Review scientific paper
UDK:373:316.6
DOI:10.7251/ZND2601152G

SECURITY IN EDUCATIONAL INSTITUTIONS - CHALLENGES AND OPPORTUNITIES

***Dr.sc. Mirko Goreta, senior lecturer*[38]**
Marko Marulić Polytechnic in Knin

Abstract: *Educational institutions' security involves protecting the physical environment of schools or other places where students learn, ensuring that students have psychological well-being while they attend school, providing digital safety and protecting organizations through efficient management. Institutions must also be able to identify and respond appropriately to various risks and challenges they may face. Modern-day issues to educational security include violence by peers, inadequately established mechanisms within educational institutions to protect students, staff, and property and the emergence of digital risks such as cyber-attacks, all of which make developing a secure framework for education even more complicated. Successful educational security will not come from just having a written policy or procedure but also implementing the best management principles available in how to provide a safe learning environment. Successful educational security depends upon the administration, employees, students, parents and community members establishing a "safety culture" through providing both awareness and responsibility for their actions. While technology provides additional options for improving safety, educational institutions are required to utilize technological to support their policies and procedures while following the legal and ethical requirements of protecting individuals' privacy. Therefore, developing an integrated approach that provides a connection between organizational and technological recommendations, along with education will create an environment that is safe, secure, stable, and conducive to learning. An integrated approach will provide a reduction of risk and potential threats and contribute to the quality of education for all who participate in them.*

Keywords: *safety in education, school safety, digital safety, risk management, technological solutions*

Introduction

In recent years the issue of security has become one of the greatest concerns for educational institutions as places of education and learning as well as social interaction amongst students, faculty, and administrative staff members of a community. The many potential hazards posed by the complexity of these institutions their size, scope, and structure abound; these include violence against persons, bullying behavior or assault, intimidation using social media, and other technology-based threats such as identity theft or cyber abuse. Because today's security landscape is evolving and requires a more systematic approach to security throughout the educational setting, which involves several areas of protection, there are significant differences in how schools have previously defined and approached the issues of protection and safety in their buildings. In many cases, security measures in the past focused primarily on building security and controlling access to buildings. With the advancement of technology and the increase in social complexity within the school through the use of technology, new types of threats to student safety are now surfacing and will continue to increase in number as long as students are sharing information with each other through text messaging, emailing,

[38] mirko.goreta@veleknin.hr

using social networks, and other digital forms of communication through their devices. In addition, there is evidence that cyberbullying is a contributing factor in decreased academic achievement, psychological stress, and/or emotional distress experienced by students, based on research conducted by Kowalski, Limber, and Agatston (2012). All these factors point to the need for a much broader, comprehensive definition of security than has previously existed. Schools and universities don't just have to fend off threats to their digital systems but also deal with issues that stem from the way they are run and managed. Schools and universities will have a harder time responding to a crisis if they have poorly defined security protocols and limited cooperation with the proper authorities. Research done by Cornell and Mayer has shown that the relationship between schools' effective security systems, on the one hand, and schools' effective technical measures on the other, is highly dependent on schools' management and their security procedures, which lead to timely detection and resolution of potential threats to the school (Cornell & Mayer, 2010). This research argues for a management approach to security in educational institutions, in which management processes and preventive mechanisms are integrated into the overall security system of an institution. An important dimension of security in educational institutions is the psychological condition of students and their feelings of safety, acceptance, and protection, which directly impacts their academic success and social development. Feelings of insecurity can create a situation in which an individual pulls away from others, becomes less involved in the classroom, and negatively affects their long-term mental well-being. Research has shown that the perceived safety of students and staff in an educational institution is often as important as the actual level of protection, and that both factors influence the behavior of individuals and the overall climate of an educational institution (Astor, Benbenishty, & Estrada, 2009).

Dimensions of security in educational institutions

In schools, safety is a complicated and complex phenomenon. There are many ways to provide safety for the students, teachers, and everyone else who works in or visits a school. Unlike many people believe, safety does not only involve providing physical security to the school but it also includes the psychological, digital, and organizational aspects of safety. Current approaches point out that safety is a dynamic process that must continually change in response to changes that occur in society and through technological advancements. According to the study by Cornell and Mayer (2004), when talking about safety in schools, the absence of violence is generally one of the most common definitions, however, in order for an educational institution to be considered a safe place for learning, there must also be a stable and supportive environment that allows the student to be able to learn productively (Cornell & Mayer, 2004). The first and most obvious dimension of safety in schools is physical safety. Physical safety refers to the protection of school property, the regulation of who can enter the premises of the school, and the prevention of physical violence occurring in an educational institution. Some of the physical safety measures that can be put into place to protect the health and wellbeing of students within a school's environment are: maintaining video surveillance on the campus, having staff present to ensure the safety of the students on the campus, providing access control systems at the entrances and exits to the school and having clearly defined evacuation plans to be implemented in case of an emergency (Addington, 2009). In addition to the use of physical safety measures to provide for the safety of students, research has shown that when physical safety is combined with other components of an overall security system, and proper procedures are followed, the number of incidents of violence and other events that would negatively affect the wellbeing of a student attending the school can be reduced (Addington, 2009). Another dimension of importance here is that of psychological safety, which refers to a perceived sense of safety, belonging, and acceptance in the educational community. From a psychological perspective, those who feel vulnerable, alone, or

are victims of violence, will suffer lower levels of academic performance and will experience higher than average levels of distress. Psychological safety can become especially compromised in situations involving victimization by peers. Research done by Astor et al. demonstrates a direct link between how safe a student perceives himself or herself to be and that student's behavior, classroom engagement level, and overall climate of the school (last quoted by Astor, Benbenishty, & Estrada 2009). Looking at this dimension supports the idea that safety not only has to do with measures of safety in terms of objective nature of safety but also the subjective experience of an individual. The third dimension of security is the growing emphasis put on digital security relative to the increasing use of information technology systems in education. Digital platforms and resources for learning, online forms of instruction, and use of social media have created both new avenues for learning, as well as new potential for exposing students to risk. Cyberbullying, identity fraud, unauthorized access to a student's personal information, and misuse of digital tools all represent major threats to making sure that students are protected. Livingstone et al. (2011) conducted research showing that youth are not always able to appreciate the risks associated with their use of digital devices or digital technologies and thus are especially vulnerable groups of youth. To keep data safe, digital security needs both technology-based solutions and education/awareness for users. Another dimension is organizational security, which describes how a school or department plans for, manages and implements effective security measures in schools. Some examples of organizational security include having clearly defined guidelines to follow, established safety protocols, crisis-response plans, and identifying the roles/responsibilities of employees when a crisis occurs. The way that the organization is set up directly relates to how well the overall security systems operate. According to Trump (2011), schools with well-defined guidelines and continuous training for employees to prepare them to respond to and manage a crisis, will have a much greater chance of successfully preventing and/or managing a crisis, than those without this support. To summarize, security in K-12 educational institutions must be inter-dependent and integrated, where a safety measure is lacking, then the opposite should also apply. Similarly, organizations will not fully utilize the effectiveness of digital security unless there is an adequate organization structure to support the implementation of that security. Newer concepts of modern security models necessitate a holistic approach, whereby multiple aspects are combined into one model/system that provides for thoughtful consideration regarding how a crisis will be addressed as well as establishing a safe and supportive environment to minimize the need for police intervention.

Contemporary security challenges

The security problems that modern educational institutions face are many and varied due to changes in society, advancements in technology, and the complicated nature of school interactions. Because many of these security problems are interconnected and often occur simultaneously, it can be very difficult to pinpoint and address them. To effectively develop strategies to address these threats, it is imperative to identify the specific threats one is trying to identify. One of the most obvious security threats faced in schools is rival violence, which, unlike previous generations, now often involves some form of digital harassment. In other words, bullying and harassment in the physical world, which would have traditionally consisted of physical and/or sexual violence or verbal abuse, now also occur in the online realm, where the spread of that content can occur quickly and permanently. According to research by Olweus, students who have been exposed to long-term rival violence are at a higher risk of developing anxiety, depression, and lower academic performance than students who have not been exposed to such violence (Olweus, 2013). The added dimension of a digital component has the potential to compound these effects since victims of peer violence often do not have a means to separate

themselves from the source of the threat. The second security challenge faced by educational institutions is that of unauthorized entry and the potential for physical incidents. While events like these are less common than other kinds of threats, they can be extremely severe, particularly when there are issues with entrance controls, insufficient personnel to provide security, and inadequate policies and procedures. According to the National Center for Education Statistics (NCES, USA), schools without well-defined security protocols report more incidents of unauthorized entry and disorderly conduct than those with established protocols (National Center for Education Statistics, 2019). Thus, these data support the importance of a systematic approach to physical security. Digital threats are becoming more prevalent in schools because of the rapidly expanding virtual environment that includes digital platforms, electronic portfolios, and distance learning systems. Therefore, the introduction of these technologies presents opportunities for a broad range of cyber threats, such as identity theft, unauthorized access to educational institutions' computer systems and abuse of student and teacher digital identities. ENISA (European Union Agency for Cybersecurity) reports that education is an increasingly popular target for cybercriminals due to underdeveloped cybersecurity programs and limited resources for protection (ENISA, 2021). Consequently, this underscores the critical need for enhancement of cybersecurity within educational institutions. The most significant barrier to strengthening security in educational institutions is a lack of resources and institutional support to facilitate the implementation of security measures. Many educational establishments operate on restricted budgets, which restricts their ability to invest in security infrastructure and safety staff training, as well as developing prevention programs (Fisher & Hennessy, 2016). Schools with limited resources usually find they are behind other schools when adopting modern security solutions and are, therefore, more prone to threats of many kinds (Fisher & Hennessy, 2016). This indicates that there are disparities across different education settings when it comes to the level of security provided. Compounding the problem is limited coordination between education settings and external entities, such as law enforcement, social services, and community resources. Effective security management requires cooperation from multiple systems, particularly during emergencies or when a serious threat or violent act occurs. In practice, however, there is often poor communication, an unclear delineation of roles and slow response times. Research supports the finding that schools that collaborate with law enforcement and other security agencies are better able to identify and prevent violent acts (Borum, Cornell & Modzeleski, 2010). Recent security-related events illustrate that security is not a fixed characteristic but rather a dynamic process of ongoing social and technological change. Peer bullying, digital threats, safety hazards and operational shortcomings combine to make security exceedingly complex in today's educational environment.

The role of management and institutions in ensuring safety

The ability to effectively manage security in educational institutions relies heavily on the collaboration of management and institutional frameworks. Management is accountable for developing, coordinating and carrying out security measures; therefore, security should not be a product of individual initiatives, but rather a collective effort through the use of a systemic approach that involves well-defined policies, procedures and responsibilities for all parties; thus, management provides an essential service by developing a security strategy while creating a culture where individuals are aware of and manage risks. Management must first develop and implement security policies. Security policies are comprised of conduct standards, crisis response procedures and mechanisms for incident reporting. All members of the educational community must have access to security policies that clearly define the rules of behavior. Previous studies by Smith and Smith have shown that institutions with clearly defined security systems are able to record fewer incidents and provide faster responses during

times of crisis (Smith & Smith, 2018). This demonstrates that implementing formalized security protocols directly impacts the overall efficiency of the security system. In addition to developing security policies, an additional role of management is crisis management organization. Different types of emergencies are to be dealt with in educational institutions including violent incidents and technical system failures or digital attacks. Crisis plans must include pre-established steps, accountability for decision-making, and effective or rapid communication channels (Perry & Lindell, 2003). Research by Perry and Lindell shows that when an organization creates a detailed crisis management plan that is followed by the conduct of regular drills or simulations, that organization is likely to demonstrate a greater degree of coordination and reduced impact from subsequent real incidents (Perry & Lindell, 2003). Thus, when considering educational institutions, preparedness has a direct effect on protecting student and employee lives and safety. Additionally, employers have a responsibility to ensure that their employees receive the necessary training regarding potential threats. As teachers and administrative staff are often the first individuals to recognize a potential threat, training must also be provided if those employees are to appropriately respond to that threat. The educational training provided to employees may include recognizing risk behaviors, how to respond to a crisis, and safety technologies. Research conducted by Allen & White supports that ongoing training of employees increases an employee's ability to promptly identify and report a security threat. The above statement further illustrates that security is dependent not only on the number of security systems in place, but also on the employees' competence in using those systems. Another important component of security management is collaborating with outside agencies. Educational institutions do not function independently from their local social network; they are part of a larger social network that includes police, hospitals and healthcare facilities, social services and community. Being able to effectively communicate and coordinate their activities with these stakeholders allows for a quicker response to serious threats to safety and provides additional resources for preventing violence or other crime-related issues. According to Mayer and Leone (1999), schools that establish partnerships with local law enforcement agencies are better equipped to handle crisis situations and to reduce incidents of violence. Another important aspect of establishing an environment that promotes the safety of students is through management's role in developing a safety culture within the organization. The establishment of safety culture involves the establishment of shared values, attitudes, and behaviors, which support a safe environment. When the administration of the school system actively promotes safety as an important priority, it is more likely that staff members and students will accept their individual responsibilities for their behavior. Research has shown that organizations with an established security culture have fewer incidents of reported crime and a higher level of preparedness to respond to crime-related problems (Reason, 2000). Ultimately, the role of management and organizations in providing safe environments is based on their ability to coordinate and integrate multiple aspects of the overall security system into a single cohesive unit. These include policy development, crisis management, training of employees, cooperation with external agencies, and the establishment of a safety culture. A lack of active and responsible involvement in and by management at educational institutions results in an ineffective and poorly managed educational system.

Technological solutions and digital security

The incorporation of modern technology greatly remodeled the landscape of protection procedures used by educational institutions. Digital technologies permit quick identification of potential threats, enhanced management of controlled spaces and increased safety over the protection of school property. As such, digital tools function to improve the security of educational institutions while simultaneously acting as vulnerabilities should they not be appropriately deployed. Video monitoring

systems are one of the most prevalent digital tools utilized in educational institutions where schools can now continuously monitor video images of the exterior of their buildings, as well as the common hallways, corridors and even the areas surrounding the entrances to their buildings. The primary purpose of utilizing these systems is to deter unwanted behaviors and allow for rapid response to an incident. Research conducted by Welsh and Farrington suggests that video surveillance systems may provide a moderate level of protection against reducing the amount of violence and vandalism within an educational environment (Welsh & Farrington, 2009). However, there should be clear procedures in place related to how video surveillance systems are operated and the procedures for responding to video surveillance footage. Another major digital tool for educational institutions is access control systems which provide digital access management via electronic cards, access tags and/or digital records of facility access. The use of these systems allows for restricted access to areas which would otherwise allow unauthorized individuals to enter. Garcia's study shows that access control systems are most successful in large educational institutions. In these places, there are many users, so it can be hard to monitor physical areas without using technology for help (Garcia, 2008). Access control systems improve monitoring capabilities but require ongoing management and maintenance. Digital security is now more critical than ever due to the increase in availability of online educational platforms and electronic teaching management. Educational centers are storing more sensitive data. This includes personal information of both students and staff, as well as academic and administrative records. All this data can be the target of a cyber-attack, which may have devastating consequences for the privacy and integrity of the institution. Von Solms and Van Niekerk indicate that the only way to effectively protect an organization's information is through the application of security policies, implementing technical controls, and providing users with ongoing training about security risks (Von Solms & Van Niekerk, 2013). This support demonstrates that digital security is not just a technical matter; it is also a matter of management on an organizational level. Threat detection systems represent an advanced technological method of protecting against threats. Threat detection systems use algorithms and data analysis to detect unusual behavior patterns in both physical and digital spaces. For instance, examples of unusual behaviors can be e.g. using an anomalous internet connection, attempting to gain unauthorized access or making abusive conduct through a communication medium where one can exhibit abusive behaviors. According to Bishop's research, systems that rely on behavioral indicators may provide an organization with enhanced early warning capabilities (Bishop, 2012). However, the use of these systems increases concerns related to privacy and ethical limitations that have accompanied some other forms of technology. An important consideration in the use of technology for security is balancing security and protecting an individual's right to privacy. The introduction of surveillance systems and data collection technology must abide by the applicable laws and regulations governing such technology and be consistent with ethical principles. The EU General Data Protection Regulation (GDPR) sets out fundamental principles that collectively set out to specifically regulate how individuals' personal data is processed. This regulation outlines clear requirements as to how personal information related to individuals is processed, including the requirements to be transparent, to have a legitimate purpose for processing personal information, and the requirements that only personal information necessary for that purpose is collected. Kuner (Kuner, 2017) found that without cooperation between information security systems, and existing data protection regulations, there will be a risk of significant legal penalties and loss of user trust due to non-compliance with privacy regulations. This demonstrates technological solutions need to be treated more equally with respect to their ability to provide members of an organization with efficient services and to protect an individual's rights. Ultimately, technological solutions are an essential component of modern education security systems. Their ability to provide greater protection is related to the extent that these systems are effectively integrated into an organization's operational processes and the

impact people have on those technologies. Access control, video surveillance, data protection, and threats detection technologies play a critical role in assisting with increasing security, but only if they are used.

Conclusion

Safety is a complex and changing process that requires an integrated approach, as well as continuous improvement in educational institutions. The research shows that security isn't just about protecting space and includes physical (security of the building), psychological (creating a environment that encourages students), digital (operational security), and organizational (operational procedures) aspects. Today's society and rapid technological advances have generated new types of threats, therefore traditional approaches to security management are not adequate anymore. Current challenges include violent peer interactions, cyber threats, and poor organizational processes, which require systems and proactive action. Problems arise due to multiple sources of interaction therefore, it is essential that a comprehensive approach is developed across multiple sectors of society. The role of the management and institution is critical; by creating well-defined policies, crisis response plans, and working with other relevant stakeholders, institutions will improve their security management systems. Technology provides numerous opportunities to improve security, but how well they work will depend on their use and integration with other systems. For instance, using video surveillance, access control, and protecting digital information all help reduce risk but do not replace the need for organizational processes and good management. It is necessary to maintain a balance between security and protecting an individual's right to privacy to maintain user trust and comply with legal standards. Ultimately, security in schools must be viewed as an ongoing effort that requires cooperation among all stakeholders, including administrators, teachers, students, parents, and the surrounding community. Creating a safe and secure educational environment can be achieved through a combination of preventive measures, technology, and the establishment of a positive safety culture. This type of approach reduces the chances of incidents occurring and helps promote better learning and the overall advancement of society.

Literature:

1. Addington, L.A. (2009). "COPS, cameras, and crisis: The potential and the problems with using surveillance technologies in schools". American Journal of Criminal Justice, 34(3–4), 479–492.
2. Allen, K. P., & White, S. (2018). "School safety and teacher training: The role of preparedness in crisis situations". Journal of School Safety, 12(1), 55–65.
3. Astor, R. A., Benbenishty, R., & Estrada, J. N. (2009). "School violence and theoretically atypical schools: The principal's centrality in orchestrating safe schools". American Educational Research Journal, 46(2), 423–461.
4. Bishop, M. (2012). Computer security: Art and science (pp. 142–145). Addison-Wesley, Boston.
5. Borum, R., Cornell, D., & Modzeleski, W. (2010). "What can be done about school shootings? A review of the evidence". Educational Researcher, 39(1), 27–37.
6. Cornell, D., & Mayer, M. (2010). "Why do school order and safety matter?". Educational Researcher, 39(1), 7–15.
7. ENISA. (2021). Cybersecurity in education: Challenges and opportunities (pp. 21–25). European Union Agency for Cybersecurity.
8. Fisher, B. S., & Hennessy, M. (2016). "School resource officers and school safety". Journal of School Violence, 15(2), 229–245.

9. Garcia, M. L. (2008). The design and evaluation of physical protection systems (pp. 203–207). Butterworth-Heinemann, Oxford.
10. Kowalski, R.M., Limber, S.P., & Agatston, P.W. (2012). Cyberbullying: Bullying in the digital age (2nd ed., pp. 64–68). Wiley-Blackwell, Malden, MA.
11. Kuner, C. (2017). Transborder data flows and data privacy law (pp. 65–69). Oxford University Press, Oxford.
12. Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (2011). Risks and safety on the Internet: The perspective of European children (pp. 102–105). EU Kids Online, London School of Economics.
13. Mayer, M.J., & Leone, P.E. (1999). "A structural analysis of school violence and disruption: Implications for creating safer schools". Education and Treatment of Children, 22(3), 333–356.
14. National Center for Education Statistics. (2019). Indicators of school crime and safety (pp. 12–15). LOUSE. Department of Education.
15. Olweus, D. (2013). School bullying: Development and some important challenges (pp. 45–49). Annual Review of Clinical Psychology.
16. Perry, R.W., & Lindell, M.K. (2003). "Preparedness for emergency response: Guidelines for the emergency planning process". Disasters, 27(4), 336–350.
17. Reason, J. (2000). "Human error: Models and management". BMJ, 320(7237), 768–770.
18. Smith, R., & Smith, M. (2018). School security and safety management (pp. 112–115). Routledge, London.
19. Trump, K. S. (2011). Proactive school security and emergency preparedness planning (pp. 27–30). Corwin Press, Thousand Oaks, CA.
20. Von Solms, R., & Van Niekerk, J. (2013). "From information security to cyber security". Computers & Security, 38, 97–102.
21. Welsh, B.C., & Farrington, D.P. (2009). "Public area CCTV and crime prevention: An updated systematic review and meta-analysis". Justice Quarterly, 26(4), 716–745.

SIGURNOST U OBRAZOVNIM USTANOVAMA - IZAZOVI I PRILIKE

Dr.sc. Mirko Goreta, viši predavač
Veleučilište Marko Marulić u Kninu

***Sažetak**: Sigurnost obrazovnih ustanova uključuje zaštitu fizičkog okruženja škola ili drugih mjesta gdje učenici uče, osiguravanje psihičke dobrobiti učenika dok pohađaju školu, pružanje digitalne sigurnosti i zaštitu organizacija učinkovitim upravljanjem. Ustanove također moraju biti u stanju prepoznati i odgovarajuće reagirati na različite rizike i izazove s kojima se mogu suočiti. Suvremeni problemi obrazovne sigurnosti uključuju nasilje vršnjaka, nedovoljno uspostavljene mehanizme unutar obrazovnih ustanova za zaštitu učenika, osoblja i imovine te pojavu digitalnih rizika poput kibernetičkih napada, što sve dodatno komplicira razvoj sigurnog okvira za obrazovanje. Uspješna obrazovna sigurnost neće proizaći samo iz pisane politike ili postupka, već i iz primjene najboljih dostupnih načela upravljanja u osiguravanju sigurnog okruženja za učenje. Uspješna obrazovna sigurnost ovisi o upravi, zaposlenicima, učenicima, roditeljima i članovima zajednice koji uspostavljaju "kulturu sigurnosti" pružanjem svijesti i odgovornosti za svoje postupke. Iako tehnologija pruža dodatne mogućnosti za poboljšanje sigurnosti, obrazovne institucije moraju koristiti tehnologiju za podršku svojim politikama i postupcima, uz poštivanje zakonskih i etičkih zahtjeva zaštite privatnosti pojedinaca. Stoga će razvoj integriranog pristupa koji pruža vezu između organizacijskih i tehnoloških preporuka, zajedno s obrazovanjem, stvoriti okruženje koje je sigurno, stabilno i pogodno za učenje. Integrirani pristup osigurat će smanjenje rizika i potencijalnih prijetnji te doprinijeti kvaliteti obrazovanja za sve koji u njemu sudjeluju.*

***Ključne riječi:** sigurnost u obrazovanju, sigurnost u školama, digitalna sigurnost, upravljanje rizicima, tehnološka rješenja*