Empowering Digital Education: Understanding Students' Perceptions about Risks and Threats in the Shifting Educational Paradigm

Monica BARBU[1]*, Alin ZAMFIROIU[1,2], Ion Alexandru MARINESCU[1,3], Dragos IORDACHE[1], Robert BUMBAC[2]

[1] National Institute for Research and Development in Informatics – ICI Bucharest,
8-10 Mareșal Averescu Avenue, Bucharest, 011455, Romania
monica.barbu@ici.ro (*Corresponding author*), alin.zamfiroiu@ici.ro,
ion.marinescu@ici.ro, dragos.iordache@ici.ro

[2] Bucharest University of Economic Studies Bucharest, 6 Piața Română, Bucharest, 010374, Romania
alin.zamfiroiu@csie.ase.ro, robert.bumbac@com.ase.ro

[3] University Politehnica of Bucharest, Doctoral School of Automatic Control and Computers,
313 Splaiul Independenței, Bucharest, 060042, Romania
ionutalexandru1778@gmail.com

Abstract: The rapid adoption of e-Learning platforms, exacerbated by the COVID-19 pandemic, has highlighted the critical need to enhance cybersecurity awareness within educational environments. This research investigates the evolution of cybersecurity risks and threats in e-Learning settings, comparing the pre-pandemic landscape with the and post-pandemic one. The challenges posed by the sudden shift to remote learning and the resulting impact on the cybersecurity posture of the educational institutions are identified through a comprehensive analysis of data and trends. The present study examines the measures taken to mitigate these risks, including security awareness programs and technological enhancements. By evaluating the efficacy of these measures, this paper provides valuable insights into safeguarding e-Learning ecosystems against cyber threats. The findings underscore the necessity for ongoing vigilance and preparedness in an ever-evolving digital educational landscape.

Keywords: e-Learning, Cybersecurity awareness, Threat assessment, Data analysis, Mitigation strategies.

1. Introduction

In recent years, there has been a significant expansion in Digital Learning (DL) across its various subsets, with the most remarkable surge being evident in the realm of e-Learning. This worldwide expansion has taken place in a backdrop where rapid technological advancements, coupled with the emergence of the COVID-19 pandemic, led to a shift towards remote education. Consequently, the integration of technology has become pervasive in education at all levels.

Over the last decade, the increasing rate of adoption of online learning resources, spanning from primary to higher education, has been driven by technological advancements, including, but not limited to, cloud computing, tablet technology, learning via social platforms, the development of learning analytics, the emergence of Massive Open Online Courses (MOOCs), and wearable technology (Bezhovski & Poorani, 2016; Iordache & Barbu, 2021). Today, the e-Learning industry is profoundly influenced by the most recent trends and innovations. These range from mobile learning, gamification, and the integration of artificial intelligence to the incorporation of Virtual Reality, thus fundamentally transforming the landscape of education. By delivering individualized, captivating, and easily accessible learning experiences, these trends are reshaping the future of e-Learning, equipping learners worldwide with newfound empowerment (Awan et al., 2021).

During the COVID-19 pandemic, over 1.5 billion students, spanning from primary school to university, had to engage in remote learning, heavily relying on digital education platforms (Breaz et al., 2022). E-Learning became universally mandatory in 2020 being an indispensable component of at-home learning and remote work (UNESCO, 2020). This sudden changing approach had a significant influence on the expansion of the e-Learning market. According to Statista (2022), the global e-Learning market size in 2020 was estimated at around $250 billion, exceeding $315 billion in 2021 (Cision, 2022), $399.3 billion in 2022 (GMI, 2023), and going to reach 848 billion in 2030 (Facts & Factors, 2023).

https://doi.org/10.24846/v32i4y202310

Along with breakdowns and data fraud, cyberattacks represent one of the main risks classified in the technological categories (Franco, 2020). In their research, Barbu et al. (2022) established a causal relationship between the widespread adoption of remote access solutions in the educational realm and the proliferation of cyber threats during the COVID-19 pandemic. The amplitude of cyber incidents in the period 2019-2021, with substantial impacts on the integrity, confidentiality, and accessibility of e-Learning, was a source of concern regarding the capacity of the academic environment to adequately address those challenges.

The need for immediate short-term educational solutions resulted in an unregulated and unsystematic shift towards e-Learning. This transition occurred in many cases, without a proper legal framework concerning the collection, access, and safeguarding of personal data, privacy rights, or adherence to best practices and principles in securing remote educational processes (Dhawan, 2020). According to the specialised studies, it has been proven that students are more vulnerable to cyberattacks both because of the longer period of online activity and the lack of the necessary skills, abilities, and knowledge to combat the dangers (Hunt, 2016; Zamfiroiu et al., 2022). On the other hand, educational institutions use naturally open campus networks that have multiple access points and are typically widely vulnerable to cyberattacks (Koohang et al., 2020). Because the human element is the cause of over 95% of security incidents and many successful security threats take advantage of human weaknesses, it becomes vital to raise the level of cybersecurity awareness (Gehem et al., 2015).

In the pre-pandemic period, there was a diversity of expert viewpoints concerning the assessment of students' cybersecurity awareness levels. These perspectives varied not only across different regions, but also with respect to the educational stage (Moallem, 2018). In certain cases, the primary concern regarding security awareness lies not in the absence of skills or knowledge, but in the practical application of that knowledge in real-life scenarios (Al Shabibi & Al-Suqri, 2023). There are also studies that indicate a lack of basic cybersecurity knowledge or awareness among university students (Garba et al., 2020).

Under these circumstances, the present research aims to investigate cyber incidents that occurred during the COVID-19 pandemic, evaluating the perceptions of students within Romanian universities regarding the security of e-Learning platforms, such as Google Classroom, Microsoft Teams, Zoom, Webex, and Moodle. This paper is structured as follows. Section 2 provides a concise overview of the key issues related to the awareness of cybersecurity threats and risks in e-Learning, as discussed in the specialised literature. Section 3 offers relevant insights concerning the extent of e-Learning cyberattacks during the pandemic, by means of a new evaluation instrument. A total of 230 students took part in the survey, answering questions concerning the security incidents that had occurred while carrying out their learning activities on e-Learning platforms during the pandemic. Section 4 presents the quantitative and qualitative analysis of the obtained results, emphasizing the consequences of cyber incidents perceived by students, and the main measures applied to prevent them. In section 5, the obtained results are compared through a study involving the vulnerabilities of e-Learning platforms identified in the Common Vulnerabilities and Exposures (CVE) list. The conclusion of this article and further discussions will be found in Section 6.

2. Related Work

2.1 Cybersecurity Awareness in e-Learning

The COVID-19 pandemic has accelerated the adoption of online learning, making it the primary mode of education for millions of people around the world. This exponential growth exposed the vulnerabilities of e-Learning systems (and not only) and led to an increased awareness of cybersecurity threats (Fauzi, 2022; Leu et al., 2023). Institutions, educators, and students have become more aware of the risks associated with online education (Maatuk et al., 2022). As e-Learning continues to evolve, educational institutions and e-Learning platforms must adapt to new challenges and implement robust security measures to protect the integrity of online learning environments. Moreover, as Anghel and Perețeanu (2020) have shown, the education environment, at a global level, and the e-Learning landscape, in particular, are constantly evolving and facing the challenges arising from emerging technologies. Thus, it is difficult to maintain control over how data is used, stored, or shared, which is why the necessity of creating a secure and standardized framework has become more necessary than ever (Vevera et al., 2022).

In (Raju et al., 2022), it is presented how Malaysia switched to the online education environment (Education 5.0) and how Digital Learning became the standard teaching method. In the study, 110 students were interviewed regarding cybersecurity awareness. The authors demonstrated that the students didn’t know how to protect their data and privacy.

Zhang-Kennedy & Chiasson (2021) conducted a review of the main research in the field, by analysing the published articles and the industry products focused on tools developed to educate and raise awareness in the field of cybersecurity, particularly targeting inexperienced users.

Najm et al. (2022) presented the security measures that must be adopted depending on the type of tool used for the training process such as LMS systems, communication platforms, notification systems, settings in user calendars (students or teachers), authentication mode within educational platforms, data cloud storage, video conference management mode, etc. Most of the solutions proposed in the material are based on cloud services (SaaS, PaaS or IaaS) in which security is centrally ensured.

In (Zamfiroiu et al., 2023) an analysis of the vulnerabilities of mobile applications used in the educational environment is carried out, by searching for them on the Common Vulnerabilities and Exposures platform (CVE, 2023).

For this material, two searches were performed for the keywords: “e-learning” and “eLearning”. 21 vulnerabilities containing e-learning keywords and 19 vulnerabilities containing eLearning keywords were identified. The year-by-year distribution of these vulnerabilities is shown in Figure 1.

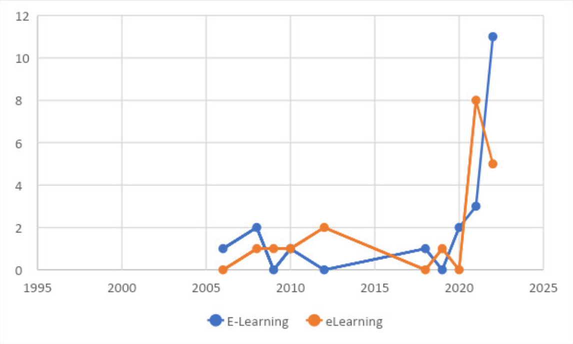

Figure 1. Distribution by year of vulnerabilities (CVE, 2023)

2.2 Previous Work

This study complements a previous initiative (Barbu et al., 2022) on the security of e-Learning platforms during the COVID-19 pandemic and carries out a rigorous analysis regarding the effects of cyber incidents among students.

3. Research Design

3.1 The Purpose of the Research

The main purpose of this study is to explore the possible implications and effects of cyber incidents at the level of teaching activities, as perceived by students, during the COVID pandemic.

3.2 Participants and Procedure

A total of 230 students took part in the survey, of which only 102 reported that security incidents had occurred while carrying out their teaching activities on e-Learning platforms during the pandemic (Question 4, Table 1). Among them, 98 were students enrolled in undergraduate programs at the Bucharest University of Economic Studies, 2 were students enrolled in master’s programs at the same university, 1 was enrolled in the undergraduate program at the University Politehnica of Bucharest and 1 at the Military Technical Academy. Students were asked to answer the questionnaire on cyber incidents between May and June 2023.

3.3 Data Collection

The development of the new evaluation instrument exposed in the present study is based on the results drawn from a previous study (Barbu et al., 2022). In the present paper, only a set of 16 items is used.

The questionnaire includes both quantitative (answers to close-ended questions – namely the items: Q2, Q6, Q12, Q13, Q14, Q15 and Q16) and qualitative data (answers to open-ended questions – the rest of the items).

Table 1 presents the following 16 questions (items) of the evaluation tool.

These questions cover a wide range of topics related to cybersecurity awareness, training, personal security practices, and confidence in e-Learning platforms. They help in gathering comprehensive data to assess the state of cybersecurity in e-Learning environments and the respondents' experiences and perceptions.

4. Evaluation Results

4.1 Quantitative Analysis

The students were asked to answer the close-ended questions of the questionnaire by rating the items on a 5-point Likert scale, starting with 5 indicating "total agreement" and ending with 1 indicating "total disagreement". The analysis was performed using IBM SPSS Statistics 23. The measures of tendency and variation are presented in Table 2.

On average, students moderately agreed (3.88) that they had access to the necessary infrastructure for online teaching activities (Q2). The standard deviation (1.04) suggested that, while there was a

Table 1. Items of cyber incidents questionnaire

No	Question
Q1	How much time did you spend using the e-Learning system each day? (in hours)
Q2	During the online studies, did you have access to the necessary infrastructure to carry out all teaching activities?
Q3	Please select your level of understanding of common types of online threats such as malware and phishing.
Q4	Has there been a cybersecurity incident during the online teaching activity?
Q5	What were the worst consequences of the security incidents that you experienced?
Q6	Have you been able to manage cybersecurity incidents/breaks during the COVID-19 pandemic (2020-2022)?
Q7	How long did it take to fix issues arising from cybersecurity incidents? (in days)
Q8	What measures do you think should be taken to prevent security incidents on e-Learning platforms in the future?
Q9	As a result of the incident(s), was there a cybersecurity training program/procedure for students organized by the university?
Q10	Do you consider it useful to have a guide with recommendations for preventing security incidents on e-Learning platforms?
Q11	Have you attended any cybersecurity course/training/webinar?
Q12	Do you consider that it is important to keep your mobile devices secure and protect your personal information?
Q13	Do you agree that software updates and security patch management are important in preventing cybersecurity incidents?
Q14	Did participation in online activities violate your privacy?
Q15	Do you consider cybersecurity important in the e-Learning process, after the COVID-19 pandemic (2020-2022)?
Q16	On a scale from 1 to 5, how much do you rate your confidence in the educational platforms used during online teaching activities?

Table 2. Descriptive statistics

No	Question	M (mean score)	SD (standard deviation)
Q2	During the online studies, did you have access to the necessary infrastructure to carry out all teaching activities?	3.88	1.04
Q6	Have you been able to manage cybersecurity incidents/breaks during the COVID-19 pandemic (2020-2022)?	3.71	.094
Q12	Do you consider that it is important to keep your mobile devices secure and protect your personal information?	4.46	1.05
Q13	Do you agree that software updates and security patch management are important in preventing cybersecurity incidents?	4.31	1.072
Q14	Did participation in online activities violate your privacy?	2.39	1.091
Q15	Do you consider cybersecurity important in the e-Learning process, after the COVID-19 pandemic (2020-2022)?	4.37	1.098

moderate level of consensus, there was also some variability in their experiences and perceptions regarding infrastructure access.

With a mean score of 3.71, students indicated that they had a moderate level of ability to manage cybersecurity incidents during the COVID-19 pandemic (Q6). The low standard deviation (0.94) suggested that responses were relatively consistent, with students having similar levels of confidence in their ability to handle cybersecurity incidents.

The high mean score of 4.46 indicated that students considered keeping their mobile devices secure and protecting their personal information to be very important (Q12). The standard deviation of 1.05 suggested that, while there was a consensus on the importance of this aspect, there might have been some variation in the degree of importance that students assigned to this aspect.

The mean score of 4.31 reflected a strong agreement among students regarding the importance of software updates and security patch management in preventing cybersecurity incidents (Q13).

The relatively low mean score of 2.39 suggested that, on average, students did not feel that their privacy was significantly violated during online activities (Q14). However, the relatively high standard deviation of 1.091 indicated that there was a wider range of responses, with some students potentially having experienced privacy concerns more than the others.

Finally, the high mean score of 4.37 indicated that, on average, students considered cybersecurity to be highly important in the e-Learning process following the COVID-19 pandemic (Q15).

4.1.1 Correlation Analysis

An analysis using Pearson's correlation shows that Q6 is positively correlated with Q2, Q12, Q13, and Q15, indicating positive relationships between the ability to manage cybersecurity incidents and infrastructure access, the importance of mobile device security, the belief in the importance of software updates and security patch management, and the perceived importance of cybersecurity in e-Learning. The correlations are illustrated in Table 3.

Table 3. Correlation analysis

Variable	Q2	Q6	Q12	Q13	Q14	Q15
Q2	1					
Q6	.387**	1				
Q12	.636**	.420**	1			
Q13	.624**	.424**	.949**	1		
Q14	-.133	-.128	.031	.017	1	
Q15	.616**	.407**	.909**	.909**	.29	1

Q12 is positively correlated with all other variables (Q2, Q6, Q13, Q14, Q15). The strongest correlation is with Q13 (importance of software updates and security patch management), with a correlation coefficient of 0.949. This suggested that students who considered mobile device security and personal information protection important, also tended to believe in the importance of software updates and security measures. Q13 shows strong positive correlations with Q12 (importance of mobile device security), Q14 (privacy violations), and Q15 (importance of cybersecurity in e-Learning).

The correlations with Q2 and Q6 are also strong, indicating that students who emphasized software updates and security measures also tended to emphasize mobile device security, the importance of cybersecurity in e-Learning, and their ability to manage cybersecurity incidents.

Q14 variable is negatively correlated with Q2 (infrastructure access), Q6 (ability to manage cybersecurity incidents), and Q12 (importance of mobile device security). These relatively weak correlations suggested that students who felt that their privacy was violated during online activities tended to have lower infrastructure access and may have perceived a lower ability to manage cybersecurity incidents.

Q15 is strongly positively correlated with Q12 (importance of mobile device security), Q13 (importance of software updates and security patch management), and moderately correlated with Q2 (infrastructure access) and Q6 (ability to manage cybersecurity incidents). These results indicated that students who considered cybersecurity important in e-Learning also tended to emphasize mobile device security, software updates, and their ability to manage cybersecurity incidents.

In summary, the correlation results provide insights into the relationships between various aspects of cybersecurity, infrastructure access, privacy concerns, and students' perceptions. Strong positive correlations suggest that these aspects are strongly related, while negative correlations indicate an inverse correlation.

4.1.2 Students' Trust in e-Learning Platforms

Table 4 presents the descriptive statistics indicators for the answers to question Q16. The high mean score of 4.06 indicated that, on average, students expressed a strong level of trust in Zoom as an e-Learning platform. The relatively low standard deviation of 1.07 suggested that there was a relatively consistent level of trust among the respondents regarding Zoom. This may be attributed to widespread use and familiarity of Zoom platform.

Table 4. Trust in e-Learning platforms

e-Learning platforms	M (mean score)	SD (standard deviation)
Zoom	4.06	1.07
Microsoft Teams	3.60	1.22
Google Classroom	3.45	1.21
Moodle	3.30	1.34
Webex	3.14	1.24

Microsoft Teams received a moderately high mean score of 3.60, indicating that students, on average, expressed a moderate level of trust in this platform. The standard deviation of 1.22 suggested that, while there was a moderate level of trust, there was also some variation in students' trust levels, potentially reflecting varying experiences or perceptions regarding the platform. Students also expressed a moderate level of trust in Google Classroom, Moodle and Webex.

4.2 Qualitative Analysis

In this subsection, the qualitative analysis regarding the answers of the open-ended questions Q3, Q4, Q5, Q7, Q8, Q9, Q10 and Q11 is presented. The answers to the open-ended questions were analysed to extract key words (attributes). Some students described only one or two aspects, while others mentioned several aspects in one sentence, resulting a total number of aspects that exceeded the sum of students participated in the study. The attributes were grouped into main categories, which were ranked in descending order of mention frequency in the tables corresponding to each analysed item.

4.2.1 Level of Understanding of Online Threats

Assessing the level of understanding of common types of online threats reveals a significant aspect of digital literacy and security awareness. The present study delves into this domain, aiming to gauge the knowledge and awareness of students regarding online threats. Furthermore, this exploration aims to provide an input for further analysis on user satisfaction with the use of e-Learning tools. Figure 2 shows the distribution of answers grouped by five categories of answers: very good, good, neutral, week, very week.

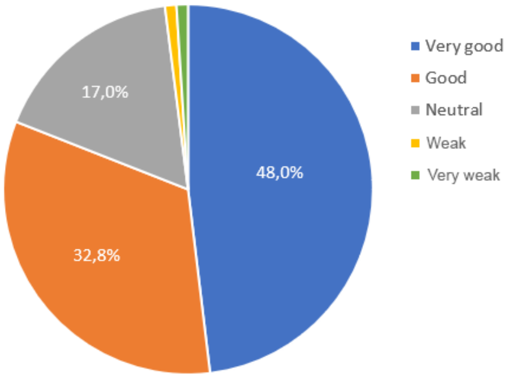

Figure 2. Level of understanding of online threats

Most students (48%) showed a strong comprehension of the mechanisms behind online threats, yet possessing limited knowledge on safeguarding against them. Subsequently, another segment of students (32.8%) asserted proficiency in both recognizing threats and understanding effective methods to protect against them simultaneously.

4.2.2 Consequences of the Security Incidents

The consequence most often mentioned by students was the "impossibility to attend the course." This indicates that more than half of the aspects mentioned by students (53) expressed the disruption of their ability to attend classes due to security incidents. The second most mentioned consequence was "data loss." A substantial number of students mentioned this as a serious issue resulting from security incidents. Data loss can involve coursework, research, and personal documents. Unauthorized access to personal data was another significant concern, being mentioned

32 times. This underscores the importance of privacy and data security.

Moreover, 29 students expressed concerns about the "inability to communicate with the teacher" because of security incidents. Effective communication with instructors is vital for learning, and disruptions in this area can hinder the educational experience. Table 5 presents the students' responses to question Q5 ordered in descending order of the frequency with which they were mentioned.

Table 5. The most serious consequences of cyber incidents perceived by students

Consequences	Frequency
Impossibility to attend the course	53
Data loss	37
Unauthorized access to personal data	32
Inability to communicate with the teacher	29
Identity theft	8
Inability to participate in the exam	6
Other consequences	10

4.2.3 Prevention of Cybersecurity Incidents

Students' responses to question Q7 showed that the duration of remediation for the effects of security incidents varied from one to 90 days, with an average of 13 days. The variability in the duration of remediating the effects of cybersecurity incidents is influenced by a combination of factors related to the incident itself, institutional response capabilities, and various procedural and logistical considerations. Table 6 shows the measures most frequently mentioned by students to prevent security incidents on e-learning platforms.

Table 6. Most mentioned measures to prevent security incidents

Prevention measures	Frequency
Improved Security	46
Two-Factor Authentication (2FA)	43
Data Encryption	39
User Training	35
Regular Audits and Monitoring	12
Collaboration and Partnerships	7
Custom e-Learning Platforms	7

Overall, these results indicated that a significant portion of students was either actively seeking or open to cybersecurity education. The pandemic appears to have played a significantly positive role in increasing awareness and participation in cybersecurity courses and training. The desire for education in this area is notable, reflecting the growing importance of cybersecurity in the digital age.

5. Extended Insight

In (Sarathchandra et al., 2016) a quantitative analysis is made regarding the implications for cybersecurity researchers and practitioners. It is important to see how security awareness was in the pre-pandemic period. The authors conducted a survey with 498 students in 2016. The survey was conducted on students spending time online, emphasizing how much time they spend per week. 80% of respondents could define some security terms, but only 50% could define the phishing attack. The results are presented in Table 7.

Table 7. Awareness of online vulnerabilities (Sarathchandra et al., 2016)

Term	Percent (%)
Overuse and Addiction	80.8
Identity theft	97
Hacking	95.4
Cyber Stalking	91
Cyber Bullying	98.7
Phishing	49.6
Malware	54.8
Trojan Horses	51.7
Viruses	89
Worms	17.3

In this analysis, the authors described the fact that students and pupils had greater fears regarding vulnerabilities that were not so important, perhaps even insignificant, but that were also presented in the news, and ignored the important vulnerabilities or the ones that could have dangerous or much more serious consequences.

In the present study, for the item "Please select your level of understanding of common types of online threats such as malware and phishing", 48% of students answered that they had a good knowledge about malware and phishing and 32% answered that they had a very good knowledge of these vulnerabilities. So, it can be observed that the awareness and information regarding the common vulnerabilities increased in this period.

Only 17% of students answered that they knew about these vulnerabilities, but they didn't know how to protect against them, while the rest of students answered that they had no information about these types of vulnerabilities.

Another study that evaluates awareness in the pre-pandemic period is (Khalid, et al., 2018). This study shows that the students even if they have a high awareness for the security, they have a lack of information for self-protection.

Compared with the pre-pandemic period, in the present study it can be find out that, in the post-pandemic period, the students are now much more aware of the threats present in the online environment, especially of the vulnerabilities of educational platforms.

This awareness grew not only for the students, but also for the specialists in the domain. In Figure 1, it could be seen that how the numbers of common vulnerabilities and exploits grew in 2020 for e-Learning field.

In the present analysis, the trust in five e-Learning platforms (Zoom, Microsoft Teams, Google Classroom, Moodle and Webex) has been calculated, as it could be seen in Table 4. Now, the number of CVEs for four of these platforms is analised. Figure 3 illustrates the evolution of the identified vulnerabilities for these four platforms, in the period 2016-2023, which includes the pre-pandemic, the pandemic and the post-pandemic periods.

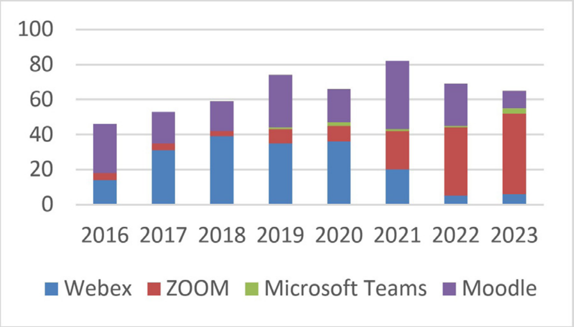

Figure 3. CVEs for e-Learning platforms (CVE, 2023)

6. Conclusion and Future Work

The results of this study show that students generally consider cybersecurity and the protection of personal information to be quite important. They also have a moderate level of confidence in managing cybersecurity incidents. Additionally, while there is a consensus on the importance of software updates and security patch management, there may be some variability in the strength of agreement. Finally, the present study demonstrates that students don't feel that their privacy is strongly violated during online activities. These findings can be valuable for educational institutions in shaping their cybersecurity and e-learning policies.

The analysis of students' trust in e-Learning platforms also reveals several insights. Zoom emerges as the most trusted platform, with students showing a high level of trust. Microsoft Teams and Google Classroom receive moderate trust levels, with some variability in trust among students. Moodle and Webex also have moderate trust levels, with some variation in students' trust perceptions.

The qualitative analysis highlights diverse and significant concerns of students regarding the consequences of security incidents. The most prevalent worries are related to disruptions in attending classes and data loss, emphasizing the importance of maintaining uninterrupted access to educational resources and safeguarding data. Privacy issues, communication challenges, and identity theft are also notable concerns. Educational institutions should use these insights to strengthen their cybersecurity measures and support students in mitigating the potential impact of security incidents on their learning experiences.

The overwhelming support for the existence of a security guide with recommendations reflects a shared recognition of the importance of cybersecurity in e-Learning and a willingness to embrace proactive measures to enhance security. The small number of disagreements suggests that there may be room for tailoring security resources to better meet the needs and concerns of all students, ensuring that the guide is not only present, but also effective in addressing security challenges.

As the findings illustrated within this paper indicate the paramount importance of ensuring robust cybersecurity measures to safeguard online educational platforms and the results of the survey highlight that a significant number of students acknowledge the potential threats and vulnerabilities present in e-Learning environments, it has become quite obvious that the study underscores the pressing need for educational institutions and policymakers to implement comprehensive cybersecurity strategies in order to protect sensitive data, preserve privacy, and maintain the integrity of online learning platforms. Importantly, the authors plan future research that could delve into exploring effective methods for educating students about cybersecurity best practices and enhance their understanding of potential risks. Additionally, further investigation into specific technological solutions and policies to strengthen cybersecurity infrastructure in e-Learning settings can be pursued to facilitate secure and seamless educational experiences for students. Moreover, these undertakings could mean a subtle refinement of the survey instrument and the publication of a best practice guide that could, perhaps, serve as guidance for stakeholders in search of safe online learning.

Acknowledgments

The research reported in this paper has been supported by the project entitled "Advanced research based on emerging and disruptive technologies – support for the society of the future – FUTURE TECH" (funded by the Romanian Core Program within the National Research Development and Innovation Plan 2022-2027 of the Ministry of Research and Innovation), project no 23380601.

REFERENCES

Al Shabibi, A. M. & Al-Suqri, M. N. (2023) Cybersecurity Awareness Among Students During the COVID-19 Digital Transformation of Education: A Case Study at the Muscat (Oman) Schools. In: Al Naimiy, H. M. K., Bettayeb, M., Elmehdi, H. M. & Shehadi, I. (eds.) *SHJEDU 2022: Future Trends in Education Post COVID-19*. Singapore, Springer, pp. 39–51. doi: 10.1007/978-981-99-1927-7_4.

Anghel, M. & Pereţeanu, G. C. (2020) Cyber security approaches in e-Learning. In: *Proceedings of the 14th International Technology, Education and Development Conference*, *2-4 March 2020, Valencia, Spain*. pp. 4820-4825. doi: 10.21125/inted.2020.1323.

Awan, R. K., Afshan, G. & Memon, A. B. (2021) Adoption of E-Learning at Higher Education Institutions: A Systematic Literature Review. *Multidisciplinary Journal for Education, Social and Technological Sciences*. 8(2), 74. doi: 10.4995/muse.2021.15813.

Barbu, M., Zamfiroiu, A., Marinescu, I. A. & Iordache, D. (2022) Cybersecurity in e-Learning During the COVID-19 Pandemic. In: *5th International Open and Distance Learning Conference Proceedings Book*, *28-30 September 2022, Anadolu University, Turkey*. pp. 165-174.

Bezhovski, Z. & Poorani, S. (2016) The Evolution of E-Learning and New Trends. *Information and Knowledge Management*. 6(3), 50-57.

Breaz, T., Fülöp, M. & Cioca, L. I. (2022) The role of E-Learning generated by the COVID-19 epidemic in higher education. *International Journal of Computers, Communications & Control (IJCCC)*. 17(5), 4854. doi: 10.15837/ijccc.2022.5.4854.

Cision. (2022) *E-Learning Market Size*. https://www.prnewswire.com/news-releases/e-learning-market-size-surpassed-315-billion-in-2021-and-projected-to-hit-20-cagr-from-2022-to-2028-301610252.html [Accessed 16th October 2023].

Common Vulnerabilities and Exposures (CVE). (2023) *CVE List*. https://cve.mitre.org/ [Accessed 16th October 2023].

Dhawan, S. (2020) Online Learning: A Panacea in the Time of COVID-19 Crisis. *Journal of Educational Technology Systems*. 49(1), 5-22. doi: 10.1177/0047239520934018.

Facts & Factors. (2023) *E-Learning Market Size, Share & Growth Analysis Report 2022-2030*. https://www.fnfresearch.com/e-learning-market [Accessed 16th October 2023].

Fauzi, M. A. (2022) E-learning in higher education institutions during COVID-19 pandemic: current and future trends through bibliometric analysis. *Heliyon*. 8(5), e09433. doi: 10.1016/j.heliyon.2022.e09433.

Franco, E. G. (2020) *The Global Risks Report 2020*. World Economic Forum, Geneva, Switzerland. Report number: 15. https://www.weforum.org/reports/the-global-risks-report-2020/ [Accessed 15th October 2023].

Garba, A., Sirat, M., Othman, S. & Dauda, I. (2020). Cyber Security Awareness Among University Students: A Case Study. *Science Proceedings Series*. 2(1), 82–86. doi: 10.31580/sps.v2i1.1320.

Gehem, M., Usanov, A., Frinking, E. & Rademaker, M. (2015) *Assessing Cyber Security: A Meta-*

Analysis of Threats, Trends, and Responses to Cyber-Attacks. The Hague, Netherlands, Hague Centre for Strategic Studies.

Global Market Insights (GMI) (2023) *E-learning industry analysis*. https://www.gminsights.com/industry-analysis/elearning-market-size [Accessed 16th October 2023].

Hunt, T. (2016) *Cyber security awareness in higher education*. Thesis. Central Washington University, pp. 1–14.

Iordache, D. D. & Barbu, M. (2021) Comparative analysis of three e-Learning platforms used by students during the COVID-19 pandemic. *Revista Română de Informatică și Automatică [Romanian Journal of Information Technology and Automatic Control]*. 31(4), 55-66. doi: 10.33436/v31i4y202105.

Khalid, F., Daud, M. Y., Rahman, M. J. A. & Nasir, M. K. M. (2018) An investigation of university students' awareness on cyber security. *International Journal of Engineering & Technology*. 7(421), 11-14. doi: 10.14419/ijet.v7i4.21.21607.

Koohang, A., Nowak, A., Paliszkiewicz, J. & Nord, J. H. (2020) Information security policy compliance: Leadership, trust, role values, and awareness. *Journal of Computer Information Systems*. 60(1), 1–8. doi: 10.1080/08874417.2019.1668738.

Leu, D. M., Udroiu, C., Raicu, G. M., Gârban, H. N. & Șcheau, M. C. (2023) Analysis of some case studies on cyberattacks and proposed methods for preventing them. *Revista Română de Informatică și Automatică [Romanian Journal of Information Technology and Automatic Control]*. 33(2), 119-134. doi: 10.33436/v33i2y202309.

Maatuk, A. M., Elberkawi, E. K., Aljawarneh, S., Rashaideh, H. & Alharbi, H. (2022) The COVID-19 pandemic and E-learning: challenges and opportunities from the perspective of students and instructors. *Journal of Computing in Higher Education*. 34(1), 21-38. doi: 10.1007/s12528-021-09274-2.

Moallem, A. (2018) Cyber Security Awareness Among College Students. In: Ahram, T. & Nicholson, D. (eds.) *Advances in Human Factors in Cybersecurity. AHFE 2018. Advances in Intelligent Systems and Computing, vol 782*. Cham, Springer, pp. 79–87. doi: 10.1007/978-3-319-94782-2_8.

Najm, Y. A., Alsamaraee, S. & Jalal, A. A. (2022) Cloud computing security for e-learning during COVID-19 pandemic. *Indonesian Journal of Electrical Engineering and Computer Science*. 27(3), 1610-1618. doi: 10.11591/ijeecs.v27.i3.pp1610-1618.

Raju, R., Abd Rahman, N. H. & Ahmad, A. (2022) Cyber Security Awareness in Using Digital Platforms among Students in a Higher Learning Institution. *Asian Journal of University Education*. 18(3), 756-766.

Sarathchandra, D., Haltinner, K. & Lichtenberg, N. (2016) College students' cybersecurity risk perceptions, awareness, and practices. In: *2016 Cybersecurity Symposium (CYBERSEC), 18-20 April 2016, Coeur d'Alene, ID, USA*. pp. 68-73. doi: 10.1109/CYBERSEC.2016.018.

Statista. (2022) *Global e-learning market size by segment 2019 with a forecast for 2026*. https://www.statista.com/statistics/1130331/e-learning-market-size-segment-worldwide/ [Accessed 16th October 2023].

United Nations Educational, Scientific and Cultural Organization (UNESCO). (2020) *1.3 billion learners are still affected by school or university closures*. https://www.unesco.org/en/articles/13-billion-learners-are-still-affected-school-or-university-closures-educational-institutions-start [Accessed 16th October 2023].

Vevera, A. V., Cîrnu, C. A. & Radulescu, C. Z. (2022) A Multi-Attribute Approach for Cyber Threat Intelligence Product and Services Selection. *Studies in Informatics and Control*. 31(1), 13-23. doi: 10.24846/v31i1y202202.

Zamfiroiu, A., Boncea, R., Petre, I. & Voicu, S. (2023) Vulnerabilities of Mobile Applications Used in Distance Learning Environment. In: Mafalda Carmo, M. (ed.) *Proceedings of END – Education Conference, vol. 2, 24-26 June 2023, Lisbon, Portugal*. pp. 13-17. doi: 10.36315/2023v2end003.

Zamfiroiu, A., Sharma, R. C., Constantinescu, D., Pană, M. & Toma, C. (2022) Using Learning Analytics for Analyzing Students' Behavior in Online Learning. *Studies in Informatics and Control*. 31(3), 63-74. doi: 10.24846/v31i3y202206.

Zhang-Kennedy, L. & Chiasson, S. (2021) A systematic review of multimedia tools for cybersecurity awareness and education. *ACM Computing Surveys (CSUR)*. 54(1), 1-39. doi: 10.1145/3427920.