Importance of Introducing Cyber Security Policy Regulations and Practices into Education Systems in Bosnia and Herzegovina

By: Amila Planinčić

DCAF Young Faces 2023 Participant

Abstract

Multiple public educational institutions in Bosnia and Herzegovina have recently been target of cyber-attacks (i.e. series of bomb alerts received by a large number of primary and secondary schools from an unknown, alleged Russian email address). The evidence on cyber vulnerability of educational institutions in BiH is still scarce. However, analysis of the existing cyber security policy framework and digital infrastructure of the education systems in BiH showcases that education systems are widely unprepared for cyber threats. Additionally, a large majority of educational workers has very limited ICT competences, and low awareness level regarding threats and challenges in online space. This policy paper aims to address the importance of building a legal framework and enhancing technical capacities of education systems in the cyber security domain, as to prevent, mitigate and address the ongoing and future cyber security-related threats and challenges.

Keywords: cyber security policy regulations, cyber security practices, education systems[1], digital transformation

Introduction

Since 2020, the COVID-19 outbreak has accelerated the digital transformation of the education sector by forcing hundreds of millions of students and teachers across the globe to transition from in-person to digital learning and teaching. Online learning offers many opportunities, as it can enhance the quality and relevance of learning, strengthen inclusion, and improve education administration and governance, as well as prevent learning disruptions in times of crisis. However, these opportunities come with a cost, as relying more on digital learning tools can represent a major gateway for cyber security threats. According to the CSO Online findings, during the first half of 2017, the education sector accounted for 13 per cent of data breaches, resulting in the compromise of around 32 million records.[2] "Although educational institutions may not seem as wealthy or as target-rich as healthcare organizations or private businesses, they in fact house a great deal of sensitive personal and financial information, as well as valuable proprietary research data."[3] In May 2022, in Bosnia and Herzegovina's Canton Sarajevo, all primary and most of the secondary schools were target of a series of cyber-attacks (i.e. bomb alerts received from an alleged Russian email address).[4] The authorities reported that

[1] Throughout this document, *education systems* term is used in plural to reflect a decentralized education sector structure in Bosnia and Herzegovina, consisting of 16 government authorities/line ministries with competences in education (at state, entity, Brčko District and cantonal levels)

[2] *Top Cybersecurity Threats Active in the Education Sector Today – and Why You Should Care,* (2018, September 28), CSO Online.com, available at: https://www.csoonline.com/article/3250862/top-cybersecurity-exploits-active-in-the-education-sector-today-and-why-you-should-care.html

[3] ibid.

[4] *Bosnia Swamped with Hundreds of Fake Bomb Alerts,* (2022, June 02), Eyewitness News, available at: https://ewn.co.za/2022/06/02/bosnia-swamped-with-hundreds-of-fake-bomb-alerts

these threats reached 110 educational facilities and approximately 18,000 students.[5] Over the same period, the Ministry of Civil Affairs of BiH (as part of the BiH Council of Ministers)[6], a state-level coordination body in the education sector was disabled for two weeks due to a massive cyber-attack on its IT infrastructure.[7]

Analysis

This policy paper aims to address the importance of building a legal framework and enhancing the technical capacities of education systems in the cyber security domain, as to prevent, mitigate and address the ongoing and future cyber security-related threats and challenges.

Building on the main hypothesis that the lack of cyber security policy regulations and practices in the education sector in BiH makes education systems vulnerable to cyber security threats and challenges, this document provides a set of recommendations for relevant education authorities aimed at enhancing cyber-security policies and practices in education systems in BiH.

The main findings were collected through desk research of the existing education- and cyber security-related policy documents and assessments, studies and standard-setting documents. Additionally, interviews with relevant cyber security experts from BiH were conducted to complement the desk research and generate evidence-based and actionable recommendations.

Complex education sector structure

The education sector in Bosnia and Herzegovina is highly decentralized. According to the constitutional order of Bosnia and Herzegovina, education is under the full jurisdiction of the entity Republika Srpska, ten cantons in the Federation of Bosnia and Herzegovina entity and Brčko District of Bosnia and Herzegovina. Each of these 12 administrative units has its own Ministry of Education, education legislation and budgets, as well as creates and implements its own education policies and adopts curricula, standards and norms. Moreover, they assumeall other rights and obligations arising from their full responsibility for the organization and the functioning of the education system in their territory.[8] Furthermore, based on the data from the BiH Agency for Statistics, in Bosnia and Herzegovina in the 2021/2022 school year, almost 482,000 students attended education from pre-primary to tertiary level.[9]

Highly decentralized cyber security system

It is noteworthy to mention that the cyber security ecosystem in Bosnia and Herzegovina **is decentralized due to BiH's** complex politico-administrative settings.

[5] *Wednesday's 110 bomb threats in Sarajevo Canton are treated as terrorism*,(2022, May 25), N1 Sarajevo, available at: https://n1info.ba/english/news/wednesdays-110-bomb-threats-in-sarajevo-canton-are-treated-as-terrorism/

[6] BiH Council of Ministers is the state-level executive body in Bosnia and Herzegovina

[7] *Hina: Bosnia's state IT systems disabled for two weeks now due to cyber-attack,* (2022, September 23), N1 Sarajevo, available at: https://n1info.ba/english/news/hina-bosnias-state-it-systems-disabled-for-two-weeks-now-due-to-cyber-attack/

[8] Ministry of Civil Affairs BiH and United Nations in BiH, *Report on the Consultations: Transforming Education at all Levels of Government in Bosnia and Herzegovina (TES Report)*, September 2022, p.6.

[9] Agency for Statistics BiH, *Education Statistics 2021/2022*, available at: https://bhas.gov.ba/Calendar/Category/15

The cyber security policy framework in Bosnia and Herzegovina is still under development. In 2022, Bosnia and Herzegovina was the only country in the Western Balkans region without a state-level cyber security strategy and operational CERT and CIRT at national level.[10] Despite the adoption of the Decision on establishing the state level CERT[11], the development of this institutional body has been in a deadlock since 2017, However, some progress has been achieved recently. In 2023, the Council of Ministers of BiH, approved Rulebook on the Internal Organization ofthe Ministry of Security of BiH,enabling the measures and actions to be taken for formation and full operationalization of the CERT for state level institutions.[12] In the Federation of BiH entity, steps have also been made towards establishing a FBiH level CERT.[13] However, at the moment of writing this paper, Republika Srpska entity is the sole administrative unit in BiH with a cyber security policy framework adopted[14] and relevant entity level CERT established. Moreover, the Ministry of Defence BiH has adopted the Cyber Security Strategy of the Ministry of Defence and Armed Forces of BiH and established its own CSIRT. The latter is responsible for protection of defence-related infrastructure, thus not relevant for the cyber security protection of the education sector.

Based on ITU's Digital Development Country Profile (2021), there are several relevant actors regarding digital policy in Bosnia and Herzegovina. "The Ministry of Civil Affairs and the Ministry of Communications and Transport are responsible for international representation of the country and international cooperation related to education, science and technology, which also incorporates ICTs. The mandate for developing policy related to digital agenda, including operational jurisdiction, breaks down at the entity level on FBiH and RS. For FBiH, the task falls to the Ministry of Transport and Communications, the Federal Ministry of Education and Science and in some limited way on the Ministry of Development, Entrepreneurship, and Craft. Additionally, there are also ministries coordinating science and technology in all 10 cantons across the FBiH. As for the Republika Srpska entity, the Ministry of Scientific and Technological Development, Higher Education and Information Society plays a crucial role in policymaking decisions. When it comes to infrastructure development, at the state level, the Ministry of Communications and Transport holds a policy-maker role, including national policy, strategic documents and legislation. Finally, the Ministry of Security leads the cybersecurity agenda."[15]

[10] DCAF, *Cyber Security and Human Rights in the Western Balkans: Mapping Governance and Actors*, 2022, p.35.

[11] BiH Council of Ministers, *The Decision on the Appointment of CERT for Institutions of BiH*, Official Gazette, 2017, available at: http://www.sluzbenilist.ba/page/akt/g4E0HNrVpsc=

[12]Council of Ministers BiH, *Statement on the Council of Ministers Session*, (2023, May 11), available at: https://www.vijeceministara.gov.ba/saopstenja/sjednice/saopstenja_sa_sjednica/default.aspx?id=40379&langTag=hr-HR

[13] FBiH Government, *The Decision on the Appointment of CERT for Institutions of FBiH* , 2022, available at: https://fbihvlada.gov.ba/bosanski/zakoni/2018/rjesenja/4.html

[14] Law on Information Security (2011); Regulation on Information Security Measures (2012); Rulebook on Information Security Standards (2012); Other relevant legislation: Law on Electronic Signature (2008) Law on Electronic Document (2008) Law on Electronic Management (2009), p.10.; available at: https://www.dcaf.ch/sites/default/files/publications/documents/NationalCybersecurityStrategiesWB_2021.pdf Strategy for Countering Cyber Security Criminal 2019-2023 (2019), available at: https://www.narodnaskupstinars.net/?q=en/node/17688

[15] ITU, *Bosnia and Herzegovina: Digital Development Country Profile*, 2021, p. 9-10, available at: https://www.itu.int/en/ITU-D/Regional-

Accelerated digital transformation of education in BiH

In recent years, education systems in BiH have undergone through a digital transformation. The unprecedented shift to digital learning during COVID-19 has prompted education systems in BiH to start investing in digital infrastructure[16]. The benefits of digital learning are numerous, from broadening the scope of open educational resources for students and educators, to improving access to education for vulnerable and students with disabilities to providing platforms for collaborative and research work.

According to the findings of the Analysis of the existing ICT infrastructure elements for primary, secondary and higher education in the administrative units of Bosnia and Herzegovina, conducted in 2021, the vast majority of educational institutions have official communication channels. Specifically, 97% of higher education institutions, compared to 70% of secondary and primary schools have an official website. Furthermore, almost all institutions from primary to higher education level have an official e-mail address (97% of higher education institutions, 92% of secondary schools, and 97% of primary schools, respectively). In the previous years, more than one-third of higher education institutions, as well as approximately half of secondary and primary schools established some sort of learning management systems/platforms to allow for online and blended learning delivery (ICT: 2021, p.44)

As digital tools proved to be an effective tool for advancing educational and school management, information management systems in education (EMIS) are established in 31% of higher education institutions, 75% of secondary schools and 77% of primary schools. These systems are designed to enable more efficient data collection, and real-time monitoring of the education process, as well as to support strategic and informed budget planning and investing (ibid, p. 56)

However, the increasing use of digital tools exposes the education sector to a wide array of cyber threats and challenges, such as data breaches, cyber-attacks on school infrastructure and networks and a variety of cybercrime actions.

According to the recent Microsoft Intelligence findings, education is the most targeted sector by cyber incidents and attacks. The most common cyber incidents include Denial of Service (DoS) attacks, phishing, ransomware attacks, malware installation and zoombombing.[17] Evidence gathered in Cyber Security Threat Assessment in BiH pointed out that 9.2 million cyber security threats were registered in Bosnia and Herzegovina, between November and December 2022, illustrating the vulnerability of citizens, companies and institutions to cyber-attacks (CSEC: 2023, p.8) These could threaten key sectors, such as the rule of law, economy, energy, health or

Presence/Europe/Documents/Publications/2023/Digital%20Development%20Country%20Profile%20Bosnia%20and%20Herzegovina%20%5bfinal-%20March%202023%5d.pdf

[16] Examples of the recent investment projects in digitalization of education in BiH: a) purchase of laptops for schools in Sarajevo Canton: https://www.mo.ks.gov.ba/aktuelno/ministarstvo-za-odgoj-i-obrazovanje-izdvojilo-1254684-km-pocela-isporuka-900-novih; b) establishment of Information Management System in Una-Sana Canton: https://bosniaherzegovina.un.org/en/165282-digital-learning-%E2%80%93-look-future; c) digital transformation of education in West-Herzegovina Canton, Canton 10, Herzegovina-Neretva Canton, Posavina Canton: https://skole.sum.ba/udaljeno_ucenje/novosti/volaric:-sumit-lider-u-digitalizaciji-cijele-vertikale-obrazovanja

[17] *Microsoft Security Intelligence, Global Threat Activity*, available at: https://www.microsoft.com/en-us/wdsi/threats

education. However, for the time being, there is not an exhaustive analysis of the most common types of cyber security attacks on the education sector in BiH (ibid).

Lack of technical capacities and protective measures of education systems

Besides the scarcity and disharmony of the cyber security legal framework, education ministries, as well as educational institutions, mostly have rather weak technical capacities for the prevention of and reaction to the potential threats and challenges from cyberspace. Furthermore, educational institutions, as well as most of other governmental bodies are faced with a systematic shortage of IT/cyber security expert workforce, primarily due to the current business trends in the IT market, which provides more attractive conditions and benefits in the private sector. In addition, the ICT equipment in educational institutions in all administrative units, at all levels of education, is mostly maintained by employees of these institutions, i.e. designated IT teachers. Apart from employees of institutions, the equipment is to a lesser extent maintained by service technicians authorized by the educational institution (at the ministries of education level).[18]

The Analysis of the Existing ICT Infrastructure at all Education Levels in BiH (2021) found that ICT equipment is usually old and poorly maintained, and that operational systems and virus/malware protection software are not regularly updated. Furthermore, Analysis of Quality Delivery of Online and *Blended Learning in Primary and Secondary (and TVET) Schools during COVID-19 Pandemic* (2021*)* showed insufficient levels of digital skills of teachers, particularly at primary and secondary education levels. This directly implies that educational workers are not equipped with the necessary skills to identify and/or transfer the digital-related content to the students.

Who responds to a potential cyber-attack on the education systems in BiH?

As previously stated, cyber security policy framework is still very vague and critical infrastructure mostly exposed to cyber threats, due to a lack of technical infrastructure. According to the expert from the Cyber Security Excellence Centre (CSEC) in Sarajevo[19], education systems (both education ministries and educational institutions at all levels) are part of the governments' critical infrastructure. As most of the administrative units at different governance levels still do not have either legal (adequate policy framework) or operational capacities (CERTs and CSIRTs), currently there are no clear procedures and protocols for the response in a case of cyber-attacks to educational institutions. This was proved in 2022 when the cyber-attacks to the state-level bodies occurred, interrupting their work for two weeks and disabling their IT infrastructure.

In an ideal scenario, in addition to the CERTs established at the state-, entity- and Brčko District-level, each ministry of education should have an operational CSIRT in place to prevent and respond to the potential cyber-attacks and threats. In the case these teams are not established

[18] UNESCO-UNICEF in BiH, *Analysis of the existing ICT infrastructure elements for primary, secondary and higher education in the administrative units of Bosnia and Herzegovina*, 2021, p.19.

[19]Head of Cyber Security Excellence Centre in Sarajevo was identified as a key interview informant for this policy paper. More info about CSEC can be found at: https://www.csec.ba/

within the organizational structures, ministries of education can outsource these services to competent private IT companies or seek technical expert assistance from prominent cyber security entities. For example, in 2022, a group of academics and experts established the Cyber Security Excellence Centre in Sarajevo. Acting as an "academic CERT" this organization's objective is capacity development of diverse partners as well as providing consultancy and support for preparing and addressing cyber security threats. Its ultimate mission is to raise awareness of the importance of cyber security in the country. For instance, in the absence of the relevant CERTs and CSIRTs, education authorities could establish a formal cooperation with CSEC in order to benefit from the expert technical assistance in analysis, prevention or mitigation of cyber security attacks to the education systems. Moreover, in the case of a cyber-attack, CSEC could propose timely and efficient measures to be undertaken to mitigate its effects.

Finally, education authorities, as well as relevant government bodies could leverage the expertise and existing professional networks of a range of experts to enhance their legal and operational capacities in the cyber security domain to keep pace with the emerging and dynamic cyber security developments.

Conclusion

The digital transformation of education in BiH has been significant. The process included the integration of technology in classrooms and development/use of online learning platforms. However, the education systems in BiH are not well prepared to tackle the potential risks and threats from cyberspace. The lack of cyber security policy regulations and practices in the education sector has made education systems vulnerable to cyber security threats and challenges. BiH education systems lack the necessary technical expertise and infrastructure to detect and respond to cyber security threats.

The authorities at all relevant governance levels should prioritize the development and implementation of a comprehensive legislative framework to address the lack of preparedness and vulnerability of education systems to cyber security threats.

Apart from the Republika Srpska entity, there are currently no operational entities or responsible bodies in charge of responding to and mitigating the effects of cyber-attacks/breaches in the education systems in BiH. This lack of established entities increases the vulnerability of education systems in BiH to cyber security threats and challenges. Therefore, there is an urgent need to elaborate a comprehensive cyber security policy framework, as well as to establish entities that will be responsible for responding to and mitigating the effects of cyber-attacks/breaches in the education systems in BiH (as part of the critical government infrastructure).

Recommendations

Introduce a comprehensive legislative framework:

The relevant government authorities in BiH need to develop a comprehensive legislative framework that identifies procedures and responsible entities to provide an emergency response to cyber security attacks/threats on education systems. The framework should address the lack of preparedness and vulnerability of education systems to cyber security threats and challenges.

Establish entities responsible for responding to cyber security threats:

There is an urgent need to establish entities that will be responsible for the prevention of and response to cyber threats in the education sector. The establishment of relevant CERTs and CSIRTs should take into consideration the protection of education systems, as part of the critical infrastructure.

Full implementation of ICT standards in the education sector, with emphasis on ICT maintenance and security provisions:

In 2021, all education authorities in BiH jointly adopted the document *Basic Technical Standards for Tools of Information and Communication Technologies at all Education Levels in BIH* with the objective to establish minimum technical specifications for ICT for educational purposes. This standard-setting document also defines basic requirements regarding the safety and security of digital infrastructure as well as the protection of software used in educational institutions. In this regard, relevant education authorities should invest maximum efforts for the full implementation of this document, particularly of provisions related to the maintenance and security of ICT at all education levels.

Development of protocols for cyber security in educational institutions:

The development of protocols for cyber security in educational institutions is crucial for enhancing cyber security in the education sector in BiH. The protocol should include an incident response plan, security awareness training, access control policies, regular vulnerability assessments, data protection policies, and monitoring and reporting procedures. These protocols should be regularly reviewed and updated to ensure that they remain effective against evolving cyber security threats. For example, in 2022, the United Kingdom Department for Education issued the *Cyber Security Standards for Schools and Colleges*[20] document outlining the guiding principles in ensuring a safe cyber security ecosystem in the education sector. This covers provisions related to technical ICT standards to monitoring and reporting procedures in the event of a cyber security attack.

Increasing budgets for IT infrastructure and strengthening technical resources of education ministries and educational institutions:

Increasing budgets for IT infrastructure and strengthening technical resources of education ministries and educational institutions are essential steps for enhancing cyber security in the education sector in Bosnia and Herzegovina. Educational institutions in BiH should increase investment in cyber security resources such as antivirus software, firewalls, and intrusion detection systems. These resources will help protect the IT infrastructure from cyber threats. Moreover, a highly skilled technical workforce should complement the quality and secure digital

[20] UK Government-Department of Education, *Meeting Digital and Technology Standards in Schools and Colleges*, 2022, available at: https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-standards-for-schools-and-colleges

infrastructure. Thus, relevant education authorities should work on attracting IT specialists to the public sector by providing competitive professional benefits.

Consider outsourcing IT services through enhanced public-private partnerships:

The interview conducted with the Head of the Cyber Security Excellence Center (CSEC) in Sarajevo pointed out that the first step in building a cyber security structure in the education sector in BiH is the establishment of relevant CERTs, in accordance toas per the administrative organization of BiH. As the role of the CERTs is cyber security coordination and capacity-building of the critical infrastructure, which entails a large number of government institutions, bodies and agencies, including education institutions, the establishment of CERTs may not be sufficient to ensure the full-scale protection of the education sector. In that regard, educational institutions may consider outsourcing cyber-security-related services to experienced and reputable third-party providers. More precisely, third-party contractors can exercise the role of a cyber incident response team (CIRT) and provide immediate actions in the case of cyber security-attack occurrence.

Continuous capacity building of educational workers and students in cyber security hygiene:

It is essential to provide regular training programmes for IT technical staff, teachers and students to equip them with up-to-date knowledge of the latest cyber security threats and to empower them with the skills and knowledge to safeguard themselves and their institution against cyber threats. These trainings should cover topics such as password management, email security, safe internet use, cybercrime and cyberbullying, etc.

Involvement of academia in the process of cyber security policy framework and practices development:

Academia possesses relevant knowledge and expertise in the domain of cyber security as well as an overview of the needs and capacities of educational infrastructure, students and educational workers' needs and skills. The involvement of academia is particularly important in the development of cyber security educational curricula for students and teachers

Strengthen collaboration and sharing of best practices:

Educational institutions should collaborate and share best practices in cyber security to learn from each other's experiences and prevent cyber threats. Educational institutions can create a platform for sharing information and experiences, and promote collaboration between institutions and industry stakeholders. A good example can be found in Montenegro, where within the TEMPUS program, a consortium of higher education institutions and organizations from Slovenia, Great Britain, Italy and Montenegro, led by the University of Maribor in the period 2013-2016, implemented the project Enhancement of Cyber Educational System of Montenegro (ECESM). The main goal of the project was to improve, develop and implement standards, guidelines and procedures in the area of cyber security at the national level in Montenegro, to allow creation of a skilled and professional workforce able to respond to the dynamic cyber threats.[21]

[21] OSCE, *Guide Through Information Security in the Republic of Serbia*, p.52., available at: https://www.osce.org/files/f/documents/2/7/272171.pdf

Bibliography

Agency for Statistics BiH *Education Statistics 2021/2022* (2022), available at: https://bhas.gov.ba/Calendar/Category/15

Baraković, Sabina and Baraković-Husić Jasmina *We Have Problems for Solutions”: The State of Cybersecurity in Bosnia and Herzegovina* (2015), available at: http://connections-qj.org/article/we-have-problems-solutions-state-cybersecurity-bosnia-and-herzegovina

Cyber Security Excellence Centre-CSEC *Cyber Security Threat Assessment Bosnia and Herzegovina* (2023), available at: https://www.csec.ba/_files/ugd/7e0f63_6fb033e4bbce48e3b7bd9ddf310cf75e.pdf?index=true

CSO Online.com, *Top Cybersecurity Threats Active in the Education Sector Today – and Why You Should Care,* (2018), available at: https://www.csoonline.com/article/3250862/top-cybersecurity-exploits-active-in-the-education-sector-today-and-why-you-should-care.html

DCAF, *Cyber Security and Human Rights in the Western Balkans: Mapping Governance and Actors* (2022), available at: https://www.dcaf.ch/sites/default/files/publications/documents/NationalCybersecurityStrategiesWB_2021.pdf

ENISA, *Cyber Security Education Initiatives in the EU Member States* (2022), available at: https://www.enisa.europa.eu/publications/cybersecurity-education-initiatives-in-the-eu-member-states

ENISA *Threat Landscape 2022*(2022), available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Eyewitness News, *Bosnia Swamped with Hundreds of Fake Bomb Alerts,* (2022), available at: https://ewn.co.za/2022/06/02/bosnia-swamped-with-hundreds-of-fake-bomb-alerts

ITU, *Bosnia and Herzegovina: Digital Development Country Profile* (2021), available at: https://rb.gy/bc1hd

Ministry of Civil Affairs BiH and United Nations in BiH *Report on the Consultations: Transforming Education at all Levels of Government in Bosnia and Herzegovina (TES Report)*, (2022)

N1 Sarajevo, *Wednesday’s 110 bomb threats in Sarajevo Canton are treated as terrorism* (2022), available at: https://n1info.ba/english/news/wednesdays-110-bomb-threats-in-sarajevo-canton-are-treated-as-terrorism/

N1 Sarajevo, *Hina: Bosnia’s state IT systems disabled for two weeks now due to cyber-attack* (2022), available at: https://n1info.ba/english/news/hina-bosnias-state-it-systems-disabled-for-two-weeks-now-due-to-cyber-attack/

OSCE, *Guide through Information Security in the Republic of Serbia*, Belgrade, available at: https://www.osce.org/files/f/documents/2/7/272171.pdf

UNESCO-UNICEF in BiH,, *Analysis of the existing ICT infrastructure elements for primary, secondary and higher education in the administrative units of Bosnia and Herzegovina* (2021)

UNESCO-UNICEF, Ministry of Civil Affairs BiH, *Basic Technical Standards for Tools of Information and Communication Technologies for Education Systems in BiH* (2021)