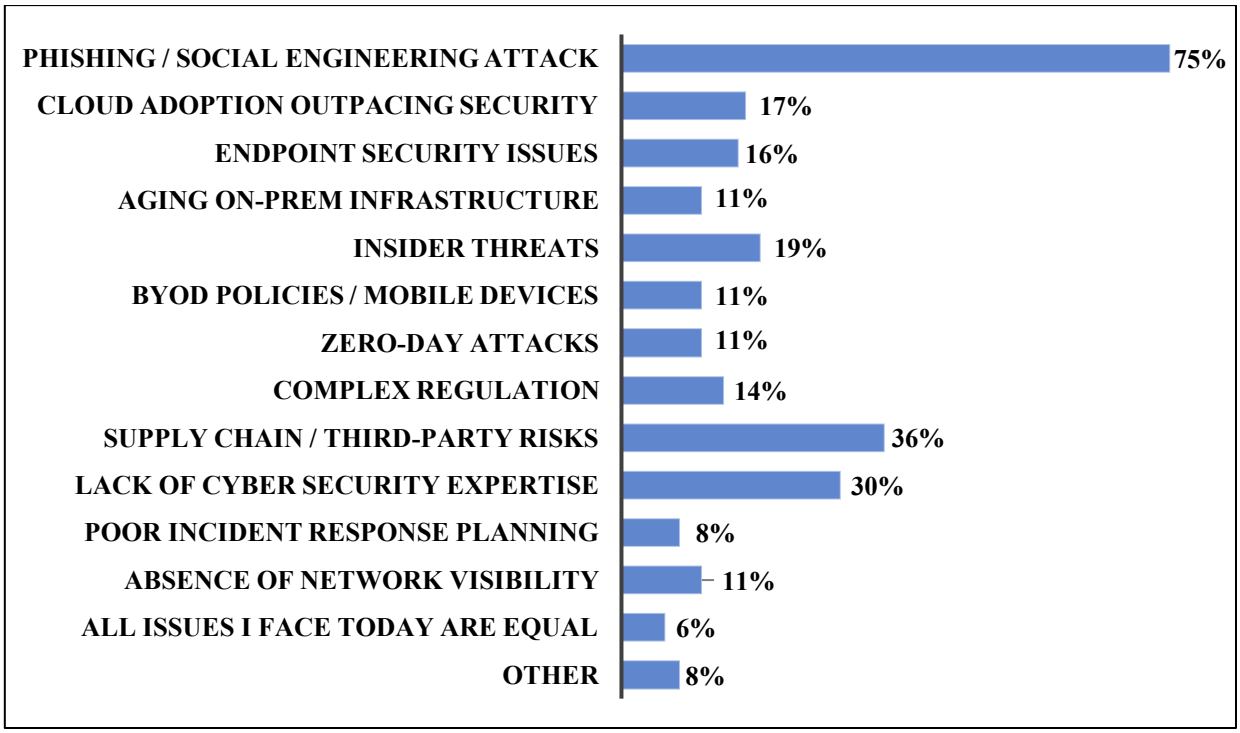

Fig. 3. *Cyberattack indicators as of mid-2022*

Ransomware attacks in the education sector:

- In 2020-2021, 84 ransomware attacks targeted 1,681 higher education institutions.[1]
- 66% of universities lacked basic email security settings in 2021.[2]
- 38% of universities examined in the 2021 Higher Education Cybersecurity Report had unsecured or open database ports.[3]
- The education sector was the primary target of ransomware attacks last year, with 79% of global higher education institutions affected.[4]
- 59% of higher education institutions hit by ransomware reported significant business or revenue losses, while 28% reported minor losses.[5]
- The average cost of recovering from a primary education ransomware attack was $750,000 in 2023.[6]
- The average cost of a data breach in the education sector in 2023 was $3.65 million.[7]

The Preventive Response Measures

Preventing cyberattacks involves more than just configuring devices; it requires a comprehensive system that begins with policy, addresses human behavior and operational controls, implements technical measures, and adheres to legal regulations. Protection is structured in a layered or hierarchical architecture, ensuring compliance with fundamental policies, procedures, and standards, integrating organizational culture and human factors, implementing controls for data, applications, networks, and access in a phased approach, and continuously enhancing detection and response capabilities across all layers. This approach enables controls to work together synergistically, reducing the risk of a complete breach compromising all defenses.

[1] International Institute for Democracy and Electoral Assistance. IDEA (2019). *Cybersecurity in elections: Models of interagency collaboration*.
[2] Emsisoft Malware Lab. (2021, January 18). The state of ransomware in the US: Report and statistics 2020. *Emsisoft*.
[3] BlueVoyant. (2021). *Higher education cybersecurity report*.
[4] BlueVoyant. (2022). *Higher education cybersecurity report*.
[5] Sophos. (2023). *The state of ransomware 2023 report*.
[6] Ibid
[7] Ibid

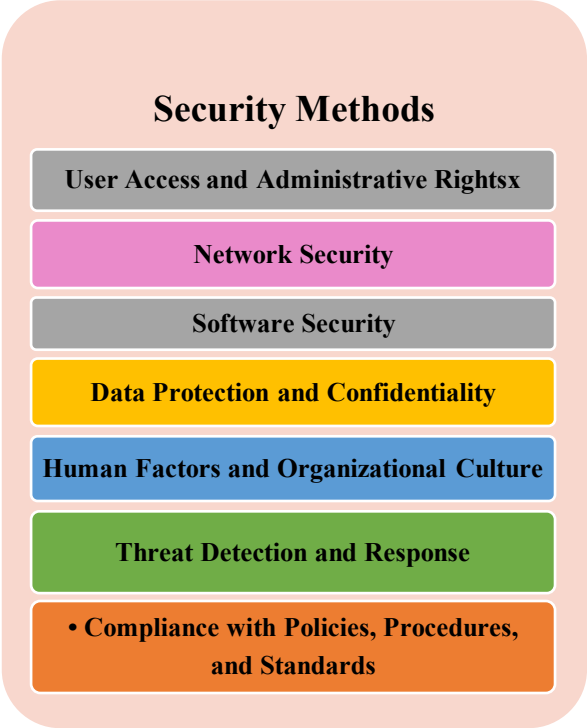

Diagram 2. *The various strategies for thwarting cyber attacks.*

There are various policies, programs, and initiatives internationally to ensure cybersecurity.

Some of the initiatives initiated by the Government of India include:

- ***National Education Policy (NEP) 2020:*** NEP 2020 emphasizes the importance of cybersecurity education and advocates for the integration of cybersecurity concepts into school curricula.
- ***Cyber Security and Health Awareness Network (CSHAN):*** CSHAN is a government initiative that aims to raise awareness about cybersecurity among students, teachers, and parents through workshops, training programs, and online resources.
- ***Cyber Surakshit Bharat Mission:*** The Cyber Surakshit Bharat Mission aims to enhance India's cybersecurity capabilities, including through targeted interventions in the education sector.

Rules and regulations that are in effect in the European Union

- The implementation of the EU General Data Protection Regulation (GDPR) has heightened the significance of cybersecurity and data protection. Cyber attackers employ social engineering tactics to infiltrate and undermine systems, deceive individuals into opening emails, downloading harmful files, and visiting deceptive websites. While the consequences can be severe, the potential risks can be greatly mitigated through educating staff and students about cybersecurity awareness.
- The government is actively striving to diminish cybersecurity threats within its supply chain, and entities vying for government contracts, such as universities pursuing research grants, have the option to acquire the Cyber Essentials Plus certification at no cost.

Programs initiated by certain US technology firms:

- Intel IT has introduced the "Online Safety for Kids" initiative to safeguard information security. The program is designed to educate children and adolescents about cyber threats through presentations, parental guidance, and age-appropriate Q&A sessions for students aged five to 18. This effort will mitigate the effects of cyberattacks.

Cyber security measures in Mongolia's education sector are being implemented gradually. The Ministry of Digital Development, Innovation and Communications, with support from the Japan International Cooperation Agency (JICA), is carrying out a technical cooperation project to enhance cyber security and develop human resources. University teachers and civil servants are actively involved in this initiative.

Additionally, the ***"Let's be cyber-savvy"*** e-development day event is being launched in Bayankhongor aimag, the first aimag of the Khangai region. Representatives from the Telecommunications Regulatory

Commission and other organizations are conducting training sessions for teachers and students in secondary schools in Bayankhongor aimag.

The training covers topics such as child protection in the online environment, technological advancements, regulations related to children's rights online as outlined in the revised "Law on Child Protection," career options, and essential learning skills.

There are 18 organizations authorized to offer information security audits, consultations, training, and services, which is crucial for the digital advancement of our nation. However, there is a scarcity of comprehensive reports on cybersecurity.

Notably, the absence of reports on the education sector suggests insufficient efforts to address cybersecurity in this area. A development model for enhancing cybersecurity in the education sector has been created using a method that guarantees the alignment of system strategic assessment and planning.

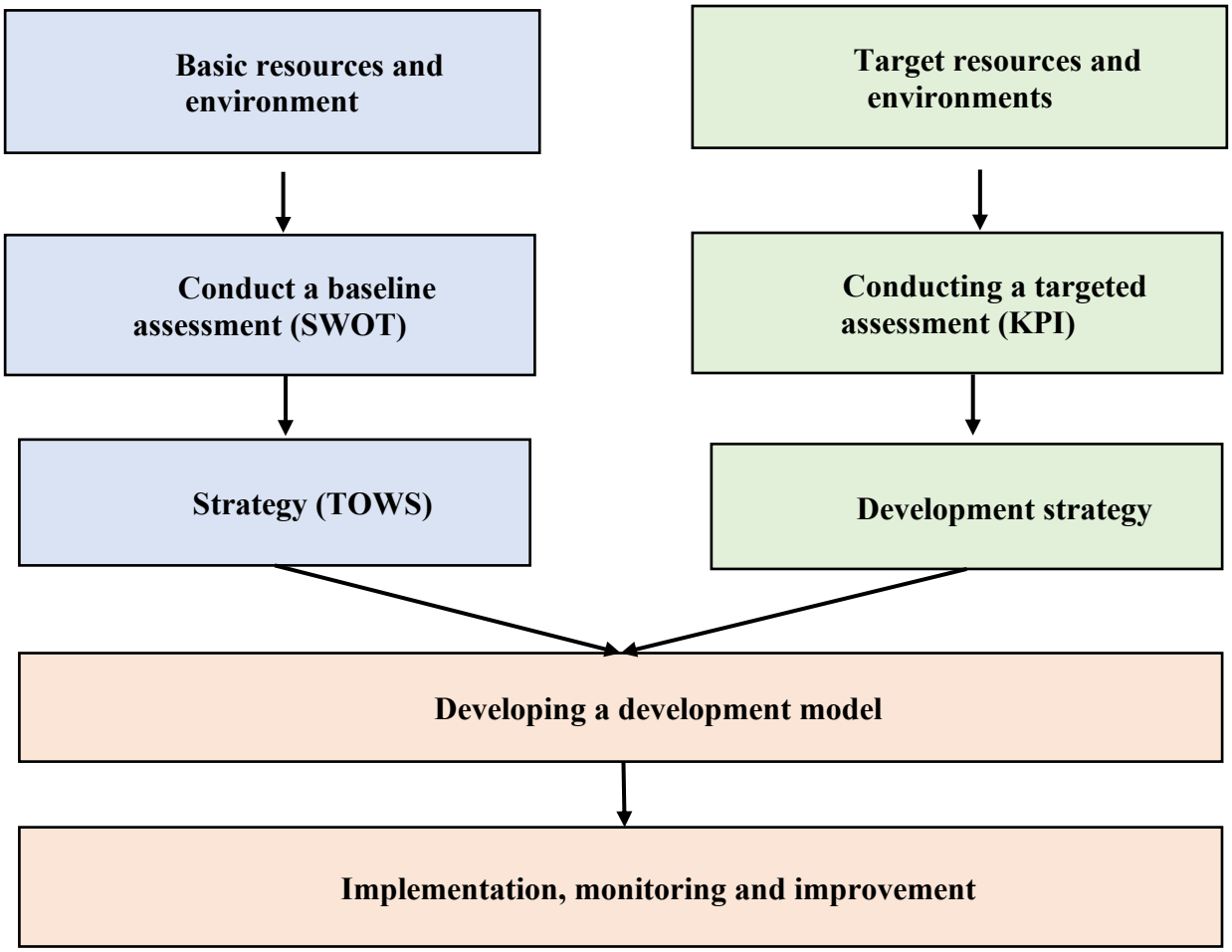

Diagram 3. *Planning the development of a cybersecurity environment in Mongolia's education sector.*

Identifying the basic resources and environment

- ***Legal environment:*** Reviewing the laws, regulations, and standards governing cybersecurity in the education sector to identify any overlaps, gaps, or inconsistencies. For example: The "Cybersecurity Law," the level of implementation of the international ISO/IEC 27001 standard.
- ***Cybersecurity capacity:*** Evaluating the skills, training, and certification status of industry professionals (CEH, CISSP, etc.), and their experience in detecting and preventing threats.
- Technical and technological conditions: Assessing whether the infrastructure, including networks, servers, data storage and backup systems, and security software (firewall, IDS/IPS), is sufficient.
- Stakeholder knowledge and information: Examining the perceptions, attitudes, and practices of teachers, students, and IT staff regarding cyber risks.

Conduct a baseline assessment (SWOT)

- Strengths: Effective aspects of the existing security setup, experienced staff numbers, and local support.
- Weaknesses: Inadequate financial resources, obsolete technology, and lack of user expertise.
- Determine strengths and weaknesses along with contributing factors.
- Incorporate real incidents and data on security breaches in the analysis.

Strategy (TOWS)

- In the future, all educational institutions will have robust information security measures in place to protect against cyber attacks.
- Automated security systems will swiftly identify and address threats,
- Ensuring a strong cybersecurity culture that complies with both national and international standards.

Target resources and environments

- Identify the necessary technology, standards, human resource capabilities, and financial investments needed to reach the envisioned future state.
- Explore global best practices and evaluate their adaptability to the education industry for potential implementation.

Conducting a targeted assessment (KPI)

- Plan to capitalize on strengths and opportunities, and mitigate weaknesses and risks.
- Examples of opportunities:
- Establish a connection to a national data center.
- Mandatory cybersecurity training at all levels.
- Implement an AI-based intrusion detection system.
- Goals and indicators: Reduce personal data breaches by 50% annually and achieve an automated detection rate of 95%.

Development strategy

- Short-term goal (1–2 years): Implement legal reforms and provide user awareness training.
- Medium-term goal (3–5 years): Implement infrastructure reforms and establish a national cyber testing laboratory.
- Long-term goal (5+ years): Fully deploy an automated security platform.

Developing a development model

- Compare the existing state with the desired future state to identify the gap in achieving the goal.
- Create a comprehensive implementation plan, including budget, timeline, responsible department, and evaluation metrics.

Implementation, monitoring and improvement

- Ensure that the education cybersecurity strategy is in line with the National Cybersecurity Policy and national initiatives like “Electronic Mongolia”.
- Secure funding from the state budget, international sources, and collaboration mechanisms.
- Encourage involvement from government, private sector, and external partners to enhance cybersecurity efforts in education.

The cybersecurity development model in Mongolia's education sector is comparable to the approach used for creating a cybersecurity strategy, offering benefits such as systematic and incremental planning, proactive risk mitigation, alignment with national policies, inter-sectoral coordination, measurable outcomes, and active engagement in international collaboration.

Conclusions

Educational institutions gather and store a significant amount of sensitive data, including personal details of students and their parents, academic records, specific health information, home addresses, contact numbers, and financial details. This data is a prime target for cybercriminals and is often used for illicit activities like identity theft, fraud, and extortion. The rising number of cyberattacks on the education sector underscores the critical need for robust cybersecurity measures. Safeguarding the cybersecurity of educational institutions is not just a sector-specific concern but a national priority.

Research organizations in various countries, such as the United States, Canada, the United Kingdom, Germany, India, China, Hong Kong, and the Republic of Korea, regularly analyze cybersecurity trends in the education sector and publish reports. These studies are crucial for informing other nations' prevention and

response strategies and understanding global cybersecurity developments. The findings offer valuable insights for evaluating the sector's current security posture, devising growth models, and formulating policy approaches.

However, in Mongolia, the absence of comprehensive reports and official data on cybersecurity in the education sector hampers efforts to prevent, mitigate, and swiftly address data breaches. While national-level educational institutions must enhance their cybersecurity protocols and systems, local primary and secondary schools struggle with limited human resources, cybersecurity expertise, and financial and technical capabilities, leaving them vulnerable to cyber threats.

Efforts are underway to enhance the cybersecurity knowledge and skills of educational staff through training programs and projects supported by government and international entities. However, the lack of a centralized and sustainable mechanism for delivering these initiatives hinders the establishment of a uniform level of protection. Therefore, a systematic assessment of cybersecurity in the education sector, including risk evaluations, analysis, and the development and implementation of a comprehensive strategic plan, is essential across Mongolia.

REFERENCES

1. BlueVoyant. (2021). *Higher education cybersecurity report*.
2. BlueVoyant. (2021). *State of education 2021 report*. https://www.bluevoyant.com/resources/cyber-attacks-against-smb-defense-contractors-report-bluevoyant
3. BlueVoyant. (2022). *Higher education cybersecurity report*.
4. The Strategic and International Studies. (2023). *Significant cyber incidents since 2006*.
5. Check Point Security. (2023). *Security report*.
6. Department for Digital Development and Communications. (2024). *Cyber literacy program*.
7. Department for Science, Innovation & Technology. (2023, June 22). *Cyber essentials scheme process evaluation*. GOV.UK. https://www.gov.uk/government/publications/cyber-essentials-scheme-process-evaluation/cyber-essentials-scheme-process-evaluation
8. Emsisoft Malware Lab. (2021, January 18). The state of ransomware in the US: Report and statistics 2020. *Emsisoft*.
9. India Today Education Desk. (2024, January 18). *Cybersecurity threats rising in educational institutions across India*.
10. Intel. (2023). *The importance of technology in education*.
11. International Institute for Democracy and Electoral Assistance. IDEA (2019). *Cybersecurity in elections: Models of interagency collaboration*.
12. International Telecommunication Union. (2024). *Global cybersecurity index 2024*.
13. IT Governance. (2023). *What is social engineering? Examples & prevention tips*.
14. Mahashevta, & Sharma, S. (2023). Ensuring cybersecurity in the digital India context of NEP 2020.
15. Microsoft. (2023). *Global threat activity tracker research report*.
16. Ministry of Digital Development, Innovation and Communication. (2024). *Mongolian education cybersecurity survey*.
17. National Cyber Security Center. (2023). *NCSC annual review 2023*. https://www.ncsc.gov.uk/collection/annual-review-2023
18. National Cyber Security Center. (2023). *Cyber threat report 2022/2023*. https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-2022.2023-Cyber-Threat-Report.pdf
19. Sophos. (2023). *The state of ransomware 2023 report*.
20. Center for Strategic and International Studies (2023), *CSIS annual review 2023*.