Chapter 4
Importance of Cybersecurity Education to Reduce Risks in Academic Institutions

Javier Guaña-Moya, Nelson Salgado-Reyes, Yamileth Arteaga-Alcívar, and Alejandra Espinosa-Cevallos

Abstract Technology has become a fundamental part of current educational processes, which is why many academic institutions have adopted technological tools in order to improve teaching and learning practices. However, as digital dependence increases in the educational field, it becomes increasingly necessary to guarantee that the systems adopted are secure and protected against cyber threats, considering that academic institutions store a high amount of confidential information, from personal data of students to cutting-edge research, especially at higher levels. For this reason, it is vital that these institutions promote continuous education and training in cybersecurity, both for staff, students, and other members of the educational community. That is why this bibliographic review was developed with the objective of establishing the importance of cybersecurity education for the reduction and control of risks associated with computer attacks within academic institutions, considering the main risks they face, as well as the possible strategies that can be applied to avoid them.

J. Guaña-Moya · N. Salgado-Reyes (✉)
Pontificia Universidad Católica del Ecuador, Quito, Ecuador
e-mail: nesalgado@puce.edu.ec

J. Guaña-Moya
e-mail: eguana953@puce.edu.ec

Y. Arteaga-Alcívar
Instituto Tecnológico Universitario Internacional, Quito, Ecuador
e-mail: yamileth.arteaga@iti.edu.ec

A. Espinosa-Cevallos
Instituto Tecnológico Universitario Cordillera, Quito, Ecuador
e-mail: paola.espinosa@cordillera.edu.ec

J. Choudrie et al. (eds.), *ICT for Intelligent Systems*, Smart Innovation, Systems and Technologies 403, https://doi.org/10.1007/978-981-97-5799-2_4

4.1 Introduction

In today's digital age, cybersecurity has become an issue of fundamental importance for all organizations, which includes educational institutions, considering that the constant technological advancement and dependence on IT systems in academic institutions at all levels have made them attractive targets for cyber criminals, finding that these cyber-attacks can have devastating consequences and put at high risk the integrity of students' personal and academic data, as well as the institution's, which affects the proper development of educational processes [1].

All academic institutions store a large amount of confidential information ranging from students' personal data to cutting-edge research in the case of higher education institutions. University information systems and networks are very often used by thousands of users, and if you add the wealth of data contained, the likelihood of suffering some kind of attack and security incident is very high, as hackers and cybercriminals try to access this information for illegal use, such as identity theft, extortion, or black-market sales [2].

It is essential for academic institutions to be clear about the risks associated with information theft and disclosure. One example of a successful attack is ransomware, which can encrypt important files and demand a ransom for their release, disrupting academic and administrative activities, affecting not only students and educators, but also the reputation of the institution and its ability to fulfill all educational responsibilities. Therefore, it is very important that institutions pay attention to cybersecurity and take preventive measures to protect critical systems and data [3].

For all of the above reasons, the present literature review was proposed with the aim of establishing the importance of cybersecurity education for the reduction and control of risks associated with cyber-attacks within academic institutions, considering the main risks they face, as well as the possible strategies that can be applied to avoid them.

4.2 Methodology

This research was developed in accordance with the systematic literature review structure proposed by Kitchenham [4], in order to obtain relevant information linked to the research questions proposed for the development of the research.

This methodological process establishes three stages:

- Planning the search.
- Conducting the search.
- Analysis and documentation of results.

4.2.1 Planning the Search

The primary objective of this study is to collect relevant data on cybersecurity and computer security with a focus on digital education, considering the growing increase of these risks within academic institutions, highlighting information from experts and leaders in the field about the present and future of cybersecurity and computer security.

To address this issue in a systematic way, the following research questions are proposed:

Q1: What are the main cybersecurity risks faced by academic institutions?
Q2: What are the benefits of cybersecurity education for academic institutions?
Q3: What are the strategies to reduce cybersecurity risks in academic institutions?

Digital databases such as IEEE eXplorer, Science Direct, ACM Digital Library, SCOPUS, Springer Link, and specialized web-based databases on topics associated with computer security, cybersecurity, trends in the area of digital security, and expectations of data security in educational institutions were used to obtain the most recent data, examining academic journals and technical publications as reliable sources of information, published between 2018 and 2023, to obtain the most recent data.

The search method focused on aspects addressed to the proposed research questions, using keywords such as “computer security”, “cybersecurity”, “information security”, “digital era”, “computer attacks”, “digital defense strategies”, always focused on the area of academic institutions.

In addition, in order to refine the selection, the following inclusion/exclusion criteria were applied (see Table 4.1).

Table 4.1 Selection criteria

Inclusion criteria	Exclusion criteria
Articles that discuss the cybersecurity and IT security risks faced by academic institutions, statistics on cyber-attacks, and future expectations for cybersecurity in education	Information published on non-specialized websites
Documents presenting analysis from leaders and specialists in the area of cybersecurity, focused on the academic environment	Documents with irrelevant contributions
Articles with information about the most current defense methods developed to prevent cyber-attacks	Information from blogs

4.2.2 Conducting the Search

At this stage, the most relevant articles were identified considering the key words and the selection criteria. In each document, the titles, development, and conclusions were reviewed, in order to establish the contribution, they make to the questions posed.

After executing the search, a total of 52 documents were obtained, from which 35 were selected, all of which met the criteria defined above.

4.2.3 Analysis and Documentation of Results

In order to analyze the importance of cybersecurity education to minimize the risks faced by academic institutions, it is important to know which are the most frequent threats faced by organizations belonging to the educational sphere, answering this by developing Q1: What are the main cybersecurity risks faced by academic institutions?

The crisis generated by the COVID-19 pandemic had a major impact on the increase in cyber-attacks on academic institutions, finding that among the cybersecurity threats that occur most frequently within the educational environment is phishing, defined as a technique employed by cybercriminals that aims to deceive users and obtain confidential information, such as passwords or bank details [5]. MacKay [6] notes that between 2019 and 2020, 70% of UK universities were victims of phishing attacks, as well as being targeted by email scams. These attacks generally take the form of fake emails, very similar to legitimate ones, which are sent to students and employees, inviting them to click on malicious links or provide personal information, leading to identity theft or allowing the attackers access to the institution's internal networks [7].

Another type of threat with a high presence is malware, that is, malicious software designed to infiltrate systems and cause damage, this type of attack occurring through downloads of infected files, compromised websites, or external storage devices. According to the survey carried out by the cybersecurity company Kaspersky in 2020 [8], of all the malwares detected, 90% were risk software, that is, files that allow cybercriminals to carry out actions without the user's consent after of your installation. Once these malicious files infiltrate the system, they have the ability to steal confidential information, damage, lock files, and even allow remote control of the computer [9, 10].

Educational institutions also face the risk of ransomware attacks, where hackers encrypt files and demand a ransom in order to be released. According to the Verizon Data Breach Investigations Report 2022 [11], 30% of data breaches in the education sector were attributed to ransomware attacks. This attack modality has a significant impact, considering that it can bring the institution's operations to a halt and jeopardize the confidentiality and integrity of critical data [3, 12].

With respect to distributed denial-of-service (DDoS) attacks, these represent a type of cyber-attack that saturates a server or a website with continuous junk traffic, and over time, the website slows down or fails, making servers and websites unavailable to real users. In the context of educational institutions, a DDoS attack will make it impossible for students and staff to log into the learning management system to access online learning materials and other essential services, making it necessary for educational institutions to invest heavily in additional resources or services to recover from its effects [13].

It is evident that educational institutions, both higher and basic education, are increasingly being cyber-attacked, with 60% having suffered such threats in 2021, while in 2020, this percentage was 44%. In addition, educational institutions also faced the highest rate of data encryption compared to other sectors last year, as well as the longest recovery time, with 7% taking at least three months to recover, almost double the average time for other sectors, according to Sophos' State of Education Cyberattacks 2022 survey [14].

Q2: What are the benefits of cybersecurity education for academic institutions?

The above indicates that cybersecurity is crucial in the education sector, especially in higher education institutions, for a number of reasons, including the protection of sensitive data, since universities handle a large amount of data, such as personal information, academic records, and financial data of students and staff, and cybersecurity measures are essential to safeguard this information from unauthorized access, theft, and other cyber threats [15, 16]. It is very common for educational institutions to be the target of cyber-attacks, including phishing attacks, ransomware, and denial-of-service attacks, so a robust cybersecurity system helps prevent these types of threats and protects the institution's IT infrastructure.

Furthermore, cybersecurity is vital to maintaining academic integrity; online learning and testing are becoming increasingly common, so there is a need to ensure that students' grades and achievements are genuine and secure [17]. As regulated organizations, universities must comply with various privacy and data protection laws; consequently, cybersecurity measures are necessary to comply with these regulations and avoid legal consequences. Cybersecurity breaches can have serious consequences on the reputation of an academic institution; therefore, by implementing robust cybersecurity measures, they demonstrate a commitment to protecting student and staff data, as well as maintaining their reputation as a secure institution [18].

It can be argued that cybersecurity is critical in education, especially in higher education institutions, to protect sensitive data, prevent cyber-attacks, maintain academic integrity, comply with state regulations to avoid the legal implications of data breaches in the storage of student and faculty information, as well as manage the reputation of the institution by complying with digital security regulations [19, 20].

On the other hand, cybersecurity education is not only important to protect against online threats, but also offers many benefits, including learning to recognize and avoid such threats, enabling users to recognize and prevent them, because informed users can make informed decisions about the security of their information and privacy [21].

Through cybersecurity knowledge, users can better protect their personal and financial data online, including knowing how to create strong passwords, use two-factor authentication, and avoid sharing sensitive information online, as well as teaching cybersecurity best practices for browsing the internet safely, avoiding clicking on suspicious links, downloading software from trusted sources, and keeping software and applications update [22]. Consequently, cybersecurity education helps to increase online protection and privacy, because informed users can take steps to protect their information and privacy, which decreases the likelihood of falling victim to cyber-attacks.

In addition, it is important to note the consequences of cybersecurity ignorance, which has serious implications, both financially and emotionally. Online security breaches can be costly for victims, with recovery costs including hiring cybersecurity experts, removing malicious software, restoring lost files, and implementing new security measures, and in most cases, these costs can be so high that academic institutions may struggle to afford them [23].

Cybersecurity education can save money in the long run by preventing online security breaches. By being informed about online risks, users can take preventative measures to avoid falling victim to cyber-attacks. This means that they will not have to face the costs of recovering from a security breach, saving money and time in the process [24].

On the other hand, in addition to the financial costs, online security breaches can also have a significant emotional cost, as victims may feel invaded, vulnerable, and exposed, experiencing anxiety, stress, and fear of future cyber-attacks [25]. Consequently, ignorance of cybersecurity can have serious consequences in terms of both financial and emotional costs. However, cybersecurity education can prevent such breaches and save money in the long run, so if you want to avoid the costs of an online security breach, investing in cybersecurity education is one of the best decisions you can make.

It is indisputable that educational institutions are an inherently vulnerable cybersecurity target and in many cases are not given as much attention and adequate re-courses compared to other sectors and industries [26]. However, increasing cyber incidents against educational institutions and technologies threaten the privacy of students and staff, cause financial and reputational damage, jeopardize intellectual property, affect the potential for foreign grants and investments, disrupt the overall teaching–learning processes, and thus pose a problem for the education sector; therefore to pose a critical national security risk problem that should not be transferred to educational institutions to deal with alone, it is essential that cybersecurity in education can be seen as a national policy challenge, requiring public strategies to manage it [27].

Park [28] points out that the cybersecurity of academic institutions can be ensured if five maturity principles are respected, which are: incomplete, initial, management, developing, and optimizing, where initial means that cybersecurity principles are used but poorly; incomplete indicates that the codes are not implemented or partially implemented; while the developing model means that the principles are well implemented. On the other hand, the management principle means that regulations are established as standard business policy and practice, so this progressive optimization model implies a deliberate focus on continuous improvement and optimization.

Q3: What are the strategies to reduce cybersecurity risks in academic institutions?

Given the existence of cyber-attacks, it is necessary for educational institutions to prepare themselves in the best way to face these threats by considering the implementation of effective and proactive strategic measures to protect their IT systems. The main strategies that help educational institutions to strengthen cybersecurity and, consequently, protect critical systems and data against ever evolving threats include establishing clear cybersecurity policies aimed at promoting awareness, addressing issues such as the safe use of passwords, protection of personal data, safe Internet browsing, and proper handling of suspicious emails. It is also essential to educate and raise awareness among students, teachers, and administrative staff about good cybersecurity practices through awareness campaigns, training, and the dissemination of relevant information [29].

It is also important to protect systems and networks by implementing robust security measures, including the installation and configuration of firewalls and intrusion detection and prevention systems to monitor network traffic. Furthermore, it is vital to have up-to-date anti-virus and anti-malware solutions in place to detect and eliminate potential threats. It is essential that institutions develop and implement two-factor authentication mechanisms to gain access to systems, networks, and databases, which provide an additional layer of security by requiring a second verification factor, such as photo authentication of the user and/or institutional ID [30].

Another important measure is the implementation of data backup and recovery plans, by performing regular backups of critical data and developing a disaster recovery plan, which involves establishing regular automatic backup policies and regular verification of the integrity of the backups. In this regard, it is advisable to define procedures and responsibilities in case of a security incident in order to ensure a quick and effective response. Periodic recovery tests can assess the effectiveness of plans and ensure the ability to restore data in the event of an emergency [31].

Ongoing collaboration with cybersecurity experts and conducting audits should also be considered, as these professionals can develop security audits that assess the existing security infrastructure, identify potential vulnerabilities, and provide specific recommendations to strengthen defenses. In addition, these cybersecurity experts can assist in the implementation of advanced protection solutions and the proper configuration of systems, providing expert advice and ensuring that institutions are aware of and prepared for the latest trends [32].

Also, effective response to security incidents by establishing a specialized response team in the area to support the defined action plan. This involves designating clear roles and responsibilities within the team, establishing efficient communication channels, and defining the steps to be taken in the event of an incident. Emphasizing that a quick and effective response time is crucial to minimize the impact of incidents and avoid the spread of threats, it is therefore advisable to conduct a post-incident evaluation to identify lessons learned and continuously improve existing security measures [3].

In line with all of the above security measures, it is essential that educational institutions promote continuous cybersecurity education and training for staff, students, and other members of the educational community. This should include organizing workshops, courses, and seminars on cybersecurity-related topics, providing educational resources and regularly updating users on new threats and best security practices [1]. In addition, it is important to foster a security mindset throughout the educational community by encouraging users to report suspicious incidents and to stay up-to-date on implemented security measures [3].

Since the emergence of cybersecurity as an area of interest, several authors have dedicated themselves to the development of this topic, such as the research of Dar [33] where he describes and analyzes the key information security challenges within educational institutions and proposes a framework for management to ensure sustainability, growth, and development. Similarly, Sikos and Haskell-Dowland [34] describe the key challenges and solutions for computer and network security in education, and Custer [35, 36] provides an extensive theoretical analysis of information security threats, data assets, and risks in higher education with challenges and solutions, highlighting that all these studies emphasize the importance of cybersecurity education as a risk control mechanism in academic institutions.

4.3 Conclusions

Cybersecurity is crucial in any business environment, but especially in academia, considering that the education sector experienced an incredible increase in cyberattacks during the COVID-19 pandemic as the number of users and the use of connected devices in academic institutions at all levels increased, resulting in a variety of incidents by cybercriminals, from ransomware to data breaches and phishing.

Cyber-attacks not only compromise the security of teachers and academic administration, but also the privacy of students, given that millions of users now learn through technology in hybrid, remote, or face-to-face environments, making it difficult to keep secure the devices that are central to students' learning experiences and teachers' work.

In conclusion, adopting cybersecurity measures is critical for academic institutions in order to protect student data, prevent cyber-attacks, maintain business continuity, protect intellectual property, and ensure compliance with data privacy laws. Therefore, these institutions must take this aspect very seriously and implement robust cybersecurity measures to protect their networks and data so that they can provide a safe learning environment for students, ensuring learning and development in today's digital world.

Acknowledgements We wish to express our sincere gratitude to the Pontificia Universidad Católica del Ecuador for their support of our research, which was conducted as part of the activities of the Applied Information Systems and Technologies research group (SITECIA), registered under GI-Quito-071-2022. Furthermore, we extend our heartfelt appreciation to the Anonymous Reviewers whose thoughtful and constructive recommendations greatly enhanced the quality of this paper. Their expertise and feedback played a pivotal role in refining our research and ensuring its rigor and credibility.

References

1. Rahman, N., Sairi, I., Zizi, N., Khalid, F.: The importance of cybersecurity education in school. Int. J. Inform. Educ. Technol. **10**, 378–382 (2020). https://doi.org/10.18178/ijiet.2020.10.5.1393
2. Nakama, D., Paullet, K.: The urgency for cybersecurity education: the impact of early college innovation in hawaii rural communities. Inform. Syst. Educ. J. **16**, 41–52 (2018)
3. Flores, V.: Let's Talk Cybersecurity: Recommendations for Higher Education Institutions," Proctorizer, 6 June 2023. https://proctorizer.com/ciberseguridad-para-instituciones-de-educacion-superior/. Accessed 19 Sept 2023
4. Kitchenham, B., Pearl Brereton, O., Budgen, D., Turner, M., Bailey, J., Linkman, S.: Systematic literature reviews in software engineering—a systematic literature review. Inform. Softw. Technol. **51**(1), 7–15 (2009). https://doi.org/10.1016/j.infsof.2008.09.009.
5. Cuchta, T. et al.: Human Risk Factors in Cybersecurity, pp. 87–92 (2019). https://doi.org/10.1145/3349266.3351407.
6. MacKay, J.: How Universities Can Protect Themselves from Cyberattacks. 25 July 2020. https://www.metacompliance.com/es/blog/security-awareness-training/how-universities-can-protect-themselves-from-cyber-attacks. Accessed 20 Sept 2023
7. Priestman, W., Anstis, T., Sebire, I.G., Sridharan, S., Sebire, N.J.: Phishing in healthcare organizations: threats, mitigation and approaches. BMJ Health Care Inform. **26**(1), e100031 (2019). https://doi.org/10.1136/bmjhci-2019-100031
8. Level 4.: Malware Affects Educational Institutions in Latam (2020). https://blog.nivel4.com/nivel4/malware-afecta-instituciones-educativas-en-latam. Accessed 20 Sept 2023.
9. Krishnamurthi, R., Kumar, A., Gill, S.S.: Autonomous and Connected Heavy Vehicle Technology. Academic Press (2022)
10. Lallie, H., Thompson, A., Titis, E., Stephens, P.: Understanding Cyber Threats Against the Universities, Colleges, and Schools (2023)
11. Kost, E.: The State of University Cybersecurity: 3 Major Problems in 2023 | UpGuard (2023). https://www.upguard.com/blog/top-cybersecurity-problems-for-universities-colleges. Accessed 20 Sept 2023
12. Barker, W., Fisher, W., Scarfone, K., Souppaya, M.: Ransomware risk management: a cybersecurity framework profile. In: National Institute of Standards and Technology, NIST Internal or Interagency Report (NISTIR) 8374 (2022). https://doi.org/10.6028/NIST.IR.8374
13. Chancey, T.: Cybersecurity in Schools: The Importance of Cyber Security in the Education Sector (2023). https://www.scarlettcybersecurity.com/ImportanceOfCyberSecurityInEducationAndSchools. Accessed 21 Sept 2023
14. Cavanillas, L.: El 60% de las instituciones educativas ha sido víctima del ransomware. Escudo Digital (2022). https://www.escudodigital.com/ciberseguridad/60-instituciones-educativas-victima-ciberataque-ransomware_52857_102.html. Accessed 20 Sept 2023.
15. Ulven, J.B., Wangen, G.: A systematic review of cybersecurity risks in higher education. Fut. Int. **13**(2) (2021). https://doi.org/10.3390/fi13020039
16. Giszczak, J., Paluzzi, D.: Pass or Fail? Data Privacy and Cybersecurity Risks in Higher Education. 23 August 2016. https://www.mcdonaldhopkins.com/insights/news/Pass-or-fail-Data-privacy-and-cybersecurity-risks. Accessed 23 Sept 2023
17. Beaudin, K.: The legal implications of storing student data: preparing for and responding to data breaches. New Dir. Inst. Res. **2016**(172), 37–48 (2017). https://doi.org/10.1002/ir.20202

18. Dadkhah, M., Borchardt, G., Maliszewski, T.: Fraud in academic publishing: researchers under cyber-attacks. Am. J. Med. **130**(1), 27–30 (2017). https://doi.org/10.1016/j.amjmed.2016.08.030
19. Univaf. Why Cybersecurity in Education Matters. 30 March 2023. https://www.univaf.com/why-is-cybersecurity-important-in-education/. Accessed 19 Sept 2023
20. Beaudin, K.: College and University Data Breaches: Regulating Higher Education Cybersecurity under State and Federal Law. J.C. & U.L **41**, 657 (2015)
21. Guaña Moya, J.: La importancia de la seguridad informática en la educación digital: retos y soluciones. RECIMUNDO: Revista Científica de la Investigación y el Conocimiento **7**(1), 609–616 (2023)
22. Amankwa, E.: Relevance of cybersecurity education at pedagogy levels in schools. J. Inform. Secur. **12**(4), 4 (2021). https://doi.org/10.4236/jis.2021.124013
23. Best, F.: Cybersecurity ignorance risk. Cyber Risk Leaders, 7 March 2022. https://cyberriskleaders.com/cybersecurity-ignorance-risk/. Accessed 21 Sept 2023
24. Brown, A.: How cybersecurity can help your business save money—compare your business costs (2022). https://compareyourbusinesscosts.co.uk/how-cybersecurity-can-help-your-business-save-money, https://compareyourbusinesscosts.co.uk/how-cybersecurity-can-help-your-business-save-money. Accessed 21 Sept 2023
25. Impulse_06.: The Importance of Cybersecurity Education, Impulse (2023). https://impulso06.com/?p=13268. Accessed 19 Sept 2023
26. Mello, S.: Data Breaches in Higher Education Institutions, Honors Theses and Cap-stones (2018), [Online]. Available at: https://scholars.unh.edu/honors/400
27. Fouad, N.S.: Securing higher education against cyberthreats: from an institutional risk to a national policy challenge. J. Cyber Policy **6**(2), 137–154 (2021). https://doi.org/10.1080/23738871.2021.1973526
28. Park, H.: A study on cyber crime deterrence recognition: the influence of recognition of punishment for cyber crime on intention to report crime. Korea Assoc. Crim. Psychol. **16**(4), 85–98 (2020). https://doi.org/10.25277/KCPR.2020.16.4.85
29. Khando, K., Gao, S., Islam, S.M., Salman, A.: Enhancing employees information security awareness in private and public organizations: a systematic literature review. Comput. Secur. **106**, 102267 (2021). https://doi.org/10.1016/j.cose.2021.102267
30. Birkinshaw, C., Rouka, E., Vassilakis, V.G.: Implementing an intrusion detection and prevention system using software-defined networking: defending against port-scanning and denial-of-service attacks. J. Netw. Comput. Appl. **136**, 71–85 (2019). https://doi.org/10.1016/j.jnca.2019.03.005
31. Kesa, D.M.: Ensuring resilience: integrating it disaster recovery planning and business continuity for sustainable information technology operations. World J. Adv. Res. Rev. **18**(3), 3 (2023). https://doi.org/10.30574/wjarr.2023.18.3.1166
32. Catal, C., Ozcan, A., Donmez, E., Kasif, A.: Analysis of cyber security knowledge gaps based on cyber security body of knowledge. Educ. Inf. Technol. **28**(2), 1809–1831 (2023). https://doi.org/10.1007/s10639-022-11261-8
33. Dar, W.: Cyber security challenges on academic institutions and need for security framework towards institutional sustainability growth and development. I manager's J. Inform. Technol. **5**, 1 (2016). https://doi.org/10.26634/JIT.5.1.4795
34. Sikos, L.F., Haskell-Dowland, P.: Cybersecurity Teaching in Higher Education. Spring-er Nature (2023)
35. Custer, W.: Information security issues in higher education and institutional research. New Dir. Inst. Res. **2010**, 23–49 (2010). https://doi.org/10.1002/ir.341
36. Guaña-Moya, J., et al.: Ataques informáticos más comunes en el mundo digitalizado. Revista Ibérica de Sistemas e Tecnologias de Informação E **54**, 87–100 (2022)