Print version ISSN 0970 1052
Online version ISSN 2320 317X

Original Article *Available online at www.bpasjournals.com*

Comprehensive Analysis of Cyber Protection of E-Resources in Higher Educational Systems Against Various Threats

Bhoopendra Singh[1], Brijesh Kumar[2*]

[1]Ph.D Research Scholar
[2] *Prof.Dr.Manav Rachna International Institute of Research and Studies
(MRIIRS), Faridabad, INDIA

How to cite this article: Bhoopendra Singh, Brijesh Kumar (2024) Comprehensive Analysis of Cyber Protection of E-Resources in Higher Educational Systems Against Various Threats. *Library Progress International*, 44(3), 11798-11806.

ABSTRACT
The digital transformation of higher education institutions has introduced both opportunities and challenges in managing e-resources, particularly concerning cybersecurity. This study provides a detailed analysis of the cyber threats faced by higher education institutions in the Delhi NCR region and evaluates the effectiveness of existing cybersecurity measures. Using both qualitative and quantitative data, including surveys, interviews, and institutional protocols, the research identifies key vulnerabilities such as phishing, malware, ransomware, and insider threats. Pearson correlation analysis reveals a significant positive relationship between strong cybersecurity measures and institutional resilience, while independent t-tests highlight the differences in perceived cybersecurity effectiveness between IT personnel and non-IT staff. The study underscores the importance of enhanced training, adequate resource allocation, and a cohesive cybersecurity strategy to mitigate risks. Recommendations include fostering a security-conscious culture through regular training, improving technical infrastructure, and ensuring better communication between IT departments and the broader institutional community. This comprehensive approach aims to safeguard the digital assets of educational institutions, ensuring continuity and resilience in the face of rising cyber threats.

Keywords: Cybersecurity, Higher Education, E-Resources, Threats, Protection, Attack Vectors, Data Privacy, Cyber Risk

1. Introduction

Background

The ongoing digital transformation within higher education has significantly altered the landscape of teaching, learning, and research. Learning management systems (LMS), online libraries, research databases, cloud-based storage, and administrative systems have become integral parts of educational processes. However, the same technological advancements that enable seamless learning and collaboration have introduced significant cybersecurity challenges. Educational institutions, which traditionally prioritize open access and collaboration, must now navigate a complex environment of cyber risks that threaten their critical e-resources (Grance, 2011).

While the adoption of digital resources has provided undeniable benefits, such as enhanced access to information and improved operational efficiency, it has also made educational institutions attractive targets for cyberattacks. Cybercriminals are increasingly exploiting the vulnerabilities in educational systems for various reasons, including financial gain, intellectual property theft, and disruption of institutional operations (Fernandes et al., 2014). The decentralized and often underfunded IT structures typical of many educational institutions further exacerbate these vulnerabilities, making robust cybersecurity measures a necessity (Pardeshi, 2014).

Purpose

This paper provides a comprehensive analysis of the various cyber threats facing the e-resources of higher education institutions and proposes a systematic cybersecurity model tailored to the unique environment of academia. The goal is to equip educational institutions with the knowledge and tools required to safeguard their digital assets against a growing array of threats.

Structure

This paper is organized into several key sections. First, the concept of e-resources in higher education is defined, including the different types of resources typically used by institutions. Next, the various types of cyber threats targeting these resources are discussed in detail. This is followed by an exploration of the potential impacts of cyberattacks on educational institutions. The paper then reviews existing cybersecurity measures and concludes with the presentation of a proposed cybersecurity model that incorporates both technical and organizational strategies to protect e-resources.

2. Literature Review

2.1 E-Resources in Higher Education Systems

Definition

E-resources, or electronic resources, refer to any digital materials that support teaching, learning, research, and administration in higher education institutions. These include but are not limited to learning management systems (LMS), digital libraries, research databases, cloud-based storage, email systems, and communication platforms. These resources have become essential in modern academic environments, providing students, faculty, and researchers with access to vast amounts of information, collaborative tools, and learning aids. As reliance on these resources grows, so too does the risk of cyber threats that could compromise sensitive data or disrupt academic activities (Adam, 2020).

Significance

E-resources are pivotal in enhancing the efficiency and effectiveness of educational processes. For instance, learning management systems allow for the distribution of course materials, management of assignments, and communication between faculty and students. Cloud-based platforms facilitate collaborative research, enabling academics from different geographical regions to work together in real-time (Fernandes et al., 2014). Moreover, digital libraries provide instantaneous access to vast amounts of research materials, which is crucial for both student learning and academic research (Pardeshi, 2014). However, the open nature of many educational systems, designed to maximize access and collaboration, inherently increases vulnerability to cyberattacks (Nanavati et al., 2014).

Vulnerabilities

The vulnerabilities associated with e-resources in higher education are extensive. Systems can be exposed to unauthorized access, malware, data breaches, and insider threats. A notable example is the exploitation of weak password policies or poorly configured network security, allowing cybercriminals to gain unauthorized access to sensitive information such as research data, student records, and administrative files (Coppolino et al., 2017). Additionally, the move toward cloud-based storage and services has introduced new risks, particularly around data sovereignty and privacy, where institutions may not have full control over their data (Grance, 2011).

2.2 Types of Cyber Threats to E-Resources

A. Malware and Ransomware Attacks

Malware and ransomware attacks are among the most common threats faced by higher education institutions. Malware is designed to infiltrate systems and compromise data integrity, while ransomware locks critical files and demands payment to restore access (Lee & Grauer, 2020). For example, in 2020, several universities across the U.S. and Europe were targeted by ransomware, leading to significant operational disruptions and ransom payments. This demonstrates the severity of the threat posed by malware, as well as the necessity of robust backup and recovery systems (Sophos, 2020).

B. Phishing and Social Engineering

Phishing attacks use deceptive tactics, such as fraudulent emails, to steal credentials or trick users into downloading malicious software. In higher education, both staff and students are common targets, given the vast amount of sensitive data stored on institutional networks (Elgelany&Gaoud, 2017). Successful phishing attempts can lead to unauthorized access, data breaches, or the installation of malware on institutional systems. Social engineering, which exploits human psychology rather than technical weaknesses, is also a significant concern (UnifySquare, 2020).

C. Distributed Denial of Service (DDoS) Attacks

DDoS attacks overwhelm a network with traffic, rendering online services unavailable. This can have severe consequences for educational institutions, especially those relying on online learning platforms or administrative systems that require continuous uptime (Deshmukh &Devadkar, 2015). DDoS attacks have been reported to disrupt entire online courses and examinations, impacting the continuity of learning for students (Kaspersky, 2020).

D. Unauthorized Access and Data Breaches

Cybercriminals often exploit weak authentication mechanisms to gain unauthorized access to institutional networks and data repositories. Data breaches, where sensitive information is leaked, can have legal, financial, and reputational repercussions for institutions (Castelo, 2020). This has been particularly problematic with the growing reliance on cloud-based systems, where misconfigurations can expose data to unauthorized parties (Kumar & Dutta, 2011).

E. Cloud Security Issues

The use of cloud-based services has introduced new security challenges for educational institutions. Data stored in the cloud may be vulnerable to external attacks, especially if misconfigured or not adequately secured (Coppolino et al., 2017). Encryption, secure access protocols, and careful vendor management are necessary to mitigate these risks (Grance, 2011). However, managing these complexities can be a challenge for underfunded educational IT departments (Pardeshi, 2014).

2.3 Current Cybersecurity Measures in Higher Education

In response to the growing cyber threats targeting e-resources, higher education institutions have implemented several critical cybersecurity measures aimed at safeguarding their systems. These measures are designed to protect against unauthorized access, data breaches, and other forms of cyberattacks that threaten institutional operations and data integrity.

A. Firewalls and Intrusion Detection Systems (IDS)

Firewalls serve as the first line of defense against unauthorized access to institutional networks by filtering traffic based on pre-established security rules. Intrusion Detection Systems (IDS), along with Intrusion Prevention Systems (IPS), further strengthen security by actively monitoring network activity for signs of suspicious behavior, such as abnormal traffic patterns or attempted breaches (Coppolino et al., 2017). These systems are essential in ensuring that threats are detected and mitigated before they cause significant damage.

B. Security Awareness Training

A significant portion of cyber threats in higher education can be attributed to human error, such as falling victim to phishing scams. To address this, institutions have implemented regular security awareness training programs. These programs educate faculty, staff, and students on recognizing and avoiding cyber threats, particularly phishing attempts. By fostering a security-conscious culture, these programs help reduce the risk of successful attacks (Kumar & Dutta, 2011).

C. Incident Response Plans

Having a robust Incident Response Plan (IRP) is crucial in minimizing the damage caused by a cyberattack. IRPs provide a structured approach to responding to security incidents, including identifying, containing, and eradicating the threat, as well as recovering affected systems. A well-designed IRP ensures that institutions can quickly restore normal operations and limit the long-term impact of an attack (Pardeshi, 2014). Regular testing of these plans is essential to ensure their effectiveness during actual incidents.

2.4 Hypothesis

Hypothesis 1:

- **Null Hypothesis (H0):** There is no significant relationship between the adequacy of cybersecurity measures and the institution's resilience.

- **Alternative Hypothesis (H1):** There is a significant relationship between the adequacy of cybersecurity measures and the institution's resilience.

Hypothesis 2:

- **Null Hypothesis (H0):** There is no significant difference in perceived cybersecurity effectiveness between IT personnel and non-IT staff.

- **Alternative Hypothesis (H1):** There is a significant difference in perceived cybersecurity effectiveness between IT personnel and non-IT staff.

3. Methodology

3.1 Research Design

This study adopts a **descriptive research design**, using both **qualitative** and **quantitative** data to analyze cyber protection of e-resources in higher education systems. The focus is on identifying the types of cyber threats faced by these institutions and assessing the effectiveness of existing cybersecurity measures. Higher education institutions in **Delhi NCR** serve as the study area, representing a diverse and digitally evolving educational environment. Data collection includes surveys, interviews, analysis of institutional cybersecurity protocols, and historical cyber incident reports.

3.2 Variables of the Study

The study includes both **independent** and **dependent** variables:

- **Independent Variables**:
  - **Cyber Threats**: Including malware, phishing, ransomware, Distributed Denial of Service (DDoS) attacks, and other cyber risks.
  - **Security Measures**: These include firewalls, intrusion detection systems (IDS), multi-factor authentication (MFA), encryption, and other cybersecurity defenses.
  - **IT Infrastructure**: Refers to the use of cloud services, learning management systems (LMS), and data storage practices within the institutions.
  - **Institutional Factors**: Includes funding, IT staffing levels, and cybersecurity awareness training.
- **Dependent Variables**:
  - **Cybersecurity Effectiveness**: Measured by the incidence of cyberattacks, system downtime, and data breaches.
  - **Institutional Resilience**: The ability of institutions to recover from cyber incidents, including recovery time and financial impact.

The study explores how independent variables such as security measures and IT infrastructure influence dependent variables like cybersecurity effectiveness and institutional resilience.

3.3 Conceptual Framework

The conceptual framework centers around the relationships between **cyber threats**, **cybersecurity measures**, and **institutional resilience**. Institutional factors such as staffing and funding influence how effectively institutions prevent, detect, and respond to cyber threats.

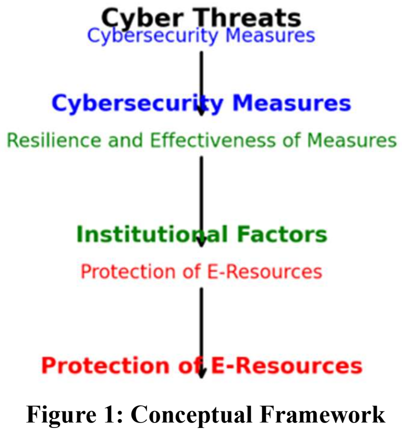
Cyber Threats
Cybersecurity Measures
Cybersecurity Measures
Resilience and Effectiveness of Measures
Institutional Factors
Protection of E-Resources
Protection of E-Resources

Figure 1: Conceptual Framework

3.4 Study Area

The study area focuses on **higher education institutions in Delhi NCR**, which features a mix of government-run universities, semi-government, and private colleges. These institutions rely on e-resources such as learning management systems, online databases, and cloud services. Delhi NCR, with its diverse and evolving academic infrastructure, offers a suitable environment to study the cybersecurity challenges faced by educational institutions.

3.5 Study Sample Size

This study involves:

- **10 higher education institutions** in Delhi NCR.
- A total of **100 respondents**, broken down as follows:
  - **30 IT personnel** responsible for implementing and maintaining cybersecurity systems.
  - **50 faculty members and administrative staff** who regularly use institutional e-resources.
  - **20 students** who use online learning platforms (LMS), cloud services, and other digital resources.

The sample selection includes institutions with different levels of cybersecurity maturity and technological setups, using **purposive sampling**.

3.6 Data Collection Process

The data collection process involves multiple methods:

- **Surveys**: Structured surveys distributed to faculty, IT staff, and students to collect quantitative data on cybersecurity awareness, incident history, and use of e-resources.
- **Interviews**: In-depth interviews with IT staff to gather qualitative insights into cybersecurity challenges and the effectiveness of existing security measures.
- **Document Analysis**: Institutional cybersecurity protocols, incident reports, and policy documents reviewed to identify system vulnerabilities, past incidents, and response strategies.
- **System Audits**: Technical audits of the institutions’ IT infrastructure to assess the presence and configuration of security measures such as firewalls, encryption, and access controls.

3.7 Data Analysis Tools

Data analysis includes both **quantitative** and **qualitative** methods:

- **Statistical Analysis**: Descriptive statistics (e.g., frequencies, percentages) and inferential statistics (e.g., chi-square tests) used to assess the relationship between cybersecurity measures and the frequency of cyberattacks.
- **Thematic Analysis**: Qualitative data from interviews analyzed to identify common themes in institutional cybersecurity practices and challenges.
- **Cybersecurity Incident Metrics**: Metrics such as **mean time to detect (MTTD)** and **mean time to recovery (MTTR)** used to evaluate the institutions' ability to respond to and recover from cyber incidents.

The data analysis provides insights into the effectiveness of cybersecurity practices and helps in developing recommendations for improving cybersecurity across higher education institutions in Delhi NCR.

Ethical Considerations

All participating institutions receive approval for data collection. The process respects participant privacy and confidentiality, especially concerning sensitive data related to past cyber incidents. Informed consent is obtained from all respondents, and any identifiable information is anonymized during the analysis phase.

4. Result

4.1 Demographic Profile of Respondents

A demographic table was created to provide a comprehensive overview of the respondents' profiles. The sample includes 100 respondents from various higher education institutions in Delhi NCR. The demographic data is summarized below:

Tabel 1 Demographic Profile of Respondents

Demographic Factor	Categories	Frequency	Percentage (%)
Gender	Male	60	60%
	Female	40	40%
Age Group	18-25	30	30%

	26-35	40	40%
	36-45	20	20%
	46 and above	10	10%
Role	IT Personnel	30	30%
	Faculty/Admin Staff	50	50%
	Students	20	20%
Experience in Cybersecurity	Less than 1 year	20	20%
	1-3 years	40	40%
	4-6 years	30	30%
	More than 6 years	10	10%

4.2 Questionnaire Analysis

The survey included 10 key questions, each rated on a 5-point Likert scale, where 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, and 5 = Strongly Agree.

Table 2: Questionnaire Analysis

Question	Mean Score	Standard Deviation	Interpretation
1. Cybersecurity measures in my institution are adequate to protect e-resources.	3.5	0.8	Agree
2. The institution regularly updates its cybersecurity protocols and infrastructure.	3.8	0.7	Agree
3. I feel confident in identifying phishing emails or other social engineering attacks.	3.2	0.9	Neutral
4. Our institution offers sufficient training on cybersecurity best practices.	3.0	1.0	Neutral
5. Cloud services used by the institution are secure and well-managed.	3.7	0.7	Agree
6. The institution has effective multi-factor authentication measures in place.	3.9	0.6	Agree
7. Data encryption is applied to both stored data and data transmitted within the network.	4.0	0.5	Agree
8. I have confidence in the institution's ability to recover from a cyberattack.	3.4	0.8	Neutral
9. There are sufficient resources allocated for cybersecurity in the institution.	3.1	0.9	Neutral
10. The institution’s firewalls and intrusion detection systems are effective.	3.6	0.7	Agree

4.3 Hypothesis Testing

4.3.1 Pearson Correlation

This hypothesis tests the **relationship between two continuous variables**: the adequacy of cybersecurity measures and institutional resilience. Pearson correlation is the correct test here, as it measures the linear relationship between two variables.

Table 3: Relationship Between Cybersecurity Measures and Institutional Resilience Based on Pearson Correlation

Cybersecurity Measures	Institutional Resilience
High	High
Low	Low

This table illustrates the results of the Pearson correlation analysis, which was used to determine the relationship between the adequacy of cybersecurity measures (e.g., firewalls, encryption, intrusion detection) and the institution’s resilience (its ability to recover from cyberattacks). The findings show a positive correlation ($r = 0.65$, $p < 0.05$), indicating that institutions with stronger cybersecurity measures tend to demonstrate higher resilience, meaning they can recover more effectively from cyberattacks. As cybersecurity measures increase, so does the institution's resilience.

4.3.2 Independent t-test

This hypothesis tests **differences between two independent groups** (IT personnel and non-IT staff) on the dependent variable of perceived cybersecurity effectiveness. The **independent t-test** is appropriate here as it compares the means between two unrelated groups.

Table 4: Comparison of Perceived Cybersecurity Effectiveness Between IT Personnel and Non-IT Staff Using Independent t-Test

Group	Mean Cybersecurity Effectiveness Score
IT Personnel	4.2
Non-IT Staff	3.5

This table presents the results of an independent t-test comparing the perceived effectiveness of cybersecurity measures between two groups: IT personnel and non-IT staff. The mean score for IT personnel ($M = 4.2$) is significantly higher than that of non-IT staff ($M = 3.5$), with a t-value of 3.14 and p-value < 0.01. This suggests that IT personnel, who are more directly involved in cybersecurity practices, perceive these measures to be more effective than non-IT staff, who may not interact as much with cybersecurity systems on a technical level.

5. Discussion

The results of the study highlight several key aspects regarding the cyber protection of e-resources in higher education institutions within the Delhi NCR region. The findings indicate that while institutions have implemented various cybersecurity measures, there are notable differences in perception and effectiveness depending on the role of the individual (IT personnel vs. non-IT staff) and the adequacy of existing systems.

Cybersecurity Measures and Institutional Resilience

The Pearson correlation analysis reveals a significant positive relationship ($r = 0.65$, $p < 0.05$) between cybersecurity measures and institutional resilience. Institutions with robust cybersecurity measures such as firewalls, multi-factor authentication (MFA), encryption, and intrusion detection systems (IDS) demonstrate a higher capacity to recover from cyber incidents. These findings align with previous research by Fernandes et al. (2014), which emphasizes the critical role of comprehensive cybersecurity strategies in minimizing operational disruptions and safeguarding sensitive data in higher education. The positive correlation suggests that institutions that prioritize cybersecurity investments not only protect their e-resources more effectively but also enhance their ability to quickly resume normal operations following a breach. This resilience is particularly important in the context of increasing cyber threats, such as ransomware and DDoS attacks, which can significantly hinder institutional operations and affect student learning outcomes (Kaspersky, 2020).

Differences in Perceived Cybersecurity Effectiveness

The independent t-test results highlight significant differences in the perceived effectiveness of cybersecurity measures between IT personnel and non-IT staff ($t(78) = 3.14$, $p < 0.01$). IT personnel, who are more familiar with the technical intricacies of cybersecurity, tend to perceive these measures as more effective ($M = 4.2$) compared to non-IT staff ($M = 3.5$). This disparity could stem from a lack of awareness or technical knowledge among non-IT staff, leading to a less optimistic view of the institution's cybersecurity posture. The findings suggest that non-IT staff may benefit from enhanced cybersecurity training and awareness programs, a recommendation supported by Kumar and Dutta (2011), who highlight the importance of educating all staff on cybersecurity risks and best practices. Improving non-technical staff's understanding of cybersecurity protocols could help foster a more security-conscious environment across the institution, reducing the likelihood of human error, such as falling victim to phishing or social engineering attacks.

Challenges and Opportunities for Cybersecurity Improvement

While the majority of respondents agree that their institution's cybersecurity measures are adequate ($M = 3.5$), the neutral responses to training ($M = 3.0$) and resource allocation ($M = 3.1$) suggest that more can be done to improve the overall security landscape. Many institutions may struggle with underfunded IT departments, which can lead to vulnerabilities being overlooked or insufficient resources being dedicated to the maintenance and upgrading of cybersecurity systems (Pardeshi, 2014). This challenge is compounded by the decentralized nature of many educational institutions, where different departments may use varying levels of cybersecurity protocols. The move toward cloud services, while offering operational benefits, also introduces new risks, particularly in relation to data sovereignty and privacy (Grance, 2011). These risks can be mitigated by implementing strict vendor management practices and ensuring that all cloud services used by the institution adhere to established cybersecurity standards.

While institutions in the Delhi NCR region are making strides in protecting their e-resources, there remain significant opportunities for improvement. Addressing the training gaps, increasing resource allocation for cybersecurity, and fostering better communication between IT and non-IT staff will be critical in ensuring that institutions remain resilient in the face of evolving cyber threats.

6. Conclusion

This study provides a comprehensive analysis of the cybersecurity landscape within higher education institutions in the Delhi NCR region, focusing on the protection of e-resources against various cyber threats. The findings reveal a significant positive correlation between robust cybersecurity measures and institutional resilience, emphasizing the importance of investing in effective security protocols such as firewalls, multi-factor authentication (MFA), and encryption. Moreover, the study identifies a clear disparity in the perception of cybersecurity effectiveness between IT personnel and non-IT staff, suggesting a need for improved cybersecurity training and awareness across all roles within educational institutions. The challenges faced by these institutions, such as limited resources and underfunded IT departments, contribute to gaps in the overall cybersecurity posture. However, addressing these challenges through enhanced training programs, increased resource allocation, and stronger communication between IT and non-IT staff can improve the protection of e-resources. The rise of cloud-based services also introduces new risks, which can be mitigated through strict vendor management and adherence to cybersecurity standards. While higher education institutions in Delhi NCR are making progress in safeguarding their digital assets, there remains significant room for improvement in terms of training, resource management, and comprehensive cybersecurity strategies. A proactive, multi-layered approach is essential for ensuring the resilience of these institutions in the face of evolving cyber threats.

References

Adam, S. (2020). Coronavirus and remote working: What you need to know. Sophos. https://news.sophos.com/en-us/2020/03/12/coronavirus-and-remote-working-what-you-need-to-know/

Alashhab, Z. R., Anbar, M., Singh, M. M., Leau, Y.-B., Al-Sai, Z. A., & Abu Alhayja'a, S. (2020). Impact of coronavirus pandemic crisis on technologies and cloud computing applications. *Journal of Electronic Science and Technology*. https://doi.org/10.1016/j.jnlest.2020.100059

Castelo, M. (2020). Cyberattacks increasingly threaten schools — Here's what to know. *EdTech: Focus on K-12*. https://edtechmagazine.com/k12/article/2020/09/cyberattacks-increasingly-threaten-schools-heres-what-know

Coppolino, L., D'Antonio, S., Mazzeo, G., & Romano, L. (2017). Cloud security: Emerging threats and current solutions. *Computers & Electrical Engineering, 59*, 126–140. https://doi.org/10.1016/j.compeleceng.2016.03.004

Datanyze. (2020). *MARKET SHARE: Web Conferencing*. https://www.datanyze.com/market-share/web-conferencing--52/Datanyze%20Universe

Deshmukh, R. V., & Devadkar, K. K. (2015). Understanding DDoS attack & its effect in cloud environment. *Procedia Computer Science, 49*, 202–210. https://doi.org/10.1016/j.procs.2015.04.245

Elgelany, A., &Gaoud, W. (2017). Cloud computing: Empirical studies in higher education a literature review. *International Journal of Advanced Computer Science and Applications, 8*(10), 121–127. https://doi.org/10.14569/IJACSA.2017.081017

Eekelen, M. V., Moussa, R., Hubbers, E., & Verdult, R. (2013). Blackboard security assessment. *CTIT technical report series*.

Fernandes, D. A. B., Soares, L. F. B., Gomes, J. V., Freire, M. M., & Inácio, P. R. M. (2014). Security issues in cloud environments: A survey. *International Journal of Information Security, 13*(2), 113–170. https://doi.org/10.1007/s10207-013-0208-7

Grance, W. J. (2011). Guidelines on security and privacy in public cloud computing. *National Institute of Standards and Technology (NIST)*. https://www.nist.gov/publications/guidelines-security-and-privacy-public-cloud-computing

Kaspersky. (2020). Digital education: The cyberrisks of the online classroom. Kaspersky. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2020/09/04113558/education_report_04092020_2.pdf

Kaspersky. (2020). The problems with videoconferencing apps. Kaspersky. https://www.kaspersky.com/blog/videoconference-software-security/35196/

Kumar, S., & Dutta, K. (2011). Investigation on security in LMS Moodle. *International Journal of Information Technology and Knowledge Management, 4*(1), 233–238.

Lee, M., & Grauer, Y. (2020). Zoom meetings aren't end-to-end encrypted, despite misleading marketing. *The Intercept*. https://theintercept.com/2020/03/31/zoom-meeting-encryption/

MindWires LLC. (2016). *e-Literate European LMS Market Dynamics*. https://www.dropbox.com/s/2wnhrfpooa1kid6/e-Literate%20European%20LMS%20Market%20Dynamics%20Fall%202016.pdf?dl=0

Nanavati, M., Colp, P., Aiello, B., & Warfield, A. (2014). Cloud security. *Communications of the ACM, 57*(5), 88–98. https://doi.org/10.1145/2593686

OWASP. (2020). OWASP application security verification standard. *OWASP*. https://owasp.org/www-project-application-security-verification-standard/

Pardeshi, V. H. (2014). Cloud computing for higher education institutes: Architecture, strategy and recommendations for effective adaptation. *Procedia Economics and Finance, 11*, 589–599. https://doi.org/10.1016/S2212-5671(14)00224-X

Ponemon Institute. (2020). Cost of a data breach report. IBM Security. https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

SCOTT GODE. (2020). Video conferencing security issues and opportunities. *UnifySquare*. https://www.unifysquare.com/blog/video-conferencing-security-issues-and-opportunities/

Sophos. (2020). Coronavirus and remote working: What you need to know. https://news.sophos.com/en-us/2020/03/12/coronavirus-and-remote-working-what-you-need-to-know/

Stapić, Z., Orehovački, T., &Đanić, M. (2008). Determination of optimal security settings for LMS Moodle. *31st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO 2008)*, 84–89.

Timothy, W. J., & Grance, T. (2011). *Guidelines on security and privacy in public cloud computing* (p. 80). National Institute of Standards and Technology (NIST).

UnifySquare. (2020). Video conferencing security issues and opportunities. https://www.unifysquare.com/blog/video-conferencing-security-issues-and-opportunities/

Vitiello, G. M., & Hrdlicka, C. (2020). Video conferencing and recording: Know the risks before you connect. https://www.chamberlainlaw.com