AD EDUXIAN JOURNAL
A Quarterly Multidisciplinary Blind Peer Reviewed & Refereed Online International Journal
Google Scholar Indexing PIF: 1.048(I2OR), 3.125 (IIFS) & 3.8(SJIF)
Vol (3), Issue (3), July-September 2026 ISSN: 3048-7951

Cybersecurity Awareness, Digital Learning and Economic Resilience in Higher Education: A Global Bibliometric and Systematic Literature Review

Devendra Kumar[1]

DOI: http://doi.org/10.5281/zenodo.22922064
Review: 30/07/2026 Acceptance: 31/07/2026 Publication: 23/09/2026

Abstract: The rapid digital transformation of higher education has expanded the use of online learning platforms, cloud-based services, learning management systems, and other technology-mediated environments, while simultaneously increasing institutional exposure to cybersecurity threats. This paper examines the emerging landscape of cybersecurity in higher education with particular attention to major cyber threats, institutional preparedness, cybersecurity frameworks, digital transformation, artificial intelligence, and the economic and sustainability implications of cyber incidents. The review indicates that phishing, ransomware, malware, software vulnerabilities, password insecurity, denial-of-service attacks, and intellectual-property theft remain significant challenges for universities. Existing literature further highlights the importance of governance, institutional leadership, cybersecurity awareness, technical controls, and adaptable cybersecurity frameworks. The integration of artificial intelligence, machine learning, cloud technologies, simulations, virtual laboratories, and other technology-enabled approaches is increasingly shaping cybersecurity education and institutional protection mechanisms. The literature also demonstrates that cyber incidents extend beyond technical disruption, generating financial, operational, reputational, and educational consequences for higher education institutions. At the same time, cybersecurity investment is increasingly examined through economic and sustainability perspectives, particularly in relation to risk reduction, protection of critical infrastructure, data protection, and institutional trust. Overall, the reviewed literature indicates a need for comprehensive, adaptive, and institution-wide cybersecurity strategies that integrate technological, organisational, educational, financial, and sustainability dimensions. The paper identifies continuing gaps in empirical research and highlights the need for further evidence-based investigation of cybersecurity preparedness and resilience in higher education.

Keywords: Cybersecurity, Higher Education, Cyber Threats, Cybersecurity Awareness, Digital Transformation, Cyber Resilience, Sustainable Development, Economics Resilience.

Introduction: The rapid digitalisation of higher education has expanded the use of online learning platforms, learning management systems, cloud services, digital resources and other technology-mediated educational environments. Phishing, ransomware, software vulnerabilities, password weaknesses, and intellectual-property theft are among the major cybersecurity threats affecting higher education institutions. Cybersecurity awareness and institutional preparedness also remain important concerns (Afolalu & Tsoeu, 2025). Phishing has been identified as one of the most frequently reported cybersecurity threats in higher education, followed by denial-of-service attacks and ransomware. Evidence from studies published between 2020 and 2025 also indicates the continued presence of diverse cyber threats across university environments (Baleid & Abdullah, 2026). Higher education institutions face cybersecurity challenges including phishing, malware, intellectual-property theft, software vulnerabilities, password insecurity, and weaknesses in incident-disclosure practices. These challenges demonstrate the importance of strengthening institutional cybersecurity practices and awareness (Salam et al., 2026). Cybersecurity frameworks in higher education can be organised into maturity and capability models, governance and collaborative structures, and technical and operational mechanisms. Such frameworks provide

[1]**Scholar, Faculty of Education, Banaras Hindu University, Kamachha, Varanasi, Uttar Pradesh, India**

different approaches for addressing institutional cybersecurity requirements (Adamu et al., 2026). Higher-education cybersecurity frameworks need to address multiple institutional requirements and remain adaptable to changing cyber threats. Resource constraints, implementation complexity, and cultural resistance have been identified as important barriers to the effective implementation of cybersecurity frameworks (Barruga, 2025). Online cybersecurity education in universities increasingly uses learner-centred approaches, active learning, collaborative learning, case studies, and simulations. Virtual laboratories, gamification, and simulation environments are also used to provide practical learning experiences in digital cybersecurity education (Ahmed et al., 2024). Research on cybersecurity in higher education has expanded substantially, with notable growth reported from 2018 onward.

This expansion reflects increasing scholarly attention to cybersecurity issues within university and educational environments (Orosco-Fabian, 2024). Research at the intersection of artificial intelligence, cybersecurity, and educational technology has also expanded. A bibliometric analysis of 304 Scopus-indexed publications covering the period 2003–2025 identified an increasing research trajectory connecting these three areas (Islam et al., 2026). The integration of artificial intelligence into cybersecurity curricula has received increasing scholarly attention in higher education. Existing research has examined how AI concepts and cybersecurity education can be incorporated within university curricula and learning environments (Tian, 2025). Emerging technology-enabled cybersecurity controls in higher education increasingly involve artificial intelligence, machine learning, and cloud-based technologies.

These technologies are being investigated as mechanisms for responding to evolving cybersecurity threats in university environments (Bosiu & Nzama-Sithole, 2026). Empirical research on cybersecurity risks in higher education remains relatively limited despite considerable agreement regarding major cybersecurity problems affecting universities. This indicates the need for continued empirical investigation of cybersecurity risks within higher education environments (Lehto et al., 2021). Existing cybersecurity research in higher education has frequently focused on technological aspects, while broader institutional approaches involving organisational leadership and policymakers have also been identified as important for developing comprehensive cybersecurity strategies (Carr, 2021).

Digital transformation in higher education has extended beyond teaching and learning to organisational, administrative, and educational processes. Universities increasingly implement digital technologies as part of broader institutional transformation associated with technological development (Fernández et al., 2023). Digital transformation has emerged as an important area of higher education research, particularly in relation to technological developments associated with the Fourth Industrial Revolution. Universities have increasingly responded to these developments by incorporating digital technologies into institutional processes (Castro-Benavides et al., 2020).

The digital transformation of higher education is influenced by interconnected organisational and technological barriers. Addressing digital strategy, leadership, resources, digital competencies, organisational culture, and stakeholder-related factors is important for institutions undergoing digital transformation (Singun, 2025). Digital transformation provides various benefits to higher education institutions but also creates challenges related to skills, organisational capabilities, resources, and implementation. Universities therefore need to address multiple dimensions when undertaking technological transformation (Mabotha & Ngcamu, 2026). Cyberattacks against universities can produce significant financial consequences through incident-response costs, system restoration, legal and regulatory costs, opportunity costs, and disruption of teaching and research activities.

Estimating the complete financial impact can be difficult because universities may also experience indirect costs, including lost educational time and increased security expenditure (Mishra et al., 2025). Cyber incidents can affect staff resources, students, researchers, institutional reputation, and institutional budgets. These effects demonstrate that cybersecurity incidents may extend beyond technical disruption and influence wider institutional operations and resource utilisation (Jisc, 2022). Ransomware incidents can result in significant loss of services within universities, while business-email-compromise attacks may produce direct financial losses when criminals impersonate university partners or suppliers. Such incidents demonstrate the potential financial and operational consequences of cyber threats for higher education institutions (UK National Cyber Security Centre, 2022).

Economic considerations play an important role in cybersecurity investment decisions. Cybersecurity investment is influenced by factors such as incentives, externalities, and interdependence among organisations, demonstrating the relationship between cybersecurity and economic decision-making (Fedele et al., 2022). Cybersecurity investment has increasingly been examined from a financial economics perspective. Existing research has frequently employed economic and risk-based models, while comparatively less attention has been given to detailed financial parameters that distinguish cybersecurity investment from general cybersecurity expenditure (Brho et al., 2025).

Cybersecurity can contribute to economic sustainability through the protection of critical infrastructure and the reduction of financial risks. It can also support social sustainability through data protection and the development of organisational trust, demonstrating the broader relationship between cybersecurity and sustainable development (Morales-Sáenz et al., 2024).

Literature Reviews

Afolalu and Tsoeu (2025) reviewed cybersecurity in higher education and reported that phishing, ransomware, software vulnerabilities, password weaknesses and intellectual-property theft are important threats to higher education institutions, while cybersecurity awareness and institutional preparedness remain important concerns.

Baleid and Abdullah (2026) systematically reviewed 45 studies published between 2020 and 2025 and found that phishing was the most frequently reported threat, followed by denial-of-service attacks and ransomware.

Salam et al. (2026) reviewed 33 peer-reviewed studies published from 2018 to 2025 and identified phishing, malware, intellectual-property theft, software vulnerabilities, password insecurity and weak incident-disclosure practices as major cybersecurity challenges in higher education.

Adamu et al. (2026) reviewed cybersecurity frameworks used in higher education and classified them into maturity and capability models, governance and collaborative structures, and technical and operational mechanisms.

Barruga (2025) synthesized 50 peer-reviewed studies and found that higher-education cybersecurity frameworks require comprehensiveness and adaptability, while resource constraints, implementation complexity and cultural resistance were frequently reported barriers.

Ahmed et al. (2024) conducted a systematic review of online cybersecurity education and found that learner-centred approaches, active learning, collaborative learning, case studies and simulations were frequently used in university cybersecurity courses.

Ahmed et al. (2024) also reported that virtual laboratories, gamification and simulation environments were important technological tools for providing practical experiences in online cybersecurity education.

Orosco-Fabian (2024) conducted a bibliometric review of cybersecurity research in higher education and found that the field has expanded substantially, with particularly strong growth from 2018 onward.

Islam et al. (2026) conducted a bibliometric analysis of 304 Scopus-indexed publications on AI, cybersecurity and educational technology from 2003–2025 and reported an increasing research trajectory at the intersection of these fields.

Tian (2025) systematically reviewed the integration of artificial intelligence into cybersecurity curricula in higher education to examine how AI and cybersecurity are being taught together.

Bosiu and Nzama-Sithole (2026) reviewed emerging technology-enabled cybersecurity controls in higher education and examined the adoption of AI/ML and cloud-related technologies for responding to evolving cyber threats.

Lehto et al. (2021) also reported that empirical research on cybersecurity risks in higher education remained relatively scarce despite broad agreement concerning major cybersecurity problems.

Carr (2021) examined institutional cybersecurity strategies in higher education and argued that existing cybersecurity literature had often been technology-focused, creating a need for system-wide approaches relevant to institutional leaders and policymakers.

Fernández et al. (2023) conducted a multivocal literature review of digital transformation initiatives in higher education and found that universities were implementing digital technologies across organisational, administrative and educational processes.

Castro-Benavides et al. (2020) systematically reviewed digital transformation in higher education and identified digital transformation as an emerging field in which universities were responding to technological developments associated with the Fourth Industrial Revolution.

Singun (2025) systematically reviewed barriers to digital transformation in higher education and identified multiple interconnected organisational and technological barriers that institutions need to address during digital transformation.

Mabotha and Ngcamu (2026) reviewed digital transformation in higher education and examined its benefits, required skills, barriers and challenges for universities undergoing technological transformation.

Mishra et al. (2025) examined cyberattacks in the university sector and reported that cyber incidents can generate financial consequences through incident response, system restoration, legal and regulatory costs, opportunity costs and disruption of teaching and research.

Mishra et al. (2025) noted that estimating the financial impact of cyberattacks is particularly difficult for universities because of their complex data structures, collaborative networks and indirect costs such as lost educational time and increased security expenditure.

Jisc (2022) examined the impact of cyber incidents on further and higher education and research institutions and considered effects on staff resources, students, researchers, institutional reputation and budgets.

The UK National Cyber Security Centre reported that ransomware can cause significant loss of service at universities, while business-email-compromise attacks can result in direct financial losses when criminals impersonate university partners or suppliers.

Fedele et al. (2022) reviewed the economics of cybersecurity investment and showed that economic factors influence cybersecurity investment decisions, including incentives, externalities and interdependence between organisations.

Brho et al. (2025) examined the financial economics of cybersecurity investment and noted that existing research has often relied on economic and risk-based models while giving comparatively limited attention to detailed financial parameters distinguishing cybersecurity investment from expenditure.

Burgess et all the sustainability–cybersecurity literature reviewed in 2024 found that cybersecurity can contribute to economic sustainability by protecting critical infrastructure and reducing financial risks, while also supporting social sustainability through data protection and organisational trust.

The 2025 bibliometric study on cybersecurity and sustainable development analysed 425 publications and identified major research themes around cyber-resilient systems, sustainable digital management and sustainable transformation, showing that cybersecurity and sustainability are increasingly being studied as interconnected areas.

S. No.	Author (Last name, First name)	Year	Methodology	Major Finding	DOI
1	**Lehto, Mika** et al.	2021	Systematic literature review	Identified mission-critical assets, threat events, vulnerabilities and nine strategic cybersecurity risks in higher education.	10.3390/fi13020039 (MDPI)
2	**Bisri, Aria; Putri, Atina; Rosmansyah, Yusep**	2023	Systematic Literature Review	Executive leadership, institutional strategy and consistent implementation were important for successful digital transformation.	10.3991/ijet.v18i14.40201 (Online Journals)
3	**Ahmed, Ali; Watterson, Craig; Alhashmi, Saadat; Gaber, Tarek**	2024	Systematic literature review / PRISMA	Learner-centred approaches, active learning, collaborative learning, simulations, virtual laboratories and gamification were prominent in online cybersecurity education.	10.3389/fcomp.2024.1499490 (Frontiers)
4	**Morales-Sáenz, Francisco Isaí; Medina-Quintero, José Melchor; Reyna-Castillo, Miguel**	2024	Systematic Literature Review / PRISMA	Cybersecurity was associated with economic sustainability through protection of critical infrastructure and reduction of financial risks, and with social sustainability through data protection and trust.	10.3390/su16145884 (MDPI)

5	**Joshi, Sujata; Srivastava, Anugamini Priya; Prabhu, Sandeep; Pathak, Pankaj; Chirputkar, Abhijit; Pillai, Samaya**	2024/ 2025	Bibliometric + systematic review	Three major themes emerged: digital technologies, user experience and social inclusiveness.	10.1108/JARHE-02-2024-0084 (DOI)
6	**Singun, Amando Jr.**	2025	Systematic Literature Review / PRISMA	Identified nine barrier dimensions, including digital strategy, leadership, resources, competence, culture and digital ethics, with 80 subdimensions.	10.1007/s44217-025-00430-9 (Springer Link)
7	**Afolalu, Oladele; Tsoeu, Mohohlo Samuel**	2025	Systematic Literature Review	Identified phishing, ransomware and data breaches as important threats and examined zero-trust architecture, AI-driven security and cloud-based systems as emerging solutions.	10.3390/fi17120575 (MDPI)
8	**Surjawan, Daniel Jahja; Langi, Armein Z. R.; Imbar, Radiant Victor**	2025	Systematic Literature Review	Digital transformation affects teaching, administration, resource management and smart-campus operations; leadership, digital agility and resource allocation were important.	10.1109/ACCESS.2025.3557446 (DOI)
9	**Srivastava, Anugamini Priya** et al.	2025	Bibliometric + systematic review	Digital technologies were increasingly linked with teaching, learning, assessment, administration, user experience and social inclusion.	10.1108/JARHE-02-2024-0084 (DOI)
10	**Baleid, Hanan Mahmood; Abdullah, Mohammed Fadhl**	2026	Systematic Literature Review	Phishing was reported most frequently, followed by DoS and ransomware; human factors and weak internal governance were major vulnerabilities.	10.20428/jst.v31i1.3563 (UST Journals)
11	**Bosiu, Lebohang; Nzama-Sithole, Lethiwe**	2026	Systematic Literature Review / PRISMA	AI/ML, cloud services, blockchain and biometrics were identified as major emerging technologies for cybersecurity in HEIs, while integration and training remained challenges.	10.1007/s44217-026-01418-9 (Springer Link)
12	**Mabotha, Phuti Alfred Patrick; Ngcamu, Bethuel Sibongiseni**	2026	Systematic Literature Review	Digital transformation was associated with institutional performance, new business models, skills requirements, benefits, barriers and challenges in higher education.	10.3390/admsci16010001 (MDPI)

Research Objectives

RO1: To examine the global publication trends on cyber threats, digital learning and economic sustainability in higher education.

RO2: To identify the most productive countries, institutions, authors and journals in this research domain**.**

RO3: To identify the major themes and emerging research trends through keyword co-occurrence analysis.

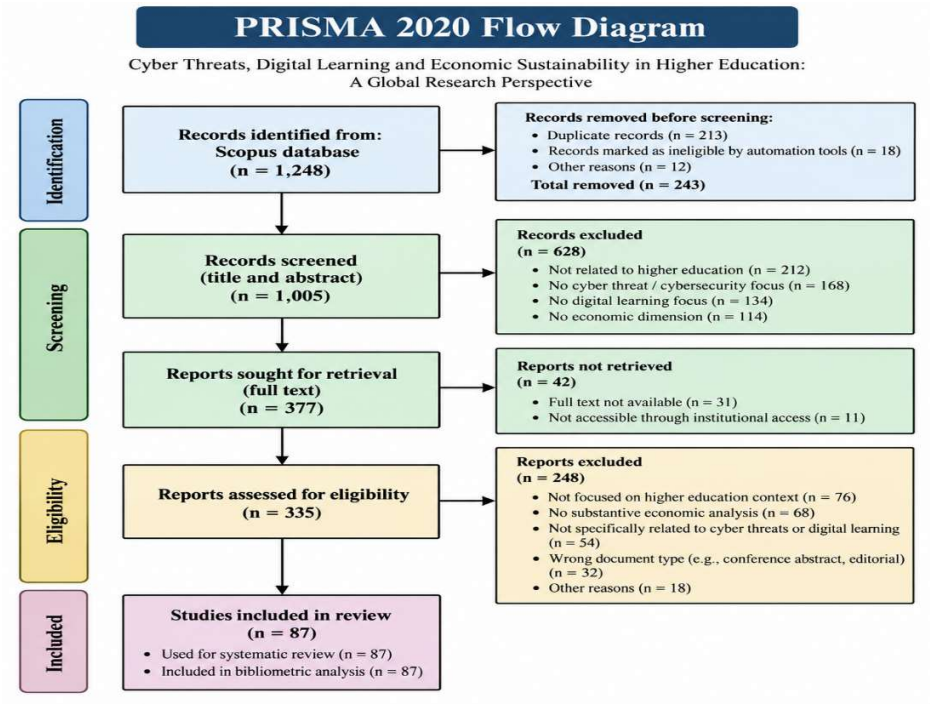
RO4: To examine the intellectual, social and thematic structure of research on cybersecurity and digital learning in higher education.

RO5: To identify the relationship between cyber threats, digital learning and economic sustainability in existing literature.

RO6: To identify research gaps and propose future research directions.

Methodology

Selection Process



Study Selection and PRISMA Procedure. The study selection process was conducted following the PRISMA 2020 framework. Relevant records were retrieved from the Scopus database using predefined search terms related to cyber threats, digital learning, higher education, and economic sustainability. The retrieved records were subsequently screened by title and abstract, followed by full-text assessment according to predefined inclusion and exclusion criteria. Duplicate and irrelevant records were removed during the screening process. The final set of eligible studies was included in the systematic review and bibliometric analysis.

Search Strategy

A structured search strategy was developed to identify relevant literature on cyber threats, digital learning, and economic sustainability in higher education. The search strategy used the Boolean operators **"AND" and "OR"** to combine and broaden the key concepts. The operator **"OR"** was used between synonyms and related terms to retrieve studies using different terminology, whereas **"AND"** was used to connect the major concepts and ensure that the retrieved studies addressed the intersection of the selected research dimensions. The search terms were organised into four main concept groups, namely cyber threats and cybersecurity, digital learning, higher education, and economic impact or sustainability.

The following Boolean search string was used in the Scopus database:

TITLE-ABS-KEY (("cyber threat" OR cybersecurity OR "cyber security" OR "cyber-attack" OR phishing OR ransomware OR "data breach*" OR "cyber fraud") AND ("digital learning" OR "online learning" OR e-learning OR "digital education" OR "online education" OR MOOCs OR "learning management system*") AND ("higher

education" OR university* OR "higher education institution*" OR "college student*") AND ("economic sustainability" OR "economic impact" OR "economic cost*" OR "financial impact" OR "financial loss*" OR "economic resilience"))**

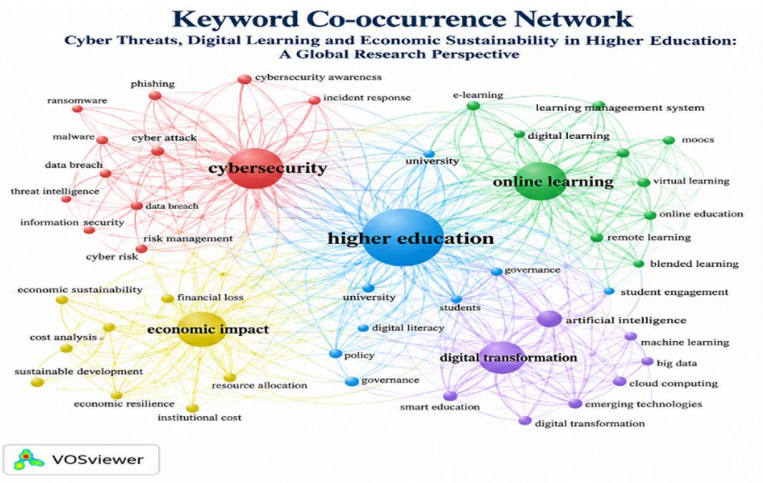
In this search strategy, the first group identifies studies related to cyber threats and cybersecurity, the second group captures different forms of digital learning, the third group restricts the literature to higher education contexts, and the fourth group identifies studies addressing economic impact, financial consequences, economic resilience, or sustainability. The asterisk (*) was used as a truncation symbol to retrieve different word endings, such as threat and threats, attack and attacks, and university and universities. The search was conducted within the title, abstract, and keywords fields of Scopus to identify literature directly relevant to the research topic.

Inclusion and Exclusion Criteria

Studies were included in the review if they were related to the context of higher education or universities, addressed cyber threats, cybersecurity, or cyberattacks, examined digital learning, online learning, e-learning, or digital education, and discussed economic impact, financial costs, economic sustainability, economic resilience, or institutional resource implications. Only peer-reviewed research articles and review papers published in the English language within the selected publication period were considered eligible for inclusion. Studies were excluded if they focused exclusively on school education, were unrelated to higher education, did not address cybersecurity or cyber threats, did not examine digital learning or digital education, or had no relevant economic dimension. Editorials, book chapters, conference abstracts, notes, and other non-eligible document types were also excluded. Duplicate records were removed before screening, and studies for which the full text could not be obtained were excluded when full-text availability was required for eligibility assessment.

Keyword Co-occurrence Network

The keyword co-occurrence network illustrates the conceptual structure of research connecting cybersecurity, digital learning, higher education, economic impact, sustainability, and emerging technologies. In a co-occurrence network, the size of a node represents the frequency or prominence of a keyword, while the links between nodes represent their co-occurrence relationships. Keywords that appear together frequently are positioned closer to one another, whereas different colours represent different thematic clusters.



4. Thematic Findings

4.1 Theme 1: Cyber Threats and Security

The first thematic cluster represents cyber threats and security, which forms one of the central dimensions of research concerning higher education in digital environments. The literature consistently identifies higher education institutions as vulnerable environments because universities operate large, interconnected and relatively

open digital infrastructures supporting teaching, research, administration and communication. Afolalu and Tsoeu (2025) reported that the increasing adoption of digital technologies in higher education has simultaneously increased institutional exposure to phishing, ransomware, data breaches, malware, password-related vulnerabilities and other forms of cyberattack. Baleid and Abdullah (2026), in their systematic review of 45 peer-reviewed studies published between 2020 and 2025, found phishing to be the most frequently reported threat, followed by denial-of-service attacks and ransomware. These findings indicate that cyber threats are not restricted to isolated technical incidents but are associated with the broader digital transformation of higher education.

The literature further indicates that the human factor remains an important component of cybersecurity vulnerability. Afolalu and Tsoeu (2025) identified insufficient cybersecurity awareness, fragmented security procedures and technology gaps among the factors contributing to institutional vulnerability. Baleid and Abdullah (2026) similarly identified human factors and weak internal governance as important causes of cybersecurity weaknesses in open academic environments. Consequently, cybersecurity research in higher education increasingly combines technological controls with awareness, training, governance and institutional preparedness.

Another important development within this theme is the movement from conventional security practices toward integrated approaches involving zero-trust architectures, artificial intelligence, cloud security and risk-management mechanisms. Afolalu and Tsoeu (2025) identified zero-trust architectures, AI-driven security and cloud-based systems as emerging approaches for strengthening institutional cybersecurity. However, Baleid and Abdullah (2026) found that conventional cybersecurity approaches remained more common than AI-based approaches, with financial limitations, knowledge gaps and privacy concerns identified as barriers to wider AI adoption.

4.2 Theme 2: Digital Learning in Higher Education

The second thematic cluster focuses on digital learning and online education, reflecting the increasing integration of digital platforms into teaching and learning processes. Research in this area demonstrates that online learning has expanded the technological infrastructure through which higher education institutions deliver educational services. Learning management systems, online courses, virtual learning environments, digital resources, remote learning and blended learning have become important components of contemporary higher education. A systematic review by Ahmed et al. (2024) examining online cybersecurity education at universities found that learner-centred approaches, active learning, collaborative learning, case studies and simulations were commonly employed in online cybersecurity courses.

The literature also demonstrates that digital learning creates a dual relationship with cybersecurity. On one hand, online learning provides flexible access to education and enables institutions to expand digital delivery; on the other hand, dependence on interconnected platforms creates additional points of vulnerability. The systematic review by Ahmed et al. (2024) specifically examined the challenges associated with designing and delivering cybersecurity education through online environments, demonstrating that institutions must adapt conventional teaching practices to digital learning conditions.

The broader digital-transformation literature shows that digitalisation in higher education extends beyond online classes to institutional management, datafication, learning analytics, artificial intelligence and smart-campus technologies. Trevisan et al. (2024) analysed 672 publications and 72 studies through bibliometric and content analysis and identified three major areas of research: sustainability competencies through digital transformation,

smart and sustainable campuses, and theoretical development concerning sustainability and digital transformation in higher education.

Research also indicates that successful digital transformation depends on institutional capacity. Singun (2025), through a systematic review of 20 peer-reviewed studies published between 2019 and 2024, identified nine dimensions of barriers to digital transformation, including digital strategy and policy, leadership and management, digital resources, digital competence, stakeholder management, digital culture, academic factors and digital ethics. This finding demonstrates that digital learning cannot be understood only in terms of technology availability because organisational readiness, digital competencies and governance also influence implementation.

4.3 Theme 3: Higher Education Context

The third thematic cluster represents the higher education institutional context, which provides the organisational setting in which cybersecurity, digital learning and sustainability intersect. The literature indicates that universities possess distinctive characteristics that differentiate them from many other organisations. Higher education institutions manage diverse groups of students, faculty, researchers, administrators and external collaborators while simultaneously supporting teaching, research, administration and public engagement. These activities require extensive digital connectivity and information sharing, creating complex cybersecurity and governance requirements.

Afolalu and Tsoeu (2025) further identified fragmented security procedures, inadequate awareness and technology gaps as important contributors to institutional vulnerability.

The institutional context also appears strongly in research on cybersecurity governance. A systematic review of cybersecurity frameworks in higher education by Adamu et al. (2026) classified existing approaches into three broad categories: maturity and capability models, governance-based and collaborative structures, and technical and operational mechanisms. The review reported that frameworks such as COBIT 5, Zero Trust and risk-assessment models are more effective when aligned with institutional governance, available resources, organisational culture and user experience.

Digital transformation research similarly demonstrates that institutional readiness is important. Singun (2025) identified digital leadership, organisational structures, digital resources, competence, culture and ethics among the dimensions influencing digital transformation in higher education. Trevisan et al. (2024) also found that sustainability-oriented digital transformation in higher education involves institutional strategies, competencies and smart-campus approaches rather than isolated technological adoption.

The higher education context therefore functions as an important connecting dimension among the three central concepts of the present study. Cybersecurity threats occur within institutional digital infrastructures; digital learning operates through these infrastructures; and the costs, benefits and resilience associated with their management influence institutional sustainability. The literature consequently suggests that cybersecurity cannot be separated from institutional governance, resource allocation, digital competence and organisational culture. The higher education institution should therefore be understood as an integrated socio-technical environment in which technological, educational, organisational and economic dimensions interact.

4.4 Theme 4: Economic Impact and Sustainability

The fourth thematic cluster focuses on economic impact, financial risk and sustainability, which provides the economic dimension of the present research framework. The literature indicates that cybersecurity is increasingly connected with economic sustainability because cyber incidents can generate financial losses, operational disruption, recovery costs and resource requirements. Morales-Sáenz et al. (2024), through a systematic literature review of cybersecurity and sustainable development, found a relationship between cybersecurity and economic sustainability, particularly through the protection of critical infrastructure and minimisation of financial risks.

The economic implications are particularly relevant for higher education institutions because cyber incidents can affect both technological operations and educational activities. Cybersecurity investments require financial resources for infrastructure, security software, professional expertise, staff training, incident response and recovery. At the same time, inadequate cybersecurity can generate additional costs when institutions experience data breaches, ransomware, system disruption or service interruptions. Thus, cybersecurity creates both a preventive investment dimension and a risk-cost dimension.

The broader sustainability literature supports this connection. Trevisan et al. (2024) examined 672 publications concerning digital transformation and sustainability in higher education and identified sustainability competencies, smart and sustainable campuses and theoretical approaches to digital transformation as major areas of research. Their findings demonstrate that digital transformation can contribute to sustainability when technological development is incorporated into broader institutional strategies.

However, the literature also reveals that the economic dimension of digital sustainability has not always been examined together with cybersecurity. Szalkowski and Johansen (2024) found that although economic and environmental implications of digital technologies have received considerable attention, security and privacy implications have been comparatively under-represented in research on sustainability. This finding is important for the present study because it indicates a need to examine cybersecurity not simply as a technical protection mechanism but as a factor that can influence sustainability outcomes.

Morales-Sáenz et al. (2024) further reported that cybersecurity contributes to sustainable development by reducing financial risks and protecting infrastructure, while also supporting social sustainability through data protection and organisational trust. Similarly, research on the relationship between cybersecurity and sustainable development has argued for integrated frameworks connecting cybersecurity with economic, social and environmental sustainability.

4.5 Theme 5: Emerging Technologies

The fifth thematic cluster represents emerging technologies, particularly artificial intelligence, machine learning, cloud computing, big data, smart education and digital transformation. The literature shows that these technologies are increasingly integrated into higher education while simultaneously creating new cybersecurity requirements. Emerging technologies therefore have a dual role: they can strengthen cybersecurity capabilities while also introducing additional digital risks and vulnerabilities. Afolalu and Tsoeu (2025) identified artificial intelligence-driven security, zero-trust architectures and cloud-based systems among the emerging approaches being considered for protecting higher education institutions. The authors also noted that higher education institutions face technology gaps and awareness limitations, indicating that technological adoption alone does not automatically eliminate cybersecurity vulnerabilities. Research on online cybersecurity education also demonstrates the growing role of advanced technologies in teaching and learning. Ahmed et al. (2024) identified virtual laboratories, simulations and technology-supported learning approaches as important methods for providing practical cybersecurity learning experiences in online university courses. Such technologies can enable

students to develop practical cybersecurity knowledge without requiring access to physical laboratory environments. The intersection between emerging technologies and sustainability has also received increasing attention. A systematic literature review on AI, sustainability and higher education examined literature from 2015 to 2024 and developed a framework connecting artificial intelligence with sustainable higher education. Similarly, Trevisan et al. (2024) identified digital transformation as an important mechanism through which higher education institutions can develop sustainability competencies and smart-campus approaches.

However, emerging technologies also create challenges related to data protection, privacy, governance and institutional readiness. Singun (2025) identified digital resources, digital competence, stakeholder management, digital culture and digital ethics as important dimensions of barriers to digital transformation in higher education. Szalkowski and Johansen (2024) additionally observed that cybersecurity and privacy implications have received comparatively limited attention in research examining the sustainability effects of digital technologies.

Findings of the Study

The literature analysis indicates that cybersecurity in higher education has developed into a multidisciplinary research area connecting cybersecurity, digital learning, digital transformation, emerging technologies, and economic sustainability. The reviewed literature identifies phishing, ransomware, malware, software vulnerabilities, password insecurity, data breaches, and intellectual-property theft as recurring cybersecurity concerns in higher education institutions (Afolalu & Tsoeu, 2025; Baleid & Abdullah, 2026; Salam et al., 2026).

The findings further indicate that the expansion of online and technology-mediated learning has increased the dependence of universities on learning management systems, cloud services, virtual laboratories, digital resources, and interconnected information systems. Online cybersecurity education has increasingly incorporated learner-centred approaches, simulations, virtual laboratories, gamification, collaborative learning, and case-based learning (Ahmed et al., 2024). This demonstrates that cybersecurity and digital learning are becoming increasingly interconnected within higher education.

Another important finding concerns the institutional dimension of cybersecurity. Existing studies indicate that cybersecurity cannot be addressed only through technical controls. Institutional governance, cybersecurity frameworks, leadership, awareness, training, organisational culture, and preparedness are also important components of cybersecurity management (Lehto et al., 2021; Adamu et al., 2026; Barruga, 2025). Resource limitations and implementation difficulties remain relevant barriers to developing comprehensive cybersecurity systems.

The literature also shows increasing integration of emerging technologies with cybersecurity and higher education. Artificial intelligence, machine learning, cloud computing, and other digital technologies are being explored for improving cybersecurity capabilities and responding to emerging threats (Bosiu & Nzama-Sithole, 2026; Tian, 2025). At the same time, digital transformation creates additional requirements related to governance, skills, infrastructure, and security (Singun, 2025; Mabotha & Ngcamu, 2026).

A further finding is the growing recognition of the economic consequences of cyber threats. Cyber incidents may generate costs related to incident response, system restoration, legal and regulatory requirements, disruption of teaching and research, lost productivity, and increased security expenditure (Mishra et al., 2025). Research on cybersecurity economics also indicates that cybersecurity investment involves economic considerations such as incentives, externalities, risk, and organisational interdependence (Fedele et al., 2022).

Finally, the reviewed literature indicates a growing connection between cybersecurity and sustainability. Cybersecurity can support economic sustainability by protecting critical infrastructure and reducing financial risks, while data protection and organisational trust can contribute to social sustainability (Morales-Sáenz et al., 2024). However, the literature remains fragmented across cybersecurity, digital learning, digital transformation, cybersecurity economics, and sustainability. This indicates a need for more integrated research examining these dimensions together within higher education.

Implications of the Study

1. Implications for Higher Education Institutions

Higher education institutions need to consider cybersecurity as an institutional responsibility rather than only a technical function. Universities should integrate cybersecurity into academic, administrative, research, and digital-learning systems. Institutional cybersecurity frameworks should incorporate technical protection, governance, awareness, training, incident response, and risk management (Lehto et al., 2021; Adamu et al., 2026).

2. Implications for Digital Learning

The increasing use of online learning platforms requires cybersecurity to be incorporated into digital-learning environments. Universities should provide cybersecurity awareness and digital-safety education to students, teachers, researchers, and administrative personnel. Practical approaches such as simulations, virtual laboratories, case studies, and experiential learning can be used to strengthen cybersecurity learning (Ahmed et al., 2024).

3. Implications for Policy and Governance

The findings suggest that institutional cybersecurity policies should address both technological and organisational dimensions. Policies should provide clear mechanisms for data protection, incident reporting, access management, cybersecurity training, risk assessment, and institutional accountability. Governance structures should also be adaptable because cyber threats and digital technologies continue to change (Adamu et al., 2026; Barruga, 2025).

4. Economic Implications

Cybersecurity planning should consider both the cost of security investments and the potential economic consequences of cyber incidents. Universities may need to consider incident-response expenditure, system-recovery costs, operational disruption, legal costs, and loss of productivity when developing cybersecurity strategies (Mishra et al., 2025). Cybersecurity investment can therefore be considered in relation to institutional resilience and long-term resource sustainability (Fedele et al., 2022).

5. Implications for Emerging Technologies

The increasing use of AI, machine learning, cloud computing, and other emerging technologies creates opportunities for strengthening cybersecurity but also introduces additional security and governance requirements. Institutions should therefore consider cybersecurity, ethical governance, data protection, and digital competencies when adopting emerging technologies (Bosiu & Nzama-Sithole, 2026; Tian, 2025).

6. Implications for Future Research

Future research should examine the relationship among cyber threats, digital learning, institutional resilience, and economic sustainability using empirical and longitudinal approaches. More research is also required on the economic measurement of cyber incidents in universities, the effectiveness of cybersecurity awareness programmes, AI-enabled cybersecurity, and cybersecurity preparedness across different higher education contexts.

Conclusion

The present study demonstrates that cybersecurity has become an important component of the digital transformation of higher education. The reviewed literature shows that universities face multiple cyber threats, including phishing, ransomware, malware, software vulnerabilities, data breaches, password insecurity, and intellectual-property theft. The increasing use of online learning platforms, cloud services, learning management systems, and digital resources has further increased institutional dependence on secure digital infrastructure (Afolalu & Tsoeu, 2025; Salam et al., 2026).

The findings also demonstrate that cybersecurity extends beyond technical protection. Institutional governance, cybersecurity awareness, staff and student training, organisational preparedness, policy development, and appropriate cybersecurity frameworks are essential for protecting higher education environments (Lehto et al., 2021; Adamu et al., 2026). Emerging technologies such as artificial intelligence, machine learning, and cloud computing are increasingly becoming part of both digital learning and cybersecurity practices, creating new opportunities as well as additional governance requirements.

Importantly, cyber threats also have economic implications for higher education. Cyber incidents can result in system-recovery expenses, incident-response costs, legal and regulatory costs, disruption of teaching and research, productivity losses, and increased security expenditure (Mishra et al., 2025). Consequently, cybersecurity should be considered in relation to institutional economic resilience and sustainability rather than solely as an information-technology concern. Research has increasingly recognised the relationship between cybersecurity and sustainable development through the protection of critical infrastructure, reduction of financial risks, data protection, and organisational trust (Morales-Sáenz et al., 2024).

References

Adamu, S. U., Ahmad, M. A., & Ibrahim, M. (2026). A systematic literature review on the adoption and effectiveness of cybersecurity frameworks in higher education institutions. *Information and Computer Security*. https://doi.org/10.1108/ICS-10-2025-0403 Emerald Publishing

Afolalu, O., & Tsoeu, M. S. (2025). Cybersecurity in higher education institutions: A systematic review of emerging trends, challenges and solutions. *Future Internet, 17*(12), 575. https://doi.org/10.3390/fi17120575

Afolalu, O., & Tsoeu, M. S. (2025). Cybersecurity in higher education institutions: A systematic review of emerging trends, challenges and solutions. *Future Internet, 17*(12), 575. https://doi.org/10.3390/fi17120575

Ahmed, A., Watterson, C., Alhashmi, S., & Gaber, T. (2024). How universities teach cybersecurity courses online: A systematic literature review. *Frontiers in Computer Science, 6*, 1499490. https://doi.org/10.3389/fcomp.2024.1499490

Ahmed, A., Watterson, C., Alhashmi, S., & Gaber, T. (2024). How universities teach cybersecurity courses online: A systematic literature review. *Frontiers in Computer Science, 6*, 1499490. https://doi.org/10.3389/fcomp.2024.1499490

Amzeyeva, A. A., & Zhumabayeva, A. E. (2025). Cybersecurity awareness among students: A systematic literature review and PRISMA-based analysis. *Gumilyov Journal of Pedagogy*. https://doi.org/10.32523/3080-1710-2025-152-3-126-144

Baleid, H. M., & Abdullah, M. F. (2026). Cybersecurity in higher education: A systematic review of threats, challenges, and mitigation strategies. *Journal of Science and Technology, 31*(1). https://doi.org/10.20428/jst.v31i1.3563

Barruga, M. B. (2025). Systematic review of cybersecurity frameworks for higher education institutions: Characteristics, components, and challenges. *International Journal of Applied Mathematics, 38*(4s). https://doi.org/10.12732/ijam.v38i4s.299

Barruga, M. B. (2025). Systematic review of cybersecurity frameworks for higher education institutions: Characteristics, components, and challenges. *International Journal of Applied Mathematics, 38*(4s). https://doi.org/10.12732/ijam.v38i4s.299

Bosiu, L., & Nzama-Sithole, L. (2026). New technology-empowered cybersecurity controls in higher education institutions: A systematic review. *Discover Education, 5*, 271. https://doi.org/10.1007/s44217-026-01418-9

Brho, M., Jazairy, A., & Glassburner, A. V. (2025). The finance of cybersecurity: Quantitative modeling of investment decisions and net present value. *International Journal of Production Economics, 279*, 109448. https://doi.org/10.1016/j.ijpe.2024.109448

Castro Benavides, L. M., Tamayo Arias, J. A., Arango Serna, M. D., Branch Bedoya, J. W., & Burgos, D. (2020). Digital transformation in higher education institutions: A systematic literature review. *Sensors, 20*(11), 3291. https://doi.org/10.3390/s20113291

Fedele, A., & Roner, C. (2022). Dangerous games: A literature review on cybersecurity investments. *Journal of Economic Surveys, 36*(1), 157–187. https://doi.org/10.1111/joes.12456

Kianpour, M., Kowalski, S. J., & Øverby, H. (2021). Systematically understanding cybersecurity economics: A survey. *Sustainability, 13*(24), 13677. https://doi.org/10.3390/su132413677

Kumar, A., Mishra, K., Mahto, R. K., & Mishra, B. K. (2024). A framework for institution to enhancing cybersecurity in higher education: A review. *LatIA*. https://doi.org/10.62486/latia202494

Morales-Sáenz, F. I., Medina-Quintero, J. M., & Reyna-Castillo, M. (2024). Beyond data protection: Exploring the convergence between cybersecurity and sustainable development in business. *Sustainability, 16*(14), 5884. https://doi.org/10.3390/su16145884

Nilupú-Moreno, K., Salas-Riega, J. L., Ninaquispe-Soto, M., & Riega-Virú, Y. (2024). Cybersecurity in university students: A systematic review of the literature. In *Intelligent Sustainable Systems* (pp. 315–332). Springer. https://doi.org/10.1007/978-981-99-7886-1_27

Salam, M., Abu Bakar, K. A., Abdul Ghani, A. T., & Mohd Aman, A. H. (2026). Cybersecurity in higher education institutions digitalisation: Addressing threats and vulnerabilities. *SAGE Open*, 1–14. https://doi.org/10.1177/21582440251143473

Salam, M., Abu Bakar, K. A., Abdul Ghani, A. T., & Mohd Aman, A. H. (2026). Cybersecurity in higher education institutions digitalisation: Addressing threats and vulnerabilities. *SAGE Open*, 1–14. https://doi.org/10.1177/21582440251413473

Singun, A. (2025). Unveiling the barriers to digital transformation in higher education institutions: A systematic literature review. *Discover Education, 4*, 37. https://doi.org/10.1007/s44217-025-00430-9

Tian, J. (2025). Integrating artificial intelligence into the cybersecurity curriculum in higher education: A systematic literature review. *Education Sciences, 15*(11), 1540. https://doi.org/10.3390/educsci15111540

Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet, 13*(2), 39. https://doi.org/10.3390/fi13020039

Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet, 13*(2), 39. https://doi.org/10.3390/fi13020039