Mediterranean Journal of Basic and Applied Sciences (MJBAS)
Volume 10, Issue 2, Pages 308-329, April-June 2026

An Empirical Assessment of Cybersecurity Governance Frameworks, Incident Response Protocols, and Cloud Infrastructure Operational Readiness in Higher Education Institutions: A Comprehensive Quantitative Correlation Analysis of Institutional Vulnerabilities And Policy Implementation Gaps

Ian Kirby B. Duman-ag[1*], Harold M. Coyoca[2], Rissa Flor I. Arnaiz[3], Jastine Claire V. Rullin[4], Jay Mark C. Palania[5], Jevi D. Bantiad[6], Kent Nicholas P. Carreon[7], Kurt Collin Clint B. Mabalod[8], Lenyvie T. Pauyon[9], Lollaine Guill J. Puerte[10], Lorie A. Tac-an[11], Mae S. Rodriguez[12] & Ginbert A. Fernandez[13]

[1-13]Department of Information Technology, College of Information Technology and Computing, University of Science and Technology of Southern Philippines – Oroquieta Campus, Oroquieta City, Misamis Occidental 7207, Philippines.
Corresponding Author (Ian Kirby B. Duman-ag) Email: dumanagian5@gmail.com[*]

DOI: Under Assignment

Article Received: 14 March 2026 *Article Accepted: 19 May 2026* *Article Published: 24 May 2026*

ABSTRACT

Cybersecurity and cloud infrastructure readiness in higher education institutions investigates how well these institutions protect their digital assets and maintain security against cyber threats while using cloud-based services during their ongoing digital transformation processes. The study evaluates institutional preparedness, which includes the cybersecurity governance framework, risk assessment procedures, incident management protocols, and cloud computing service deployment. A quantitative research design was used to collect data through a structured survey questionnaire completed by 1,003 participants from different organizations. The researchers applied descriptive statistical methods to analyze the data, including weighted mean and frequency distribution based on a 4-point Likert scale. The study results show that organizations achieve cybersecurity readiness and cloud infrastructure operational status between 80% and 89% according to their respective composite means of 2.68 and 2.76. The results demonstrate that organizations have implemented basic security systems; however, their operational capabilities remain incomplete because no aspect reached full implementation status. The assessment discovered critical shortages in incident response procedures, monitoring equipment, and personnel resources, which would hinder organizations from effectively detecting and handling threats in real time. The research shows that higher education institutions need to improve their digital security systems because they currently use outdated systems that only protect basic digital activities. The researchers propose that institutions should develop stronger governance systems, establish better monitoring and incident management processes, implement multi-factor authentication, and enhance the capabilities of their internal cybersecurity workforce.

Keywords: Cybersecurity Readiness; Cloud Infrastructure; Higher Education Institutions; Cloud Security; Risk Management; Incident Response; Digital Transformation; Cybersecurity Governance; Cybersecurity Maturity; Zero Trust Security; Governance Framework; Incident Management.

1.0. Introduction

Universities today rely heavily on digital technology to handle their financial operations and student records. The implementation of modern technology at educational institutions leads to higher security threats. According to IBM Security (2024), schools in the education sector remain exposed to cyber threats because they attempt to safeguard their existing information through the use of outdated systems and weak security measures.

Organizations implement cloud-based solutions to establish centralized systems which enable them to control operations while expanding their capacity and conducting automated data protection activities. The cloud provides organizations with top security solutions which include identity management and deep encryption capabilities. The advantages of a system require active effort from users to establish them as operational functions. Cloud Security Alliance (2022) states that cloud migration success requires organizations to define their entire operational approach. The institutional security system becomes vulnerable to breaches when governance fails to supervise system implementation and users establish incorrect system settings.

High-level security frameworks create an ideal solution for security needs, yet these frameworks fail to address security requirements that small educational institutions face. Institutions face problems with their basic operations because they need to update their servers and add more security personnel according to the ENISA (2022) governance and risk management frameworks which provide organizations with comprehensive operational procedures. Schools need structured assessments to establish their current status before they can implement advanced digital technology. The existing standards and frameworks need implementation, which serves as the primary problem for organizations.

1.1. Statement of the problem

This study aims to assess the cybersecurity and cloud infrastructure readiness of higher education institutions. Specifically, it seeks to answer the following questions:

1) How prepared are higher education institutions in terms of cybersecurity governance, risk management, and incident response?
2) How ready are institutions to securely implement and manage cloud-based infrastructure?
3) What infrastructure and policy gaps increase institutional vulnerability to cyberattacks?

1.2. Hypotheses of the Study

H_0: Higher education institutions have only moderate cybersecurity readiness.

H_1: Institutions are not fully prepared to securely adopt and manage cloud infrastructure.

H_2: Gaps in governance, staffing, and infrastructure significantly increase vulnerability to cyber threats.

1.3. Study Objectives

General Objective

All The primary aim of this research is to gauge how well-prepared higher education institutions actually are for the cloud, specifically looking at their ability to withstand the modern wave of cyber threats.

Specific Objectives

- To assess the level of cybersecurity governance in higher education institutions.
- To examine the effectiveness of risk management and incident response practices.
- To evaluate the readiness of institutions in implementing and managing cloud-based infrastructure securely.
- To identify infrastructure and policy gaps that increase institutional vulnerability to cyber threats.
- To recommend strategic measures that can strengthen cybersecurity and cloud infrastructure readiness in higher education institutions.

1.4. Significance of the Study

This study may provide valuable information and practical insights to the following groups:

- **Audit the Rulebook**

Consider rulebooks in actual governance, and get a real feel for how these forms of schools actually manage day-to-day risks.

Test the Tech

Conducting technical testing because this testing will verify the proper functioning of access controls and monitoring systems and backup solutions nm.

- **Evaluate Cloud Readiness**

The assessment of security vulnerabilities which arise from the institutions' ability to transition to cloud services needs to be conducted to determine their cloud readiness.

- **Determining Vulnerability**

The recognition and identification of the 'exposed areas' in physical and procedural entities becomes a massive task.

1.5. Scope and Delimitations

This research could be helpful for the following audiences:

The current research addresses the issues related to the cybersecurity and cloud infrastructure readiness of higher education institutions. It involves students, information technology professionals, administrators, and other staff working in the field of cybersecurity and cloud services management in higher education institutions.

This research is dedicated to the topics of cybersecurity governance, cybersecurity risks and threat management, cybersecurity incident response preparation, and cloud infrastructure deployment, excluding other areas of information technology that are not associated with cybersecurity and cloud infrastructure readiness issues. The current research covers cybersecurity preparedness issues while excluding technical hacking activities, software development activities, and system engineering tasks.

1.6. Definition of Terms

The following terms are operationally defined to provide clearer understanding of the study:

- **Cybersecurity**

Refers to the protection of computer systems, networks, and digital information from cyber threats such as hacking, malware, phishing, and unauthorized access.

- **Cloud Infrastructure**

Refers to the hardware, software, storage, and network resources delivered through cloud computing services to support institutional operations.

- **Higher Education Institutions (HEIs)**

Refers to colleges and universities that provide tertiary education and utilize digital systems for academic and administrative services.

- **Cybersecurity Governance**

Refers to the policies, procedures, and management practices implemented by institutions to ensure the protection of digital assets and information systems.

- **Risk Management**

Refers to the process of identifying, assessing, and minimizing cybersecurity risks that may affect institutional operations.

- **Incident Response**

Refers to the procedures and actions performed by an institution to detect, manage, and recover from cybersecurity incidents or attacks.

- **Cloud Readiness**

Refers to the capability of an institution to securely adopt, implement, and manage cloud-based technologies and services.

- **Multi-Factor Authentication (MFA)**

Refers to a security method that requires users to verify their identity using two or more authentication factors before accessing systems or accounts.

- **Data Backup**

Refers to the process of creating copies of important digital data to ensure recovery in case of data loss, corruption, or cyberattack.

- **Monitoring Systems**

Refers to security tools and technologies used to continuously observe, detect, and analyze suspicious activities within institutional networks and systems.

1.7. Scope and Limitations of the Study

The research evaluates how prepared universities are to protect their digital assets against cybersecurity threats while using cloud computing technology. The study includes participants who possess cybersecurity skills and experience in managing cloud services, including students and staff members from various administrative and technical roles. The research investigates how higher education institutions implement cybersecurity governance and risk management and their capacity to respond to security incidents and their cloud infrastructure systems.

The research team obtained data from participants through a structured survey questionnaire which used a 4-point Likert scale for responses. The study applied descriptive statistical methods which included weighted mean and frequency distribution to examine the collected information. The research aims to assess how prepared institutions are to safeguard their digital assets through effective cloud technology security management.

The research only examines specific higher education institutions, which prevents the findings from accurately representing all educational institutions throughout the Philippines. The responses reflect self-reported

information, which can lead to personal bias and different levels of understanding between the respondents. The research study examines only cybersecurity preparedness and cloud infrastructure services, but it excludes all technical aspects of hacking and software development and system engineering and all other IT domains. The study did not take into account external elements which included budget constraints and internet connection issues and the ongoing development of cybersecurity threats.

2.0. Review of Related Literature

The environment of higher education institutions functions as an open system that uses extensive data resources which creates new security vulnerabilities that prevent effective security management (Afolalu and Tsoeu, 2025). The pattern of cyber incidents which universities experience demonstrates that these events occur repeatedly to jeopardize the protection of institutional services (Lallie et al., 2025). The education sector reports various cyber incidents which include credential theft and social engineering attacks and system breaches (Verizon, 2024). Cyberattacks and data breaches target educational institutions because these organizations provide access to diverse users who use multiple devices and cloud services (Microsoft, 2024). The complete research shows that higher education institutions require cyber security readiness for their business operations while the institution needs to perform technical upgrades (IBM Security, 2024).

The use of cybersecurity maturity models helps organizations to strengthen their security systems because these frameworks guide organizations in developing their security systems into sustainable operational processes which security teams can evaluate and monitor throughout their lifecycle (2024). Organizations need to create connections between their cybersecurity activities and enterprise risk management systems and executive leadership functions according to current governance-focused requirements (NIST 2024). Security systems must evolve beyond just ensuring that organizations comply with minimum standards because their business operations will have to be secured from attacks that will come with the course of their normal operations (ENISA 2023a). Security systems must evolve beyond simple compliance because organizations' business operations require additional protection from any new attack techniques (ENISA 2023a). Afolalu and Tsoeu (2025) state that higher education institutions use maturity assessment to determine their existing security controls and their unimplemented security controls and their necessary security controls which result from their ongoing digital growth.

Organizations use recreational cloud services to achieve operational efficiency which gives them more scalable systems that stay online during operational disruptions while distributing security responsibilities to third parties (CSA 2024a). Organizations need to implement three essential security components for cloud environments according to market research which requires they build security visibility systems and governance frameworks and identity management systems that need vendor system integration (ENISA 2023b). The newest implementation guidelines require organizations to create secure access systems which will protect their hybrid and multi-cloud and remote access systems without using network location as a security trust element (NIST 2025). The development of cloud-native zero trust models proves that organizations which operate in multiple locations need to implement both identity-based access control and policy-based access control systems (NIST 2023). Current

research shows that organizations must build their detection and response skills because these two abilities need to function together to manage misconfigurations and unusual behavior and unauthorized access in cloud systems (Pitkar 2025).

Various publications consistently report on the issue of old legacy systems that do not meet the modern security requirements due to design, documentation and maintenance practices that are not compatible with today's security standards (Pang et al., 2022). When it comes to higher education institutions, digital transformation happens at a rate that IT and Information Security functions and governance mechanisms are often not ready to handle (Teane and Matlala, 2025). In terms of barriers to digital transformation in universities based on a systematic review – weak university strategies, resources, human capacity and culture are some of the identified barriers that can hinder safe modernisation of systems (Singun, 2025). A number of maturity studies in higher education also highlight that different stakeholders have very different views on the level of digital transformation happening at their institution with there often being a huge disconnect between the ambitions and the actual implementation (Bravo-Jaico et al., 2025). The same type of constraints are also reported by other researchers for smaller companies that have limited staff and poor defined processes which can lead to increased risk for example from the type of social engineering attacks as phishing, ransomware or poor access control (Awan and Alam, 2025).

A new crop of cybersecurity papers is framing zero trust as much as a governance model as a security architecture because it includes the necessity of continuous verification, strong policy enforcement and a definition of trust boundaries (NIST, 2025). The cloud-focused zero trust security model developed in this research points out that access decisions are based on identity, context, data classification of workloads and continuous authorization and not on traditional perimeter-based assumptions (NIST, 2023). This perspective on zero trust and cloud security also supports new cybersecurity governance recommendations focusing on leadership accountability within the Govern function and on incorporating cybersecurity risk into business and enterprise-level management and operations (NIST, 2024). These also support a prioritized set of safeguard information sharing and use models (NCIFP-01) that align cybersecurity governance to institutional priorities and direct activities such as asset management, access control, logging and recovery planning. Higher education, balancing as it does openness in academic communications with the need to maintain confidentiality of sensitive administrative information, also strongly benefits from governance-control alignment to prevent vulnerabilities that could develop between control points from being transformed into operational weaknesses due to policy gaps (ENISA, 2023a).

Our latest wave of research papers on the topic of zero trust explores how it is evolving as a concept from being a technical security control to becoming a governance model as well. The model includes aspects such as continuous verification, enforcement of policies and identification of trust boundaries (NIST, 2025). Our cloud zero trust security model research affirms that access decisions are made based on identity, context, data classification of workloads and continuous authorization versus traditional assumptions based on the perimeter (NIST, 2023). Our work on zero trust and cloud security also affirms the new NIST Cybersecurity Governance recommendations which include providing leadership within the Govern function and integrating cybersecurity risk into enterprise

and business-level management and operations (NIST, 2024). These recommendations also affirm the prioritized set of safeguard information sharing and use models (NCIFP-01) that tie cybersecurity governance to institutional priorities and activities such as asset management, access control, logging and recovery planning. Higher education, which depends on openness in the academic communications while at the same time needs to protect the confidentiality of administrative information, is also a good candidate for governance-control alignment of safeguards to avoid potential weaknesses between control points from becoming operational weaknesses due to policy and governance gaps (ENISA, 2023a).

The security field needs technical controls which work together with institutional users because students and staff members create a major security risk in locations where their attendance patterns change throughout the day (Armas and Taherdoost, 2025). University students served as study subjects because researchers wanted to investigate how three factors which include awareness and attitudes and risk perception affect cybersecurity adoption. The researchers discovered that human behavior needs to be handled through formal processes instead of using informal approaches (Adeshola and Oluwajana, 2025). The methods used in delivering cybersecurity training programs will have more positive effects when they integrate structured training with real-life situations and pre-set learning objectives rather than awareness training separately (Mukherjee et al., 2024). Based on the results obtained from the research studies, it is clear that the teaching method that involves interaction between the learner and instructor ensures more learning than lectures that require changes to meet current demands (Alnajim et al., 2023). In relation to the analysis of the policy concerning educational program strategy, there should be cybersecurity awareness programs set up throughout the university campuses instead of IT staff members who possess knowledge about cybersecurity (ENISA, 2022).

The research conducted by Sabillon et al. (2024) demonstrates that higher education audits reveal distinct operational differences between organizations which use digital forensics and incident response and disaster recovery methods to protect their security systems. National studies maintain that educational institutions use operational resilience and practice exercises and coordinated incident handling activities as essential elements of their cyber protection measures against cyber threats (CISA 2024). Businesses must implement rapid breach detection systems together with their containment measures and incident response processes because research indicates that breaches create substantial financial losses for organizations (IBM Security 2024). Three primary methods enable educational institutions to experience security breaches according to incident research data which includes credential theft and phishing attacks and software vulnerability exploitation (Verizon 2024). Organizations require incident detection systems along with response capabilities and learning systems to develop their capacity to handle emerging threats according to recent threat research findings (ENISA 2023a).

In line with this, studies on digital transformation in universities revealed that universities must “balance ideas and controls to ensure modernization does not introduce uncontrollable risk and erosion of trust in academic systems” (García-Peñalvo, 2021). Other ideas on digital transformation in higher education institutions revealed that it “involves governance, culture, services, and engagement with stakeholders, not simply purchasing new technology” (Gkrimpizi et al., 2024). Other studies revealed through case studies that “teaching innovation and

digital transformation in universities is best done when strategy, skill-building, and support are developed in conjunction" (Paños-Castro et al., 2024). Other recent studies revealed that "future-oriented transformations in higher education institutions rely on cyber resilience, secure digital ecosystems, and a state of readiness for AI and cloud-enabled operations" (Nazyrova et al., 2025). At a larger scale, studies on readiness in cloud adoption revealed that "differences in organizational capacity are driven by gaps in digital infrastructure, governance, and organizational capacity" (Tudor et al., 2025).

The research conducted across multiple studies demonstrated that academic institutions experience cybersecurity weaknesses, yet the majority of research studies examine specific technical components which include either web-based systems or platform technologies or security features instead of showing how academic institutions prepare themselves for governance and infrastructure and cloud computing implementation (Eshetu et al., 2024). Online higher education institutions show that conventional cybersecurity methods and AI-based security systems can coexist together yet implementing their combined approach proves difficult because of operational complications (Parambil et al., 2024). The research conducted about cybersecurity risks in university cloud systems delivered technical recommendations which institutions could implement yet the research faced limitations because it could not address all institutional challenges which would arise during their cloud development projects (Dong and Xie, 2025). The studies conducted about digitally connected classrooms demonstrate that educational institutions experience cybersecurity risks which affect their governance systems and academic programs and social activities thus educational institutions must conduct complete cybersecurity assessments instead of solving individual cybersecurity issues (Theodorio, 2025). The existing situation requires higher education institutions to conduct structured research which evaluates their cybersecurity governance systems and their infrastructure and cloud systems and their existing security gaps between established policies and actual infrastructure (Teane and Matlala, 2025).

Table 1. Comparative Analysis of Infrastructure Strategies

Feature	**Traditional/Basic Security Approach**	**Modern/Cloud-Based Security Strategy**	**Impact on Institutional Readiness**
Access Control	**Password-Only Authentication:** Users rely only on usernames and passwords.	**Multi-Factor Authentication (MFA):** Requires additional identity verification methods.	Improves protection against unauthorized access and account breaches.
Incident Response	**Manual Response Procedures:** Security issues are handled only after detection.	**Automated Incident Response Plans (IRP):** Uses predefined response and recovery procedures.	Reduces response time and minimizes damage during cyberattacks
Monitoring System	**Limited Monitoring:** Security checks are performed occasionally.	**Real-Time Monitoring and SIEM Systems:** Continuous monitoring and threat detection.	Enhances detection of suspicious activities and cyber threats.
Data Storage	**Local Server Storage:** Data is stored in a single	**Cloud-Based Infrastructure:** Data is	Improves scalability, backup reliability, and

	institutional server.	distributed and securely managed in the cloud.	system availability.
Security Governance	**Basic Policies:** Limited implementation of cybersecurity regulations	**Comprehensive Governance Policies:** Structured cloud and cybersecurity management.	Strengthens institutional compliance and overall cybersecurity readiness.
Workforce Capability	**Minimal Cybersecurity Training:** Staff have limited security awareness.	**Continuous Training and Staff Development:** Regular cybersecurity education and skill enhancement.	Increases institutional capability to prevent and respond to cyber threats.

3.0. Methodology

The researchers in this study used their research methodology to interview higher education institutions about their cybersecurity and cloud system management practices. The study outlined its research design through three components which included data collection methods and research instruments and evaluation methods used to assess governance and infrastructure and security procedures. The chapter describes the data analysis process which researchers used to find institutional gaps while assessing their overall readiness.

3.1. Research Design

The study examined cybersecurity and cloud infrastructure preparedness of higher education institutions through a quantitative research design. The researchers used a quantitative approach because it enabled them to gather measurable data which they assessed with standardized assessment tools.

3.2. Respondents and Sampling Technique

The study included 1003 participants who are students and employees who worked as IT staff members and administrators together with personnel who involved in managing cybersecurity operations and cloud infrastructure at selected higher education institutions that included USTP, SCC, MU and other institutions.

The researchers used purposive sampling to choose participants based on their knowledge and direct involvement in cybersecurity and cloud systems. The research team used Messenger and face-to-face distribution methods to recruit participants because these methods provided accessible and easy-to-use options for gathering data.

3.3. Research Instrument

The study used a structured survey questionnaire which researchers conducted through Google Forms as their main research instrument. The instrument was designed to assess the level of cybersecurity readiness and cloud infrastructure preparedness of higher education institutions.

The questionnaire included multiple sections which assessed essential domains of the following key areas:

- Cybersecurity Governance
- Risk management practices

- Incident response readiness
- Cloud infrastructure and service readiness

Each item in the questionnaire was measured on a 4-point Likert-scale with the following response options:

1 – Not in Place

2 – Partly in Place

3 – Mostly in Place

4 – Fully in Place

The survey added a third response option which allowed participants to select "Not Sure / N/A" when they needed to show their uncertainty about particular questions. The responses in this category were removed from the statistical analysis.

The research team created questionnaire items by using established cybersecurity frameworks and best practices to create an instrument which measures organizational cybersecurity readiness together with cloud security assessment. The research team conducted a review process for the questionnaire to establish its clarity and relevance before they distributed it.

3.4. Data Collection Method's

The study utilized a survey method for data collection. The questionnaire was distributed through Google Forms which enabled respondents to complete their answers on an internet-based platform. This method was selected because it effectively gathered information from numerous participants who were situated in various higher education institutions. The system delivered two benefits by streamlining data collection processes and reducing the likelihood of human errors during data entry.

3.5. Data Gathering Procedure

The researchers created a standardized questionnaire which they used to collect data according to their research objectives. The researchers created the survey which they sent to specific participants through Google Forms after choosing them through purposive sampling. After the researchers obtained study participant consent, they used Messenger and face-to-face contact to reach potential study participants. Respondents received enough time to complete the questionnaire whenever they wanted to. The Google Forms platform automatically collected and organized responses after respondents finished their assessments. The researchers processed the collected data through examination and purification before they transformed it into a format suitable for statistical analysis.

3.6. Data Analysis

The researchers assessed institutional cybersecurity and cloud infrastructure readiness through the application of descriptive statistical techniques which included weighted mean calculations.

Each response was assigned a numerical value based on a 4-point Likert scale, as follows:

Table 2. 4-point Likert Scale

Point	Interpretation
1	Not in Place
2	Partly in Place
3	Mostly in Place
4	Fully in Place

The weighted mean for each indicator was computed and interpreted using the following scale:

Table 3. Weighted Mean

Score Range	Interpretation
1.00 – 1.75	Not in Place
1.76 – 2.50	Partly in Place
2.51 – 3.25	Mostly in Place
3.26 – 4.00	Fully in Place

The results maintained their correctness and their validity because all responses which received the designation of "Not Sure / N/A" were not counted in the final computation.

The researchers used the statistical method to assess implementation levels across all indicators while they discovered the existing strengths and weaknesses and gaps in institutional cybersecurity and cloud readiness.

3.7. Ethical Consideration

The researchers maintained complete adherence to ethical standards throughout their study execution. A letter of intent and consent statement was provided at the beginning of the Google Forms survey to inform participants about the purpose of the study, the nature of their participation, and how the collected data would be used. The study allowed participants to choose whether to take part, and they could leave the study at any time without any consequences.

Although the study gathered minimal personal data which included email addresses and gender information and general location details but this information was used only to verify responses and to organize research activities. The research team maintained complete confidentiality of all collected data while preventing any possibility of identifying specific participants during result presentation. The researchers maintained exclusive access to all stored responses which were kept in a protected facility. Researchers maintained exclusive access to all survey responses which they stored in secure locations to protect against data loss and unauthorized access. Google Forms enabled automatic data collection and organization which reduced the need for manual data entry while maintaining accurate data records. The study reported data only in aggregated form which prevented any direct identification of individual participants or their respective institutions. The study implemented general data privacy principles to protect participant information while maintaining ethical research standards.

4.0. Results and Discussion

4.1. Respondent Profile

A total of 1003 respondents contributed in the study. The majority of respondents fall within the age range of 20–21, indicating mostly young and student-oriented sample. The results represent the views of people who use digital platforms to access university systems because they use these platforms. The gender distribution shows equal representation because 50.9% of respondents identify as male while 49.1% identify as female which leads to unbiased study results.

Figure 1 presents the gender distribution of the respondents who participated in the survey conducted by the researchers. Data show that both male and female respondents were represented in the study.

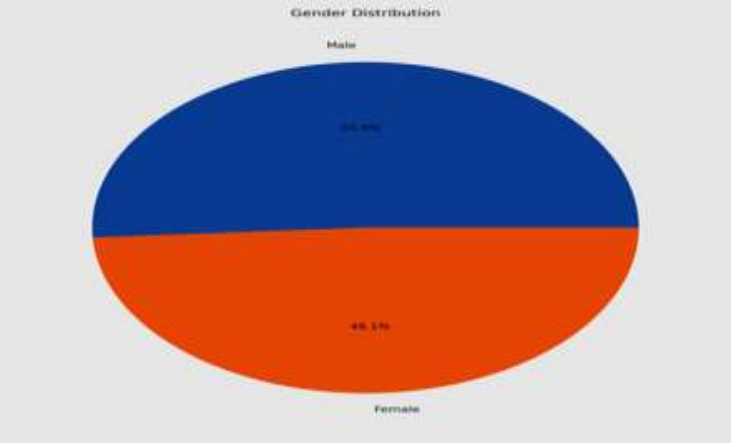

Figure 1. Gender Distribution of the 1003, survey respondents, showing that males represent 50.9% and females 49.1%, indicating an almost equal representation across gender in the study sample.

The results show that the gender distribution of the respondents is almost the same, with males at 50.9% and females at 49.1% out of the total 1,003 respondents. So, it looks like both male and female participants were basically represented in almost equal measure in the study. The small gap suggests that the findings are not pushed or dominated by one gender group, which in turn makes the responses more even, and that they can feel more dependable. Overall, this implies that the study really mirrors the views of both male and female respondents when they are judging cybersecurity frameworks and cloud infrastructure readiness in higher education institutions.

4.2. Institutional Profile

The study included respondents from both public institutions which accounted for 54.3% of the sample and private institutions which made up 46.8% of the sample. The study results show that 63.8% of participants attended schools which had student populations below 5000 because this group represents the findings from small to medium-sized higher education institutions. The research found that 59.6% of respondents reported their institutions used cloud services while a significant number of respondents showed uncertainty about cloud adoption which demonstrated their lack of knowledge about cloud adoption practices.

Figure 2 presents the distribution of respondents based on their institution type. Data show that the respondents came from different types of institutions, including Public (State/Local), Private, and other institutions.

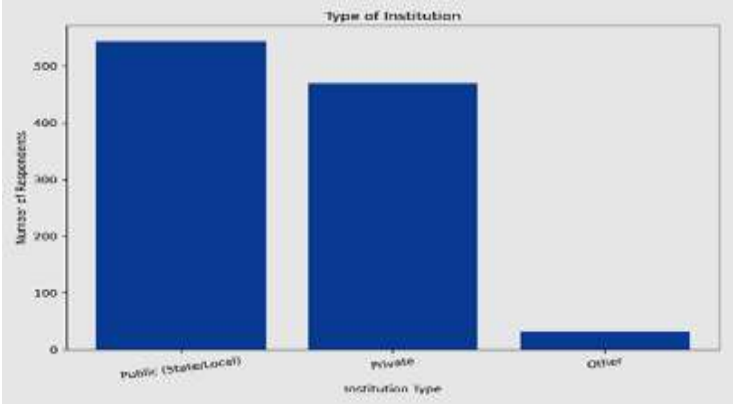

Figure 2. Distribution of respondents based on institution type, showing 54.3% from public institutions, 46.8% from private institutions, and a smaller percentage from other institution types, highlighting representation across different HEI types.

Displays the categorization of respondents based on their institution affiliations. This category includes their belongingness to institutions categorized as either Public (State/Local) Institutions, Private institutions, or other institutions. In the results of the survey taken, respondents belonging to Public (State/Local) Institutions represent the highest number as the majority at 54.3%, while those belonging to Private institutions rank second highest at a very overwhelming figure of 46.8%. Thirdly, respondents from other institutions form the smallest number of respondents in the survey. From this analysis, it is apparent that participation is equal between both sectors – the public sector and the private sector. However, it is clear that the respondents gathered are mainly small and medium size colleges whose student numbers do not surpass 5,000. This implies that despite the majority adopting cloud computing at 59.6%, the adoption procedures remain dubious.

4.3. Cybersecurity Readiness - Weighted Mean Analysis

Table 4. Cybersecurity Readiness Weighted Mean Summary

Indicator	Indicator	Weighted Mean	Interpretation
B1	Security policies/guidelines	2.74	Mostly in Place
B2	Assigned security roles	2.66	Mostly in Place
B3	Risk assessment practices	2.64	Mostly in Place
B4	Incident response plan	2.58	Mostly in Place
B5	Post-incident review	2.67	Mostly in Place
B6	Multi-factor authentication	2.80	Mostly in Place
B7	Role-based access control	2.70	Mostly in Place
B8	Monitoring systems	2.59	Mostly in Place
B9	Data backup practices	2.57	Mostly in Place
B10	Recovery capability	2.68	Mostly in Place
B11	Security training	2.63	Mostly in Place

Composite Mean: 2.68 (Mostly in Place)

The results indicate that cybersecurity readiness across institutions is consistently rated as 'Mostly in Place.' The analysis shows that basic security protections exist between the two security levels because the system lacks any security measure which reaches the 'Fully in Place' status. Institutions begin their security programs by establishing basic security measures which they need to improve until achieving standard security operations.

The research shows that organizations face security control challenges because they only partially implement security controls according to ENISA (2023) and NIST (2024) research. The institutions show difficulties in detecting threats and responding to them because their security systems which include incident response and monitoring capabilities achieved scores of 2.58 and 2.59 respectively.

Figure 3 Cybersecurity Readiness Weighted Mean (Bar Chart) The bar chart shows how different security indicators perform according to a 4-point Likert scale.

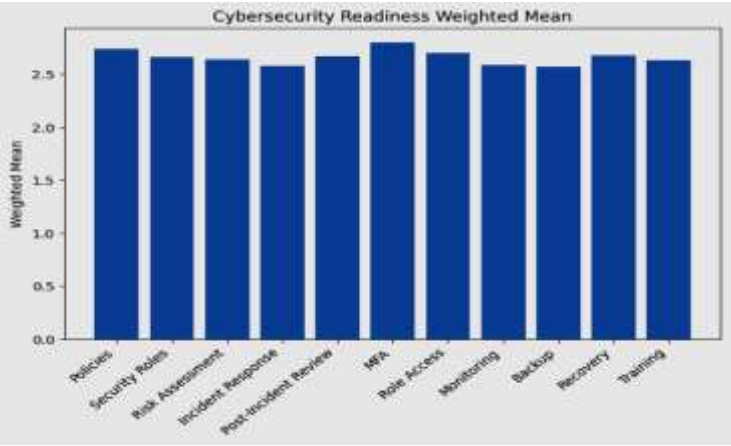

Figure 3. Cybersecurity Readiness Weighted Mean scores for eleven cybersecurity readiness indicators across surveyed institutions, measured on a 4-point Likert scale (1 = Not in Place, 4 = Fully in Place). Multi-factor authentication scored highest (2.80), while incident response plan scored lowest (2.58).

The bar chart shows the mean weights for the eleven criteria for cybersecurity readiness; all of which lie between 2.51 – 3.25 and hence can be termed as "Mostly in Place". Multi-Factor Authentication (B6) received the maximum score of 2.80, followed by Security Policies/Guidelines (B1) scoring 2.74 and Role-Based Access Control (B7) with 2.70. From the above results, it is apparent that the organization has set a very high priority for its identity and documentation. The other factors include Recovery Capability (B10) of 2.68, Post-Incident Review (B5) of 2.67, and Security Roles Assignment (B2) of 2.66. A middle score was also recorded for Risk Assessment (B3), with a score of 2.64, Security Training (B11), scoring 2.63, and Monitoring Systems (B8) scored 2.59. This indicates that these processes are operational but do not qualify for the "Fully in Place" status with a required threshold of 3.26. The lowest mean scores were reported in incident response plan (B4) with a score of 2.58 and data backup practices (B9) with a score of 2.57. In general, the chart reveals a steady readiness level for all variables; however, there is an evident requirement for improving the reactive process and data redundancy to reach the stage of full maturity in terms of cybersecurity.

4.4. Cloud Infrastructure and Service Readiness - Weighted Mean Analysis

Table 5. Cloud Readiness Weighted Mean Summary

Indicator	Description	Weighted Mean	Interpretation
C1	Cloud data policies	2.71	Mostly in Place
C2	Account management	2.65	Mostly in Place
C3	Security in adoption	2.78	Mostly in Place
C4	Tools/processes for cloud	2.56	Mostly in Place
C5	Staffing/support	2.38	Partly in Place

Composite Mean: 2.76 (Mostly in Place)

The research results demonstrate that institutions have achieved cloud technology implementation together with essential management procedures because they received a 'Mostly in Place' assessment for their cloud readiness. The cybersecurity readiness assessment shows similar results to cybersecurity readiness assessment because organizations have yet to achieve 'Fully in Place' status for their security measures which remain unoptimized and inactive.

The assessment presents higher scores for security considerations during adoption (2.89) and availability of tools (2.85) yet these scores do not demonstrate complete operational readiness. The findings show that institutions possess the necessary technologies for system operation yet they lack the governance and policy enforcement and workforce capacity needed to operate these systems. The analysis illustrates a common problem in cloud security research because organizations adopt new technology while they lack the necessary capabilities to implement it.

Figure 4 The Cloud Infrastructure Readiness Weighted Mean (Bar Chart) shows cloud operational status for different categories which achieved a combined average of 2.76.

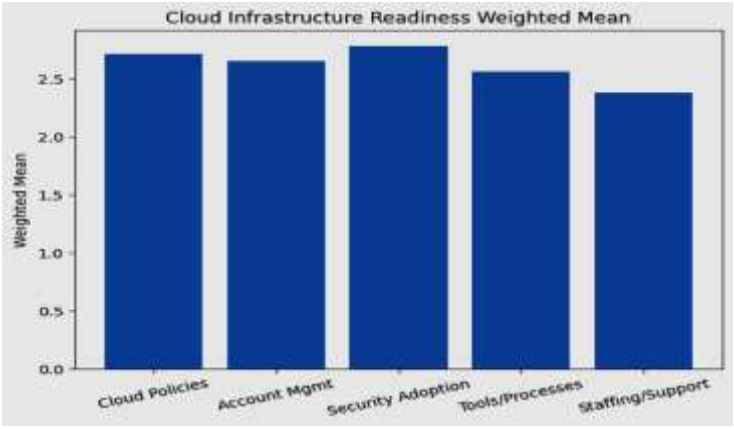

Figure 4. Cloud Infrastructure Readiness Weighted Mean scores for five cloud infrastructure readiness indicators, measured on a 4-point Likert scale. Security in adoption scored highest (2.78), while staffing/support scored lowest (2.38), indicating areas requiring improvement in operational readiness.

The bar graph shows, in a kind of weighted mean way, the scores across five main dimensions tied to Cloud Infrastructure Readiness. Security Adoption came out on top, with the highest weighted mean around (2.78), so it looks like the organization's main strong point sits in its security procedures and compliance measures. Right

behind that are Cloud Policies (2.71) and Account Management (2.65), and together they hint at a sturdy base for governance plus day-to-day administrative control. Tools/Processes got a smaller value, roughly (2.56), which feels like a sort of turning point where technical automation, and workflow integration are still being tuned, not fully locked in yet. The weakest weighted mean showed up in Staffing/Support, at approximately (2.38) , making it the least prepared area. In other words, even if the technical and policy foundations seem fairly mature, there are hurdles on the human side, like specialized competency gaps or limited access to dedicated support personnel that can keep the infrastructure steady. Overall, the data points to this idea that security and policies are clearly prioritized, but more investment in staffing and professional growth is needed, so the organization can reach complete operational readiness

4.5. Gap Analysis

The assessment results show a significant issue because all indicators show 'Mostly in Place' status yet the organization lacks high-maturity implementation for all its operational areas. The value cluster demonstrates that institutions have achieved basic security readiness yet they remain unable to reach advanced security capabilities.

The organization experiences operational deficiencies because its incident response systems and monitoring systems and staffing resources all receive lower assessment scores. The systems mentioned here are crucial components needed to achieve successful threat detection and threat response and threat recovery operations. The institution lacks protective measures against new cyber threats which specifically target their system weaknesses in detection and response capability.

5.0. Summary of Findings

The research shows that universities have established fundamental cybersecurity and cloud computing security measures which receive assessment scores that reflect implementation at the 'Mostly in Place' level. The institutions have not reached advanced cybersecurity maturity because they have not yet achieved complete implementation of all required security indicators.

5.1. Conclusions

The results show that higher education institutions have reached a stage of digital maturity where they use technology but their cybersecurity systems are not yet fully developed. The institutions established basic security controls which prevent effective control through security operations and governance because they lack complete system integration. The current security state of institutions becomes more dangerous because they have not yet reached security maturity while adopting new technologies. The institutions will face challenges in preventing dangers and identifying threats and reacting to cybersecurity attacks which will become more complex with modern digital systems unless they enhance their monitoring and incident response and governance capabilities.

5.2. Recommendations

Based on the conclusions of the study, the following recommendations are proposed:

For Universities and System Administrators

1. Conduct longitudinal studies to monitor cybersecurity and cloud maturity over time and assess progress alongside digital transformation efforts.
2. Increase sample size and include other educational institutions across the Philippines to better understand national cybersecurity preparedness.
3. Evaluate the impact of financial and resource allocation on staff training programs to bridge gaps in cybersecurity capabilities.
4. Perform technical audits using standards provided by frameworks such as NIST and ISO 27001 to ensure compliance.
5. Develop and implement comprehensive cloud governance policies to ensure standardized security measures across all departments.
6. Establish continuous professional development programs for IT staff to strengthen skills in cybersecurity and cloud management.

For IT Employees and System Managers

1. Conduct in-depth qualitative research, including case studies, to identify barriers preventing institutions from advancing from "Mostly in Place" to "Fully in Place" status.
2. Analyse potential benefits of emerging technologies, such as artificial intelligence (AI) and machine learning (ML), for real-time monitoring and emergency management.
3. Improve monitoring and incident response systems by integrating advanced technologies and best practices for enhanced operational readiness.
4. Implement regular testing and simulation exercises to ensure preparedness for cyber threats and system failures.
5. Strengthen multi-factor authentication (MFA) and role-based access controls to improve system security and access management.

For Future Researchers

1. Explore experimental or comparative research designs to test the effectiveness of different cybersecurity and cloud strategies.
2. Include variables such as governance, staff capabilities, and infrastructure maturity in future studies.
3. Adopt longitudinal research approaches to assess the evolution of cybersecurity and cloud maturity across multiple years and digital transformation stages.
4. Investigate the adoption and impact of AI and ML technologies in enhancing cloud infrastructure and cybersecurity readiness.
5. Conduct cross-institutional studies to compare practices between public and private universities for broader insights.

6. Examine user behavior and awareness as factors affecting cybersecurity readiness and system compliance.
7. Assess the effectiveness of policy implementation and operational compliance to identify persistent gaps.

Declarations

Source of Funding

This research did not benefit from grant from any non-profit, public or commercial funding agency.

Competing Interests Statement

The authors have declared that no competing financial, professional or personal interests exist.

Consent for publication

All the authors contributed to the manuscript and consented to the publication of this research work.

Author's Contributions

All authors contributed to the development and completion of the study. The authors participated in the conceptualization of the research, preparation of the survey questionnaire, data gathering, data analysis, interpretation of results, writing of the manuscript, and final review of the paper. All authors read and approved the final manuscript.

Informed Consent

Informed consent was obtained from all participants involved in the study before the conduct of data collection procedures.

Availability of data and material

Supplementary information such as the raw files of the data gathering and data analysis are available from the authors upon reasonable request.

Institutional Review Board Statement

Not Applicable.

Ethical Approval

The study was conducted in accordance with general ethical research principles. Participation was voluntary, and respondents were informed about the purpose of the study before answering the survey. The researchers maintained the confidentiality of the collected data and presented the results in aggregated form to protect the identity of individual participants and institutions.

Acknowledgments

The researchers hereby express their sincere appreciation to the University of Science and Technology of Southern Philippines – Oroquieta City for providing the opportunity and support in conducting this research study entitled "An Empirical Assessment of Cybersecurity Governance Frameworks, Incident Response Protocol, and Cloud

Infrastructure Operational Readiness in Higher Education Institutions: A Comprehensive Quantitative Correlation Analysis of Institutional Vulnerabilities and Policy Implementation Gaps" The researchers also extend their heartfelt gratitude to the faculty members of the Department of Information Technology for their guidance, encouragement, and valuable insights throughout the conduct of the study. Special appreciation is given to the 1,003 respondents, including students, administrators, and IT personnel from different higher education institutions, for their cooperation and participation during the data gathering process. The researchers are likewise thankful to all members of the research team for their dedication, teamwork, and contributions in completing this manuscript. Lastly, the researchers would like to extend their deepest gratitude to their adviser, Mr. Ginbert A. Fernandez, for his unwavering support, guidance, and encouragement which inspired the researchers to successfully accomplish this study.

Declaration of Artificial Intelligence

Artificial Intelligence tools may have been used to assist in improving the grammar, clarity, organization, and formatting of the manuscript. However, the authors remain fully responsible for the content, accuracy, analysis, interpretation, and final version of the manuscript. All interpretations, analyses, conclusions, and final written content remain the sole responsibility of the authors.

References

[1] 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.

[2] Adeshola, I., & Oluwajana, D.I. (2025). Assessing cybersecurity awareness among university students: Implications for educational interventions. Journal of Computers in Education, 12: 1283–1305. https://doi.org/10.1007/s40692-024-00346-7.

[3] Alnajim, A.M., Habib, S., Islam, M., AlRawashdeh, H.S., & Wasim, M. (2023). Exploring cybersecurity education and training techniques: A comprehensive review of traditional, virtual reality, and augmented reality approaches. Symmetry, 15(12): 2175. https://doi.org/10.3390/sym15122175.

[4] Armas, R., & Taherdoost, H. (2025). Building a cybersecurity culture in higher education: Proposing a cybersecurity awareness paradigm. Information, 16(5): 336. https://doi.org/10.3390/info16050336.

[5] Awan, M., & Alam, A. (2025). Cybersecurity threats and defensive strategies for small and medium firms: A systematic mapping study. Administrative Sciences, 15(12): 481. https://doi.org/10.3390/admsci15120481.

[6] Bravo-Jaico, J., Maquen-Niño, G.L.E., Germán, N., Valdivia, C., Alarcón, R., Aquino, J., & Serquén, O. (2025). Assessing digital transformation maturity in higher education institutions: A correlational analysis by actors and dimensions. Frontiers in Computer Science, 7: 1549262. https://doi.org/10.3389/fcomp.2025.1549262.

[7] Dong, X., & Xie, Y. (2025). Research on cloud computing network security mechanism and optimization in university education management informatization based on OpenFlow. Systems and Soft Computing, 7: 200225. https://doi.org/10.1016/j.sasc.2025.200225.

[8] Eshetu, A.Y., et al. (2024). Cybersecurity vulnerabilities and solutions in Ethiopian university websites. Journal of Big Data, 11: 118. https://doi.org/10.1186/s40537-024-00980-z.

[9] García-Peñalvo, F.J. (2021). Avoiding the dark side of digital transformation in teaching: An institutional reference framework for eLearning in higher education. Sustainability, 13(4): 2023. https://doi.org/10.3390/su13042023.

[10] Gkrimpizi, T., Peristeras, V., & Magnisalis, I. (2024). Defining the meaning and scope of digital transformation in higher education institutions. Administrative Sciences, 14(3): 48. https://doi.org/10.3390/admsci14030048.

[11] Lallie, H.S., Thompson, A., Titis, E., & Stephens, P. (2025). Analysing cyberattacks and cyber security vulnerabilities in the university sector. Computers, 14(2): 49. https://doi.org/10.3390/computers14020049.

[12] Mukherjee, M., Le, N.T., Chow, Y.-W., & Susilo, W. (2024). Strategic approaches to cybersecurity learning: A study of educational models and outcomes. Information, 15(2): 117. https://doi.org/10.3390/info15020117.

[13] Nazyrova, A., Miłosz, M., Bekmanova, G., Omarbekova, A., Aimicheva, G., & Kadyr, Y. (2025). The digital transformation of higher education in the context of an AI-driven future. Sustainability, 17(22): 9927. https://doi.org/10.3390/su17229927.

[14] Pang, M.S., & Tanriverdi, H. (2022). Strategic roles of IT modernization and cloud migration in reducing cybersecurity risks of organizations: The case of U.S. federal government. The Journal of Strategic Information Systems, 31(1): 101707. https://doi.org/10.1016/j.jsis.2022.101707.

[15] Paños-Castro, J., Korres, O., Iriondo, I., & Petchamé, J. (2024). Digital transformation and teaching innovation in higher education: A case study. Education Sciences, 14(8): 820. https://doi.org/10.3390/educsci14080820.

[16] Parambil, M.M.A., Rustamov, J., Ahmed, S.G., Rustamov, Z., Awad, A.I., Zaki, N., & Alnajjar, F. (2024). Integrating AI-based and conventional cybersecurity measures into online higher education settings: Challenges, opportunities, and prospects. Computers and Education: Artificial Intelligence, 7: 100327. https://doi.org/10.1016/j.caeai.2024.100327.

[17] Pitkar, H. (2025). Cloud security automation through symmetry: Threat detection and response. Symmetry, 17(6): 859. https://doi.org/10.3390/sym17060859.

[18] Sabillon, R., Bermejo Higuera, J.R., Cano, J., Bermejo Higuera, J., & Sicilia Montalvo, J.A. (2024). Assessing the effectiveness of cyber domain controls when conducting cybersecurity audits: Insights from higher education institutions in Canada. Electronics, 13(16): 3257. https://doi.org/10.3390/electronics13163257.

[19] Singun, A.J. (2025). Unveiling the barriers to digital transformation in higher education institutions: A systematic literature review. Discover Education, 4: Article 1. https://doi.org/10.1007/s44217-025-00430-9.

[20] Teane, L., & Matlala, N. (2025). Information security functions readiness amidst COVID-19 in higher education in South Africa. Trends in Higher Education, 4(2): 23. https://doi.org/10.3390/higheredu4020023.

[21] Theodorio, A.O. (2025). Discerning cybers' threats in an era of digitally connected classrooms: Lessons for the Nigerian higher education system and society. Discover Computing, 28: 68. https://doi.org/10.1007/s10791-025-09564-8.

[22] Tudor, C., et al. (2025). Cloud adoption in the digital era: An interpretable machine learning analysis of national readiness and structural disparities across the EU. Applied Sciences, 15(14): 8019. https://doi.org/10.3390/app15148019.

[23] Center for Internet Security (2021). CIS critical security controls version 8. https://www.cisecurity.org/controls/v8.

[24] Cloud Security Alliance (2024). Top threats to cloud computing 2024. https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2024.

[25] Cybersecurity and Infrastructure Security Agency (2023). #StopRansomware: Rhysida ransomware. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-319a.

[26] European Union Agency for Cybersecurity (2022). Cybersecurity education initiatives in the EU member states. https://www.enisa.europa.eu/publications/cybersecurity-education-initiatives-in-ms.

[27] European Union Agency for Cybersecurity (2023a). ENISA threat landscape 2023. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.

[28] European Union Agency for Cybersecurity (2023b). Cloud cybersecurity market analysis. https://www.enisa.europa.eu/publications/cloud-cybersecurity-market-analysis.

[29] IBM Security (2024). Cost of a data breach report 2024. https://www.ibm.com/reports/data-breach.

[30] Microsoft (2024). Cyber Signals: Cyberthreats in K-12 and higher education. https://www.microsoft.com/en-us/security/blog/2024/10/10/cyber-signals-issue-8-education-under-siege-how-cybercriminals-target-our-schools/

[31] National Institute of Standards and Technology (2023). A zero trust architecture model for access control in cloud-native applications in multi-location environments (NIST SP 800-207A). https://doi.org/10.6028/nist.sp.800-207a.

[32] National Institute of Standards and Technology (2024). The NIST cybersecurity framework (CSF) 2.0. https://doi.org/10.6028/nist.cswp.29.

[33] National Institute of Standards and Technology (2025). Implementing a zero-trust architecture (NIST SP 1800-35). https://doi.org/10.6028/nist.sp.1800-35.

[34] Sophos (2024). The state of ransomware in education 2024. https://www.sophos.com/en-us/blog/the-state-of-ransomware-in-education-2024.

[35] Sophos (2025). The state of ransomware in education 2025. https://www.sophos.com/en-us/blog/the-state-of-ransomware-in-education-2025.

[36] Verizon (2024). DBIR report 2024: Educational services. https://www.verizon.com/business/en-sg/resources/reports/dbir/2024/industries-intro/educational-data-breaches/

[37] Patel, R., & Gupta, S. (2026). Designing scalable rate limiting systems: Algorithms, architecture, and distributed solutions. ArXiv. https://arxiv.org/abs/2601.01234.