ESG Integration in E-Learning: Enhancing Cybersecurity and Social Well-Being for Learners

Goran Pavlović[1,*]

[1]Faculty of Management, Belgrade Metropolitan University, Tadeuša Košćuška 63, 11000 Belgrade, Serbia

Abstract

This paper examines the specific safety challenges in digital learning within higher education institutions that can adversely impact the well-being of students and employees. As HEI embrace e-learning, the integration of digital technologies brings forth concerns regarding security, trust, and the overall learning experience. The goal is to identify these critical safety issues and propose effective solutions that emphasize the importance of raising awareness and building a culture of safety in digital environments. This paper highlights the significance of environmental, social, and governance (ESG) principles in enhancing sustainability within educational contexts. Ultimately, a comprehensive safety culture will not only protect individuals but also enrich the learning experience, establishing a secure framework for effective digital education in HEI.

Keywords

E-learning, Well-being, ESG, Cybersecurity Awareness, HEI

1. Introduction

Higher education institutions (HEI) are involved in the general process of digitization and digital transformation that is taking place across organizations. However, digital technologies in HEI do not only refer to the active use of digital solutions in everyday operations to enhance efficiency and flexibility, but also their integration into the process of student education [1]. In other words, various forms of e-learning have been developed, which can be understood as the use of information and communication solutions, applications, software, and the Internet to create and transfer knowledge [2]. E-learning is thus characterized by the presence of learning materials in digital form, allowing students to learn independently of their current location, time, and other such factors. As a result of this approach, the flexibility, efficiency, and innovation of the learning process increase, as do those of the HEI themselves, which now require fewer resources and funds to develop educational programs [3].

However, while the positive changes brought about by digitization are notable, they are accompanied by negative aspects, particularly regarding security concerns. To develop talents, HEI must place special emphasis on improving the safety of learning in the digital environment, as this issue is increasingly recognized as relevant within the field of sustainability. Specifically, the integration of ESG (Environmental, Social, and Governance) principles is becoming increasingly significant in HEI. In order to enhance sustainability, HEI must focus on accountability, inclusiveness, ethical management, transparency, as well as the well-being of students and employees [4].

Digital well-being includes the impact of digital technology usage on the mental, physical, and emotional states of users (students and employees) [5]. As such, digital well-being in HEI should be viewed as a systemic and dynamic category that affects the behaviors and attitudes of students and employees through various factors [6]. Among these factors, security must be a primary concern, as the absence of trust in security measures leads to negative attitudes towards the use of digital technologies [7], which consequently threatens learning performance in HEI, as well as overall well-being, which is an important ESG dimension.

BISEC'2024: 15th International Conference on Business Information Security, November 28-29, 2024, Niš, Serbia

*Corresponding author.

goranpavlovic@metropolitan.ac.rs (G. Pavlović)

0000-0002-5557-9262 (G. Pavlović)

Based on the above, the aim of this paper is to examine the specific safety challenges in digital learning that can reduce the well-being of students and employees, and to propose potential solutions based on these issues, with special emphasis on raising awareness and building a culture of safety in digital learning.

2. E-learning as a form of sustainable HEI solution

E-learning involves the use of hardware and software solutions, the Internet, and other technologies for learning. In this context, learning resources are made available to all authorized users whenever they need them [1, 8]. With the development of the Internet, learning resources can now be accessed anytime and anywhere, significantly enhancing the efficiency and flexibility of the learning process [9]. However, despite technological advancements, e-learning systems still rely on instructors, professors, content creators, administrative staff, and IT experts who provide the necessary infrastructure, as well as the learning participants themselves [3]. In other words, in addition to technological and digital infrastructure, e-learning systems also encompass additional dimensions, namely, infrastructural, communication, network, and social elements.

The technological advancements have led to the development of various e-learning systems in HEI. Learning Management Systems (LMS) were already implemented in HEI before the onset of digital transformation, but in recent years, they have seen widespread and comprehensive adoption. Through LMS platforms, complex courses have been developed, incorporating various activities such as seminars, lessons, glossaries, practical tasks, and tests. According to the LMS system market report, the most commonly used systems in European HEI are: Moodle (65%), Blackboard (12%), Ilias (4%), and Sakai (3%). HEI also utilize cloud computing solutions, which offer numerous advantages, including efficient data storage, the organization of online classes, and the migration of university network infrastructures to cloud platforms [10].

In the Republic of Serbia, the pioneer in the field of online and distance learning, as a form of e-learning, was Belgrade Metropolitan University (BMU), which was awarded this distinction in 2005 [11]. BMU's existing e-learning platform allows both learners and instructors to upload materials. Professors, as creators and disseminators of knowledge, design lessons using specialized software called "mDita", which facilitates the creation of lessons following a model similar to traditional teaching. These lessons contain presentations, texts, images, video materials, tests, various forms of knowledge assessment, resource sharing, and a discussion forum [12]. In addition to the aforementioned platform, other tools are also used for knowledge sharing and collaboration, such as Zoom, Google Meet, and the Microsoft Teams platform, among others.

3. Security risks of e-learning systems as a threat to the well-being of learning participants

Security in learning is associated with ensuring that the resources within the e-learning system, as well as the data of the individuals involved in this process, cannot be accessed or used without authorization [9]. Given that resources, materials, and data are stored in areas accessible via the Internet, there is a significantly higher risk of misuse and unauthorized access compared to a traditional environment. Specifically, issues such as identity theft, impersonation, poor authentication, and cyberattacks must be considered [8]. HEI, like other organizations, face various forms of cyberattacks, such as phishing, malware, and data theft [13].

HEI store large volumes of sensitive data, and the theft or compromise of this data could lead to serious consequences that extend far beyond academic contexts. Cyberattacks employ the latest technologies and methods to exploit vulnerabilities in university systems, which, in some cases, are unfortunately outdated and insufficiently protected. As a result, the security of e-learning systems has become a critical area of focus for educators actively involved in teaching. These systems aim to integrate elements of in-person instruction with e-learning, webinars, and other forms of digital content. Building trust

and encouraging user engagement with an online learning system (OLS) is vital, as it facilitates both synchronous and asynchronous learning. Synchronous learning occurs in real time, with all participants communicating simultaneously, while asynchronous learning allows for independent progress, with the ability to exchange ideas and information without the simultaneous participation of other users [14].

Before analyzing the threats on online learning platforms, it is important to explain the basic principles that ensure the quality of these courses. Confidentiality is particularly crucial, especially during exams, to ensure that their content is not accessible before the scheduled time and that the tests are not exposed to unauthorized students. Learning platforms contain numerous technical and human vulnerabilities, with over 400 vulnerabilities identified in the most popular LMS systems. Threats can be categorized into four main areas: authentication, availability, confidentiality, and integrity. Authentication threats include insecure communications, such as HTTP, as well as poor session management and weak authentication algorithms. Availability threats encompass Denial of Service (DoS) attacks that overwhelm a server and logical attacks that cause servers to crash. Confidentiality threats involve insecure cryptographic storage and information leakage due to errors. Integrity threats, such as buffer overflow and Cross-Site Scripting attacks, allow attackers to execute malicious code, steal data, or alter LMS content. Similarly, video conferencing applications (VCAs) face significant security challenges. The main threats include identity theft and encryption insecurity, as many applications use transport encryption rather than end-to-end (E2E) encryption, which permits access to data from the server. Additionally, there is a risk of unauthorized access and rebroadcasting of conferences [10, 15].

Although e-learning systems are designed with pedagogical principles at the forefront, security issues are often overlooked, which can lead to undesirable situations that negatively impact the educational process and its management. For instance, students may falsify grades, impersonate others, intrude on private conversations, alter timestamps on submitted papers, or even allow tutors to access students' personal information. Advanced Persistent Threats (APTs) present a serious challenge to HEI, as they enable hackers to maintain continuous access to sensitive data, particularly intellectual property such as research work from university centers. A Distributed Denial of Service (DDoS) attack represents another significant threat to HEI, as it can disrupt access to data or networks, affecting availability. While many attacks on academic institutions do not directly threaten the confidentiality or integrity of data, DDoS attacks can create substantial issues related to resource availability. Fraud and phishing attacks have become prevalent threats in the higher education sector, particularly during the pandemic. These attacks exhibit a high success rate, reaching up to 30%, as attackers employ sophisticated machine learning techniques to craft and distribute convincing fake messages, causing victims to inadvertently compromise university or organizational networks. Phishing attacks allow hackers to steal usernames, IP addresses, and other personal information, as well as gain access to private databases. Ransomware attacks have become increasingly frequent in HEI, particularly at the beginning of new academic years. In these attacks, hackers exploit unpatched security vulnerabilities in software and hardware, as well as phishing emails, to deploy ransomware. Attackers often target backup devices, sabotaging them to hinder data recovery, encrypt virtual servers, and use scripted environments to implement ransomware [8, 13, 14]. In a study conducted by Wetini et al. in 2024, HEI reported the following most common security threats: phishing (60%), malware (40%), unauthorized access (40%), ransomware (35%), and data breaches (25%) [14].

4. Security risk management in e-learning systems

E-learning platforms must adhere to fundamental security principles, including authenticity, access control, confidentiality, integrity, availability, and non-repudiation. Authenticity is achieved by securely identifying users and assigning appropriate access privileges, thereby preventing unauthorized access and data manipulation. Best practices include enforcing strong passwords and periodic re-authentication. Access control is implemented based on user roles, permitting only authorized actions within the system. Confidentiality refers to the protection of data through proper access control mechanisms and encryption. Integrity ensures that only authorized users can modify data, and any breach of system integrity can

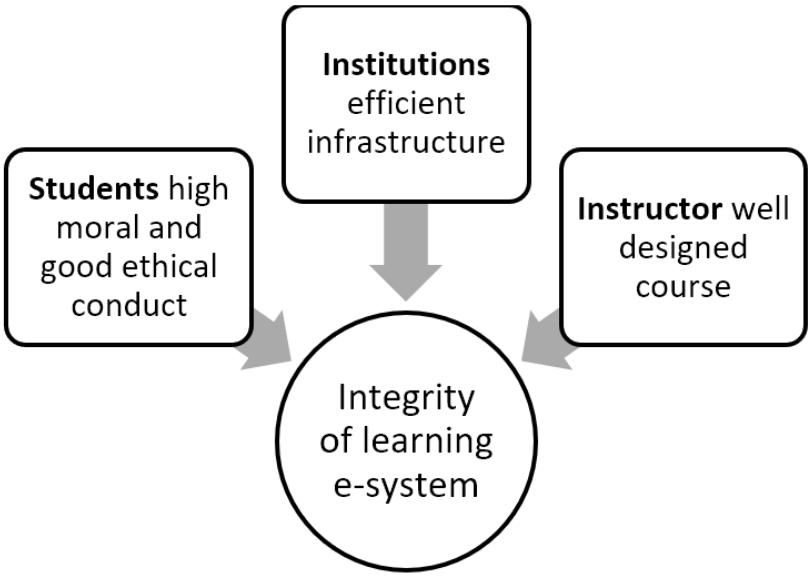

Figure 1: Integrity in e-learning systems.

lead to malfunctions. Non-repudiation means that users cannot deny performing actions, such as deleting data, with all activities being logged in protected log files [2]. If integrity is considered in the context of ensuring the well-being of learners, the system should be structured as shown in Fig. 1 [16].

E-learning systems require the implementation of various security measures to safeguard against potential threats. Cryptography plays a crucial role in ensuring data confidentiality by transforming information into an unreadable format through encryption methods such as symmetric and asymmetric encryption, which also guarantees both data integrity and authentication. Additionally, Digital Rights Management (DRM) helps regulate the distribution and reuse of e-learning content, thereby reducing the risk of unauthorized access or theft of intellectual property. To enhance the security of user accounts, biometric authentication is becoming increasingly popular, as it verifies the user's identity through physical characteristics, thus minimizing the risk of password misuse. Furthermore, digital rights management protects the copyright of e-learning content by embedding copyright information in media files, preventing unauthorized use. Finally, protection against cyber-attacks can be achieved by employing the HTTPS protocol, intrusion detection systems, and cryptographic mechanisms, while the use of additional security practices, such as CAPTCHA and SSL, further safeguards against attacks and ensures the integrity of sessions and data [15].

Regular updating of information systems and automation are key steps in maintaining a consistent level of security. Furthermore, developing information access policies is crucial to minimizing the risk of unauthorized access and data breaches, with classification of information according to access levels playing a vital role in protecting sensitive data. The application of secure protocols also ensures data protection for both end-users and HEI by encrypting data during transmission. Lastly, educating employees and students about information security is not only important for reducing the burden on IT teams but also for enhancing overall cybersecurity by distributing responsibility and raising awareness of security measures [10].

5. Increasing safety awareness and creating a safety culture

Creating a culture of security awareness is crucial for protecting HEI and e-learning systems. Although technical sophistication is necessary, technology alone, without user support, is insufficient. It is essential to develop a culture of security awareness in which all members of the organization understand the

risks and are aware of their role in protecting information. While HEI should foster openness and collaboration, this can sometimes lead to complacency among students and staff regarding security processes. Developing digital trust is even more important given the changes in HEI, which now offer significant student engagement through online learning systems (OLS). As students gain a deeper understanding of information systems and technology, they have higher expectations for the usability, security, and protection of their personal data [14].

In light of the ESG dimensions of sustainability and digitalization indicators, increasing cybersecurity awareness is particularly significant. Cybersecurity awareness training involves educating students, employees, and other learners about the importance of protecting user data, identities, and other resources that may attract cybercriminals. It also addresses the risks associated with the use of the internet, email communication, and online interactions. Security training is critical to preventing security breaches caused by human error, developing a cybersecurity culture, and preparing for potential cyber attacks [17].

Content creators in the e-learning system within the HEI should focus on providing a secure learning environment and ensuring the safe storage of confidential student data. Students and other learners form judgments about the reliability of the educational environment and are particularly concerned with protecting their sensitive personal data [14]. This practically means that it is essential to regularly evaluate the attitudes of students and other learning participants, which is a relevant indicator of the social dimension within the ESG principles of sustainability. To increase students' awareness of the risks involved in e-learning, it is important for them to grasp several key factors. First, they need to become responsible digital users who understand their online activities and their consequences. Additionally, students should recognize the value of their data and digital footprint, as every online action can leave a trace. It is also vital for them to be aware of the wide range of potential threats and vulnerabilities on the internet and learn how to identify and verify trusted digital resources. Protecting their digital devices is crucial for maintaining security and privacy, and students should actively develop a positive and ethical approach to using academic software and systems [1].

To achieve good results, it is necessary to implement safety education during e-learning. The goals of security education include enhancing responses to cybersecurity incidents, reducing violations, improving the effectiveness of security tools, increasing proficiency, and understanding new cyber threats. The initial phase of security awareness involves measuring the baseline level of awareness within the HEI before security training is implemented. This assessment helps tailor training programs to address specific areas of vulnerability and strengthen security measures. Implementing safety training involves establishing a behavioral reference point, activating safety measures, and ensuring proper behavior from the start. The benefits of cybersecurity training include reducing overall security risks, minimizing financial losses due to cybercrime, preventing security breaches when employees leave the organization, and maintaining a positive reputation with stakeholders [17]. In this context, the implementation of ESG dimensions in HEIs, including digital security during e-learning, requires intensive cooperation with key stakeholders. In these institutions, the well-being of students must be prioritized, as well as the well-being of other participants and educators, such as professors [18]. Three key stakeholders in the e-learning system (HEI, students, and teachers) play critical roles. Institutional accountability remains essential. Teachers have a significant role in presenting a true model of academic integrity. As a global standard, academic integrity is enforced by requiring institutions to authenticate each student's identity through valid logins and passwords, proctored exams, and various technologies to verify student participation [16].

In ensuring and maintaining cybersecurity in e-learning systems, all other actors in the system (IT experts, management, legal professionals, etc.) must make decisions at various stages of predicting, detecting, preventing, or defending against cyberattacks. These decisions may involve distinguishing whether a digital action or content is a cyberattack, or designing and implementing processes to actively detect, prevent, or defend against attack activities [3]. Therefore, achieving well-being in the e-learning process requires a systemic approach, integrating numerous actors whose task is to improve governance and enhance the social dimension of HEI sustainability

6. Conclusions

The examination of safety challenges inherent in digital learning within HEI reveals critical concerns that can adversely affect the well-being of both students and employees. The digital landscape offers unparalleled flexibility and efficiency, yet it also poses significant risks that can undermine trust and engagement in educational processes. As such, the integration of a robust safety culture is essential to mitigate these risks. To achieve this, it is imperative to prioritize the creation of a comprehensive safety awareness program that educates all stakeholders - students, faculty, and administrative staff, about the importance of cybersecurity and their individual roles in protecting sensitive information. This involves proactive strategies such as regular cybersecurity training, vulnerability assessments, and the establishment of clear protocols for reporting and responding to security threats.

Fostering an environment of accountability and transparency will help cultivate a culture of safety where everyone feels empowered to contribute to the organization's cybersecurity efforts. When individuals understand the implications of their online behavior and appreciate the value of protecting their digital footprint, they are more likely to engage responsibly in digital learning environments. Ultimately, by emphasizing safety awareness and a culture of vigilance, HEI can enhance student well-being, support sustainable e-learning practices, and align with ESG principles. This approach not only safeguards educational integrity but also enhances the overall learning experience.

Acknowledgment

This work was created as a result of the efforts carried out within the project SHIFT - ESG Impact Index in Higher Education, ref. no. 2023-1-ES01-KA220-HED-0001525, funded by the Erasmus+ programme.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] A. Irons, T. Crick, Cybersecurity in the digital classroom: implications for emerging policy, pedagogy and practice, in: The Emerald handbook of higher education in a post-COVID world: New approaches and technologies for teaching and learning, Emerald Publishing Limited, 2022, pp. 231–244.

[2] A. Loureiro, T. Bettencourt, The extended classroom: meeting students' needs using a virtual environment, Procedia-Social and Behavioral Sciences 15 (2011) 2667–2672.

[3] S. Ertan, T. V. Yüzer, Examination of cybersecurity in open and distance learning within the scope of technical support services, Journal of Educational Technology and Online Learning 7 (2024) 254–272.

[4] M. Alenezi, F. Alanazi, Integrating environmental social and governance values into higher education curriculum, Int J Eval & Res Educ 13 (2024) 3493–3503.

[5] P. Nageswaran, K. Leedham-Green, H. Nageswaran, A. V. M. T. Baptista, Digital wellbeing: Are educational institutions paying enough attention?, Medical Education 57 (2022) 216.

[6] K. Adomaitienė, A. Volungevičienė, Digital wellbeing: Students' perspective, Ubiquity Proceedings 4 (2024).

[7] S. Zdravković, G. Pavlović, J. Peković, Determinants of the intentions of consumers in terms of future use of mobile commerce: The moderator's effect of personal innovation, Marketing 50 (2019) 124–134.

[8] Y. Chen, W. He, Security risks and protection in online learning: A survey, International Review of Research in Open and Distributed Learning 14 (2013) 108–127.

[9] R. Hassan, W. Wahi, N. H. A. Ismail, S. A. B. Awwad, Data security awareness in online learning, International Journal of Advanced Computer Science and Applications 13 (2022).
[10] L. A. Alexei, A. Alexei, Cyber security threat analysis in higher education institutions as a result of distance learning, International Journal of Scientific and Technology Research (2021) 128–133.
[11] Belgrade Metropolitan University, Online studies, 2024. URL: https://www.metropolitan.ac.rs/online-studije-ctrl.
[12] J. Milena, Z. J. Nataša, The new virtual reality–teachers' and students' perceptions and experience in english language learning and teaching online, Inovacije u nastavi 34 (2021) 167–186.
[13] S. Watini, G. Davies, N. Andersen, Cybersecurity in learning systems: Data protection and privacy in educational information systems and digital learning environments, International Transactions on Education Technology (ITEE) 3 (2024) 26–35.
[14] I. Bandara, C. Balakrishna, F. Ioras, The need for cyber threat intelligence for distance learning providers and online learning systems, The Need For Cyber Threat Intelligence For Distance Learning Providers And Online Learning Systems (2021) 9312–9321.
[15] L. C. R. Salvador, C. L. A. Llerena, H. P. Dai Nguyen, Digital education: security challenges and best practices, Security Science Journal 2 (2021) 65–76.
[16] H. M. Judi, Integrity and security of digital assessment: Experiences in online learning, Global Business and Management Research 14 (2022) 97–107.
[17] H. H. M. Al-Fatlawi, Awareness of cyber security aspects in distance education, Journal of Pedagogical Sociology and Psychology 6 (2024) 77–88.
[18] R. Ali, H. Zafar, A security and privacy framework for e-learning, International Journal for e-Learning Security (IJeLS) 7 (2017) 556–566.