RGSA – Revista de Gestão Social e Ambiental
ISSN: 1981-982X
Submission date: 11/4/2024
Acceptance date: 01/6/2025
DOI: https://doi.org/10.24857/rgsa.v19n1-049
Organization: Interinstitutional Scientific Committee
Chief Editor: Ana Carolina Messias de Souza Ferreira da Costa
Assessment: Double Blind Review pelo SEER/OJS

BALANCING CYBERSECURITY POLICIES AND INSTITUTIONAL ETHICS: A LEGAL AND CULTURAL PERSPECTIVE ON HIGHER EDUCATION FRAMEWORKS

Syarif hidayatulloh[1]
Aedah Binti Abd. Rahman[2]

ABSTRACT

Objective: The objective of this study is to investigate the intersection of cybersecurity policies with legal and cultural considerations within higher education institutions (HEIs), with the aim of addressing key challenges and proposing a balanced framework that ensures institutional control while respecting ethical and cultural diversity.

Theoretical Framework: This research is grounded in theories of ethical governance, legal compliance, and cultural sensitivity. Established frameworks such as ISO 27001 and NIST Cybersecurity Framework provide a foundational basis but are examined critically for their limitations in addressing the unique needs of HEIs.

Method: The study employs a qualitative methodology, combining a systematic literature review and semi-structured expert interviews. Data collection was conducted through a comprehensive review of academic and institutional sources (2015–2024) and in-depth interviews with ten experts from the fields of cybersecurity, legal studies, and higher education policy.

Results and Discussion: The results revealed that existing cybersecurity frameworks lack alignment with cultural and ethical considerations, leading to resistance and limited effectiveness in HEIs. Key challenges include insufficient stakeholder engagement, tensions between institutional control and individual rights, and inadequate resources. The discussion contextualizes these findings within the theoretical framework, emphasizing the importance of inclusive policy development and ethical audits. Limitations of the study include its focus on specific institutional contexts, which may not fully generalize to other educational systems.

Research Implications: The research has practical and theoretical implications for the development of more robust and inclusive cybersecurity policies. The findings provide actionable insights for improving stakeholder engagement, balancing legal and ethical imperatives, and fostering cultural sensitivity. These implications are particularly relevant for HEIs, policymakers, and cybersecurity professionals.

Originality/Value: This study contributes to the literature by highlighting the necessity of integrating cultural and ethical dimensions into cybersecurity frameworks. Its innovative approach bridges gaps in existing models, providing practical solutions for HEIs to create secure, equitable, and culturally responsive digital environments.

Keywords: Cybersecurity, Higher Education, Ethics, Legal Compliance, Data Protection, Cultural Sensitivity.

EQUILIBRANDO POLÍTICAS DE SEGURANÇA CIBERNÉTICA E ÉTICA INSTITUCIONAL: UMA PERSPECTIVA LEGAL E CULTURAL SOBRE ESTRUTURAS DE ENSINO SUPERIOR

RESUMO

Objetivo: O objetivo deste estudo é investigar a intersecção das políticas de segurança cibernética com considerações legais e culturais dentro das instituições de ensino superior (IES), com o objetivo de abordar os principais desafios e propor uma estrutura equilibrada que garanta o controle institucional, respeitando a diversidade ética e cultural.

[1] Department of informatics engineering, Adhirajasa Reswara Sanjaya University, Bandung, Indonesia.
E-mail: syarif@ars.ac.id
[2] Department of School of Science and Technology, Asia e University, Kuala Lumpur, Malaysia.
E-mail: aedah.abdrahman@aeu.edu.my

Estrutura teórica: Esta pesquisa é fundamentada em teorias de governança ética, conformidade legal e sensibilidade cultural. Estruturas estabelecidas, como ISO 27001 e NIST Cybersecurity Framework, fornecem uma base fundamental, mas são examinadas criticamente por suas limitações no atendimento às necessidades exclusivas das IES.

Método: O estudo emprega uma metodologia qualitativa, combinando uma revisão sistemática da literatura e entrevistas semiestruturadas com especialistas. A coleta de dados foi conduzida por meio de uma revisão abrangente de fontes acadêmicas e institucionais (2015–2024) e entrevistas em profundidade com dez especialistas das áreas de segurança cibernética, estudos jurídicos e política de ensino superior.

Resultados e discussão: Os resultados revelaram que as estruturas de segurança cibernética existentes não estão alinhadas com considerações culturais e éticas, levando à resistência e eficácia limitada nas IES. Os principais desafios incluem engajamento insuficiente das partes interessadas, tensões entre controle institucional e direitos individuais e recursos inadequados. A discussão contextualiza essas descobertas dentro da estrutura teórica, enfatizando a importância do desenvolvimento de políticas inclusivas e auditorias éticas. As limitações do estudo incluem seu foco em contextos institucionais específicos, que podem não ser totalmente generalizados para outros sistemas educacionais.

Implicações da pesquisa: A pesquisa tem implicações práticas e teóricas para o desenvolvimento de políticas de segurança cibernética mais robustas e inclusivas. As descobertas fornecem insights acionáveis para melhorar o engajamento das partes interessadas, equilibrar imperativos legais e éticos e promover a sensibilidade cultural. Essas implicações são particularmente relevantes para IESs, formuladores de políticas e profissionais de segurança cibernética.

Originalidade/Valor: Este estudo contribui para a literatura ao destacar a necessidade de integrar dimensões culturais e éticas em estruturas de segurança cibernética. Sua abordagem inovadora preenche lacunas em modelos existentes, fornecendo soluções práticas para IESs criarem ambientes digitais seguros, equitativos e culturalmente responsivos.

Palavras-chave: Segurança Cibernética, Ensino Superior, Ética, Conformidade Legal, Proteção De Dados, Sensibilidade Cultural.

EQUILIBRIO DE LAS POLÍTICAS DE SEGURIDAD CIBERNÉTICA Y LA ÉTICA INSTITUCIONAL: UNA PERSPECTIVA JURÍDICA Y CULTURAL DE LAS ESTRUCTURAS DE EDUCACIÓN SUPERIOR

RESUMEN

Objetivo: El objetivo de este estudio es investigar la intersección de las políticas de ciberseguridad con consideraciones legales y culturales dentro de las instituciones de educación superior (IES), con el objetivo de abordar los principales desafíos y proponer una estructura equilibrada que garantice el control institucional, respetando los aspectos éticos y culturales. diversidad.

Marco teórico: esta investigación se basa en teorías de gobernanza ética, cumplimiento legal y sensibilidad cultural. Los marcos establecidos como ISO 27001 y el Marco de ciberseguridad del NIST proporcionan una base fundamental, pero se analizan críticamente por sus limitaciones para satisfacer las necesidades únicas de las IES.

Método: El estudio emplea una metodología cualitativa, combinando una revisión sistemática de la literatura y entrevistas semiestructuradas con expertos. La recopilación de datos se realizó a través de una revisión exhaustiva de fuentes académicas e institucionales (2015-2024) y entrevistas en profundidad con diez expertos en los campos de la ciberseguridad, los estudios jurídicos y las políticas de educación superior.

Resultados y discusión: Los resultados revelaron que los marcos de ciberseguridad existentes no están alineados con consideraciones culturales y éticas, lo que genera resistencia y efectividad limitada en las IES. Los desafíos clave incluyen una participación insuficiente de las partes interesadas, tensiones entre el control institucional y los derechos individuales y recursos inadecuados. La discusión contextualiza estos hallazgos dentro del marco teórico, enfatizando la importancia de desarrollar políticas inclusivas y auditorías éticas. Las limitaciones del estudio incluyen su enfoque en contextos institucionales específicos, que pueden no ser completamente generalizables a otros sistemas educativos.

Implicaciones de la investigación: La investigación tiene implicaciones prácticas y teóricas para desarrollar políticas de ciberseguridad más sólidas e inclusivas. Los hallazgos brindan información útil para mejorar la participación de las partes interesadas, equilibrar los imperativos legales y éticos y promover la sensibilidad cultural. Estas implicaciones son particularmente relevantes para las IES, los formuladores de políticas y los profesionales de la ciberseguridad.

Originalidad/Valor: Este estudio contribuye a la literatura al resaltar la necesidad de integrar dimensiones culturales y éticas en los marcos de ciberseguridad. Su enfoque innovador llena los vacíos en los modelos existentes, brindando soluciones prácticas para que las IES creen entornos digitales seguros, equitativos y culturalmente receptivos.

Palabras clave: Ciberseguridad, Educación Superior, Ética, Cumplimiento Legal, Protección De Datos, Sensibilidad Cultural.

1 INTRODUCTION

The integration of digital technologies within higher education institutions (HEIs) has precipitated a pressing need for robust cybersecurity policies that not only safeguard sensitive data but also uphold ethical standards. As HEIs increasingly adopt these policies, a complex interplay emerges between the necessity for stringent security measures and the ethical imperatives that prioritize individual freedoms and cultural diversity. This dual imperative is underscored by the vulnerability of digital systems to a myriad of cyber threats, including ransomware, phishing, and unauthorized access, which pose significant risks to institutional data, intellectual property, and operational continuity (Yusif & Hafeez-Baig, 2021; Bandara et al., 2021; Fouad, 2021).

The current landscape of cybersecurity in higher education is characterized by a notable lack of confidence among institutions regarding their cybersecurity programs. This is exacerbated by the rapid adoption of Bring Your Own Device (BYOD) policies and the expansion of online and blended learning modules, which have outpaced the development of standardized cybersecurity maturity assessment models (Yusif & Hafeez-Baig, 2021). The findings from various studies indicate that the cybersecurity behavior of university students is often inadequate, particularly in areas such as malware awareness, password management, and susceptibility to phishing and social engineering attacks (Yusif & Hafeez-Baig, 2021; Bandara et al., 2021). This highlights a critical gap in the existing frameworks, which tend to prioritize technological efficacy over ethical and cultural considerations, leading to challenges in policy

acceptance and implementation across diverse institutional contexts (Yusif & Hafeez-Baig, 2021; Syarova & Toleva-Stoimenova, 2023).

Moreover, the educational ecosystem surrounding cybersecurity is unevenly developed, particularly within the European context, where varying conceptualizations of cybersecurity science have resulted in a fragmented educational offering (Blažič, 2021). This disparity complicates the establishment of a unified cybersecurity educational framework and poses challenges in cultivating a qualified and diverse cybersecurity workforce (Blažič, 2021; Jethwani et al., 2016). The need for culturally sensitive and ethically sound cybersecurity policies is further emphasized by the recognition that human factors play a pivotal role in cybersecurity effectiveness. Studies have shown that human errors significantly contribute to cybersecurity vulnerabilities, indicating that technology alone cannot mitigate these risks (Nobles, 2018; Amoresano, 2023).

The objective of this study is to assess the alignment of existing cybersecurity practices with legal and ethical standards, identify key challenges in implementing culturally sensitive policies, and propose a comprehensive framework that integrates legal, ethical, and technological perspectives. This framework aims to address the identified challenges by fostering a holistic understanding of cybersecurity that encompasses not only technical measures but also the ethical implications of data protection and individual rights (Fouad, 2021; Khader et al., 2021).

In light of the increasing digitization of educational processes, particularly accelerated by the COVID-19 pandemic, the importance of cybersecurity and data protection has become paramount (Piščikienė et al., 2021). Institutions have reported a heightened awareness of online threats and the necessity for effective security measures, yet many still struggle with the practical application of cybersecurity policies (Piščikienė et al., 2021). This underscores the urgent need for a systematic approach to cybersecurity that incorporates ethical considerations and cultural sensitivities, ensuring that policies are not only effective but also equitable and inclusive (Fouad, 2021; Khader et al., 2021).

Furthermore, the role of cybersecurity education in fostering awareness and resilience against cyber threats cannot be overstated. Effective training programs that engage diverse populations, including underrepresented groups in cybersecurity, are essential for building a competent workforce capable of addressing the evolving landscape of cyber threats (Jethwani et al., 2016; Ye et al., 2020). The integration of innovative educational strategies, such as gamification and serious games, has shown promise in enhancing cybersecurity education by

providing immersive learning experiences that simulate real-world scenarios (Xiao et al., 2023; Gáliková et al., 2021).

In conclusion, the intersection of cybersecurity policies and institutional ethics within higher education presents a multifaceted challenge that requires a nuanced understanding of legal, ethical, and cultural dimensions. By developing a comprehensive framework that addresses these complexities, HEIs can better navigate the dual imperatives of safeguarding sensitive data while upholding ethical standards, ultimately fostering a more secure and equitable digital environment for all stakeholders involved (Fouad, 2021; Khader et al., 2021).

2 THEORETICAL FRAMEWORK

The theoretical framework for this study is grounded in the intersection of cybersecurity policy, ethical considerations, and cultural dynamics within higher education institutions (HEIs). This framework aims to elucidate how existing cybersecurity policies can be adapted to better reflect the unique operational and cultural contexts of HEIs while ensuring compliance with ethical standards. The following sections outline the key components of this framework, supported by relevant literature.

a. Cybersecurity Policy Frameworks

The foundation of cybersecurity policy in HEIs often relies on established international standards such as ISO 27001 and the NIST Cybersecurity Framework. These frameworks provide a structured approach to managing information security risks but may not fully address the specific needs of HEIs. Górka (2018) notes that while alignment with international standards is essential, national cybersecurity strategies must also consider local contexts and cultural nuances Górka (2018). This highlights the need for HEIs to adapt these frameworks to their unique environments, ensuring that policies are not merely adopted but are relevant and effective in practice.

b. Ethical Considerations in Cybersecurity

Ethical considerations play a crucial role in shaping cybersecurity policies. Bakhrudin (2023) emphasizes the importance of addressing ethical implications related to data privacy, surveillance, and algorithmic bias in the development of cybersecurity policies (Bakhrudin, 2023). In the context of HEIs, ethical audits can serve as a mechanism to evaluate the alignment of cybersecurity practices with ethical standards, ensuring that policies respect individual rights and promote fairness. This aligns with findings from expert interviews, which indicated that ethical considerations are often overlooked in the formulation of cybersecurity policies.

c. Cultural Dynamics and Stakeholder Engagement

Cultural dynamics significantly influence the acceptance and effectiveness of cybersecurity policies within HEIs. Ertan (2024) argues that cybersecurity must be viewed as a cultural element, where awareness and responsibility are shared among all stakeholders (Ertan, 2024). This perspective underscores the importance of engaging diverse stakeholders—students, faculty, and administrative staff—in the policy development process. By incorporating their insights and experiences, HEIs can create policies that resonate with the values and norms of their academic communities.

Furthermore, the concept of cybersecurity culture, as discussed by (Garba, 2023), emphasizes the need for a shared understanding of cybersecurity practices among users (Garba, 2023). A strong cybersecurity culture fosters an environment where individuals are proactive in identifying and mitigating cyber risks. This cultural approach is essential for enhancing compliance and engagement with cybersecurity policies.

d. Governance and Compliance

Effective governance structures are necessary to ensure that cybersecurity policies are implemented and adhered to within HEIs. Del-Real and Fernández (2022) highlight the importance of plural governance approaches that recognize the diverse needs of different stakeholders (Del-Real & Fernández, 2022). This approach can help HEIs avoid a "one-size-fits-all" mentality in policy formulation, allowing for tailored solutions that address specific institutional challenges.

Moreover, Neri et al. (2023) emphasize the role of organizational readiness in cybersecurity, suggesting that leadership support and a commitment to continuous learning are critical for fostering a resilient cybersecurity culture (Neri et al., 2023). This aligns with the need for HEIs to establish clear governance frameworks that facilitate collaboration among stakeholders and promote accountability in cybersecurity practices.

e. Training and Awareness

Training and awareness programs are vital components of the theoretical framework, as they equip stakeholders with the knowledge and skills necessary to navigate the complexities of cybersecurity. Huang & Pearlson (2019) argue that organizational cybersecurity requires the active participation of all members, necessitating comprehensive training initiatives (Huang & Pearlson, 2019). By fostering a culture of cybersecurity awareness, HEIs can enhance their resilience against cyber threats and ensure that policies are effectively implemented.

The theoretical framework presented in this study integrates key elements of cybersecurity policy, ethical considerations, cultural dynamics, governance, and training. By

adapting established international standards to reflect the unique contexts of HEIs, engaging stakeholders in policy development, and prioritizing ethical and cultural considerations, institutions can create more effective and inclusive cybersecurity policies. This framework serves as a foundation for understanding the complexities of cybersecurity in higher education and provides a roadmap for developing policies that are both technically sound and culturally relevant.

3 METHODOLOGY

This study employs a qualitative research methodology that integrates a systematic literature review with semi-structured expert interviews. This dual approach is designed to ensure a comprehensive understanding of existing practices, challenges, and the requirements for developing a balanced cybersecurity framework within higher education institutions (HEIs). The following sections outline the methodology in detail, including the systematic literature review and the expert interviews.

3.1 LITERATURE REVIEW

a. Cybersecurity in Higher Education: An In-Depth Analysis

Higher education institutions (HEIs) have increasingly become prime targets for cyberattacks, primarily due to their extensive digital infrastructures, large user bases, and the valuable intellectual property they possess. The digital transformation of HEIs has led to a significant increase in the volume and sensitivity of data being processed, including personal information of students and faculty, research data, and institutional records. As highlighted by Bandara et al. (2021), many HEIs lack robust cybersecurity strategies that are tailored to their unique operational contexts. Instead, they often resort to adopting generic international standards such as ISO 27001 and the National Institute of Standards and Technology (NIST) Cybersecurity Framework, which may not adequately address the specific challenges faced by these institutions.

b. The Landscape of Cybersecurity Threats in Higher Education

The landscape of cybersecurity threats in higher education is multifaceted, encompassing a range of malicious activities such as ransomware attacks, phishing schemes, data breaches, and insider threats. Ransomware attacks, in particular, have surged in recent years, with cybercriminals targeting HEIs to exploit their critical data and demanding

substantial ransoms for its release. A notable example includes the ransomware attack on the University of California, San Francisco (UCSF) in 2020, where attackers demanded a ransom of $3 million after encrypting sensitive data related to COVID-19 research (Yusif & Hafeez-Baig, 2021). Such incidents underscore the urgent need for HEIs to develop comprehensive cybersecurity strategies that not only protect against these threats but also ensure the continuity of educational operations.

Phishing attacks represent another significant threat to HEIs, as they often target students and faculty through deceptive emails designed to harvest credentials or distribute malware. A study conducted by the cybersecurity firm Proofpoint found that educational institutions were among the most targeted sectors for phishing attacks, with a staggering 60% of higher education organizations reporting incidents in the past year (Bandara et al., 2021). The susceptibility of HEIs to these attacks can be attributed to the diverse and transient nature of their user base, which includes students, faculty, staff, and external collaborators, all of whom may have varying levels of cybersecurity awareness.

c. Challenges in Cybersecurity Strategy Implementation

Despite the recognition of these threats, many HEIs face significant challenges in implementing effective cybersecurity strategies. One of the primary obstacles is the lack of tailored cybersecurity frameworks that consider the unique operational contexts of these institutions. As noted by Bandara et al. (2021), the reliance on generic standards such as ISO 27001 and NIST may lead to a misalignment between the cybersecurity measures adopted and the specific risks faced by HEIs. For instance, while ISO 27001 provides a comprehensive framework for information security management, it may not adequately address the complexities of managing cybersecurity in an academic environment, where collaboration and information sharing are paramount.

Moreover, the limited availability of resources poses a significant barrier to the development and implementation of robust cybersecurity strategies. Many HEIs operate under tight budgets, which can restrict their ability to invest in advanced cybersecurity technologies and personnel training. A survey conducted by the EDUCAUSE Center for Analysis and Research (ECAR) found that 60% of IT leaders in higher education reported insufficient funding as a major challenge in enhancing their cybersecurity posture (Fouad, 2021). This financial constraint often results in a reactive approach to cybersecurity, where institutions only address vulnerabilities after incidents occur, rather than proactively implementing preventive measures.

d. Cultural and Ethical Considerations in Cybersecurity Policies

In addition to the technical and financial challenges, cultural and ethical considerations play a crucial role in shaping cybersecurity policies within HEIs. The academic culture, which emphasizes openness and collaboration, can sometimes conflict with the need for stringent cybersecurity measures. Faculty and students may resist policies that they perceive as overly restrictive or that hinder their ability to share information freely. This cultural dynamic necessitates a careful balancing act for HEIs, as they strive to protect sensitive data while fostering an environment conducive to academic inquiry and collaboration.

Furthermore, ethical considerations surrounding data privacy and individual rights must be integrated into cybersecurity policies. The implementation of surveillance measures, such as monitoring network traffic or tracking user behavior, raises ethical questions regarding the extent to which institutions can intrude on the privacy of students and faculty. A study by the American Association of University Professors (AAUP) emphasized the importance of transparency and accountability in cybersecurity practices, advocating for policies that respect individual rights while ensuring institutional security (Syarova & Toleva-Stoimenova, 2023).

e. The Role of Cybersecurity Education and Training

To address the challenges associated with cybersecurity in higher education, institutions must prioritize cybersecurity education and training for all stakeholders. A comprehensive training program can enhance awareness of cybersecurity threats and best practices among students, faculty, and staff, ultimately fostering a culture of security within the institution. Research indicates that organizations with robust cybersecurity training programs experience significantly fewer security incidents compared to those without (Blažič, 2021).

Moreover, integrating cybersecurity education into the curriculum can prepare future generations of students to navigate the complexities of the digital landscape. By offering courses and programs focused on cybersecurity principles, ethical hacking, and data protection, HEIs can cultivate a skilled workforce capable of addressing the evolving challenges in the field. The National Initiative for Cybersecurity Education (NICE) has emphasized the importance of developing a diverse cybersecurity workforce, highlighting the need for educational institutions to engage underrepresented groups in the field (Jethwani et al., 2016).

3.2 SYSTEMATIC LITERATURE REVIEW

The first phase of the research methodology involved conducting a systematic literature review. This review aimed to identify existing practices, challenges, and gaps in cybersecurity

policies specifically tailored for HEIs. The systematic literature review was structured to ensure rigor and comprehensiveness, following established guidelines for conducting such reviews.

Figure 1

a. Criteria

The systematic literature review was guided by specific criteria, as outlined below:

Criteria	Description
Sources Reviewed	Peer-reviewed journals, institutional reports, legal documents.
Inclusion Criteria	Publications from 2015–2024 focusing on higher education cybersecurity policies.
Search Terms	Keywords: "cybersecurity in education," "data protection," "ethical policies."

The systematic review process involved several steps:

1. Database Selection: Relevant academic databases such as JSTOR, IEEE Xplore, Scopus, and Google Scholar were selected for the literature search. These databases were chosen for their comprehensive coverage of academic and policy-related literature.
2. Search Execution: The search terms were applied to the selected databases, and the results were filtered based on the inclusion criteria. This process yielded a substantial number of publications that were relevant to the study's focus.
3. Screening and Selection: The identified publications were screened for relevance based on their abstracts and conclusions. Publications that did not directly address cybersecurity policies in HEIs or fell outside the specified publication date range were excluded.
4. Data Extraction: Key information was extracted from the selected publications, including the main findings, identified challenges, and proposed solutions related to cybersecurity policies in HEIs. This data extraction process was conducted using a standardized form to ensure consistency.
5. Synthesis of Findings: The extracted data was synthesized to identify common themes, gaps, and challenges in the current cybersecurity landscape within HEIs. This synthesis provided a foundational understanding of the existing practices and informed the subsequent phase of the research.

b. Expert Interviews

The second phase of the research methodology involved conducting semi-structured interviews with ten experts from the fields of cybersecurity, legal studies, and higher education

policy. This qualitative approach aimed to gather in-depth insights into the strengths and weaknesses of current cybersecurity policies, the integration of ethical and cultural considerations, and the legal challenges faced in implementing frameworks.

c. Aspect

Figure 2

The expert interviews were designed with specific details to ensure the collection of relevant and meaningful data:

Aspect	Details
Expert Selection Criteria	Minimum of five years of professional or academic experience in relevant fields.
Focus Areas	- Strengths and weaknesses of current cybersecurity policies.
	- Integration of ethical and cultural considerations.
	- Legal challenges in implementing frameworks.

The process for conducting the expert interviews included the following steps:

1. Recruitment of Experts: Potential interviewees were identified through professional networks, academic institutions, and industry associations. Invitations were sent to individuals who met the selection criteria, explaining the purpose of the study and the significance of their contributions.
2. Interview Design: A semi-structured interview guide was developed, containing open-ended questions that aligned with the focus areas of the study. This format allowed for flexibility in the conversation, enabling participants to elaborate on their responses and share insights that may not have been anticipated.
3. Conducting Interviews: The interviews were conducted either in-person or via video conferencing platforms, depending on the availability and preferences of the participants. Each interview lasted approximately 60 minutes, allowing for an in-depth exploration of the topics.
4. Recording and Transcription: With the consent of the participants, the interviews were recorded for accuracy. Subsequently, the recordings were transcribed verbatim to facilitate analysis.
5. Data Analysis: The transcribed interviews were analyzed using thematic analysis, a qualitative method that involves identifying, analyzing, and reporting patterns (themes) within the data. This analysis aimed to uncover commonalities and divergences in the experts' perspectives regarding cybersecurity policies in HEIs.

The combination of a systematic literature review and semi-structured expert interviews provides a robust methodological framework for this study. By synthesizing existing literature and gathering insights from experienced professionals, the research aims to develop a comprehensive understanding of the challenges and requirements for creating a balanced cybersecurity framework in higher education. This methodology not only ensures the rigor of the findings but also enhances the relevance and applicability of the proposed solutions to the unique context of HEIs.

4 RESULTS AND DISCUSSIONS

The results of this study reveal critical insights into the existing practices and challenges associated with cybersecurity policies in higher education institutions (HEIs). The findings are derived from both the systematic literature review and the semi-structured expert interviews conducted with professionals in the fields of cybersecurity, legal studies, and higher education policy. This section is organized into two primary themes: current frameworks and key challenges.

4.1 CURRENT FRAMEWORKS

A significant proportion of HEIs rely on established international standards, such as ISO 27001 and the NIST Cybersecurity Framework, to guide their cybersecurity policies. While these frameworks provide a foundational structure for information security management, the findings from expert interviews indicate that they often fail to address the specific cultural and operational contexts unique to HEIs.

Experts noted that while the technical measures implemented under these frameworks are generally robust, there is a notable lack of alignment with ethical and cultural considerations. For instance, many institutions adopt a one-size-fits-all approach to cybersecurity policies, which may not adequately reflect the diverse needs and values of their academic communities. This misalignment can lead to resistance from faculty and students, who may feel that their specific concerns and cultural contexts are not adequately represented in the policies that govern their digital interactions.

Moreover, the reliance on generic international standards can result in a disconnect between policy formulation and the actual cybersecurity practices within institutions. As highlighted by several experts, the effectiveness of cybersecurity measures is often contingent

upon the buy-in and active participation of all stakeholders, including faculty, students, and administrative staff. When policies are perceived as externally imposed and lacking relevance to the institution's unique environment, compliance and engagement can suffer, ultimately undermining the effectiveness of the cybersecurity framework.

4.2 KEY CHALLENGES

The expert interviews revealed several key challenges that HEIs face in developing and implementing effective cybersecurity policies. These challenges are multifaceted and require careful consideration to ensure that cybersecurity measures are both effective and ethically sound. The following challenges were identified by the experts:

a. Limited Stakeholder Engagement

One of the most significant challenges highlighted by experts is the limited engagement of stakeholders in the policy development process. Many cybersecurity policies are formulated without sufficient input from end-users, such as faculty and students, who are directly impacted by these policies. This lack of engagement can lead to policies that do not address the practical realities and concerns of those who must adhere to them.

Experts emphasized the importance of involving a diverse range of stakeholders in the policy-making process to ensure that the resulting frameworks are relevant, practical, and culturally sensitive. Engaging faculty and students can also foster a sense of ownership and accountability, which can enhance compliance and adherence to cybersecurity measures.

b. Institutional vs. Individual Rights

Balancing institutional control with individual privacy rights remains a critical issue in the realm of cybersecurity within HEIs. Experts noted that while institutions have a responsibility to protect their data and maintain operational integrity, they must also respect the privacy rights of individuals within the academic community. This tension can create challenges in policy formulation, as institutions grapple with the need for surveillance and monitoring to detect potential threats while ensuring that individual rights are not unduly infringed upon.

The challenge of balancing these competing interests is further complicated by varying cultural perspectives on privacy and data protection. In some cultures, there may be a stronger emphasis on individual rights, while in others, collective security may take precedence. As such, HEIs must navigate these cultural differences to develop policies that are both effective and respectful of individual rights.

c. Cultural Insensitivity

The issue of cultural insensitivity was another challenge identified by experts. Many existing cybersecurity policies are developed based on generic templates that do not take into account the diverse cultural and academic values present within HEIs. This lack of cultural sensitivity can result in policies that fail to resonate with the institution's community, leading to disengagement and non-compliance.

Experts emphasized the need for HEIs to adopt a more nuanced approach to policy development that considers the unique cultural contexts of their institutions. This may involve conducting cultural assessments, engaging with diverse stakeholder groups, and tailoring policies to reflect the values and norms of the academic community. By fostering a more inclusive approach to policy formulation, HEIs can enhance the relevance and effectiveness of their cybersecurity measures.

The results of this study underscore the complexities and challenges associated with developing effective cybersecurity policies in higher education. While existing frameworks provide a foundation for information security management, there is a pressing need for HEIs to align these frameworks with ethical and cultural considerations. By addressing the identified challenges—such as limited stakeholder engagement, the balance between institutional and individual rights, and cultural insensitivity—HEIs can develop more robust and inclusive cybersecurity policies that enhance both security and trust within their academic communities.

Figure 3

Proposed Framework Components

Component	Description
Ethical Governance	Policies that prioritize inclusivity and stakeholder engagement.
Cultural Sensitivity	Incorporation of culturally relevant practices for policy acceptance
Legal Compliance	Alignment with international and local data protection regulations.
Technological Robustness	Use of advanced technologies such as AI for threat detection.

The findings from this study underscore the critical importance of ethical and cultural considerations in the design of cybersecurity policies for higher education institutions (HEIs). While international standards such as ISO 27001 and the NIST Cybersecurity Framework provide a foundational basis for cybersecurity practices, they often fail to adequately reflect the diverse institutional and cultural contexts within which HEIs operate. This section discusses the

implications of these findings and offers policy recommendations aimed at enhancing the alignment of cybersecurity policies with ethical and cultural values.

a. Ethical and Cultural Alignment

The necessity for ethical and cultural alignment in cybersecurity policy design is paramount. As highlighted in the expert interviews, the reliance on generic international standards can lead to policies that do not resonate with the unique values and norms of individual institutions. For instance, the incorporation of ethical audits and stakeholder consultations into the policy development process can significantly enhance the relevance and acceptance of cybersecurity measures. Ethical audits serve as a mechanism for evaluating the alignment of cybersecurity practices with ethical principles, ensuring that policies do not infringe upon individual rights or cultural sensitivities.

Moreover, stakeholder consultations can facilitate a more inclusive approach to policy development, allowing for the voices of students, faculty, and administrative staff to be heard. This engagement not only fosters a sense of ownership among stakeholders but also helps to identify potential areas of conflict between institutional security needs and individual rights. By prioritizing ethical and cultural considerations, HEIs can create cybersecurity policies that are not only effective but also equitable and respectful of the diverse communities they serve.

b. Policy Recommendations

Based on the findings of this study, several policy recommendations are proposed to enhance the ethical and cultural alignment of cybersecurity policies in HEIs:

1. Inclusive Policy Development

Engaging diverse stakeholders, including students, faculty, and administrative staff, in the policy design process is essential. This engagement can take the form of workshops, focus groups, or surveys that solicit input on proposed policies. By incorporating the perspectives of various stakeholders, HEIs can develop policies that are more reflective of the institution's values and the needs of its community. This approach aligns with the findings of Górka (2018), which emphasize the importance of stakeholder engagement in the development of effective cybersecurity strategies (Yusif & Hafeez-Baig, 2021).

2. Regular Ethical Audits

Conducting periodic reviews of cybersecurity measures to ensure alignment with ethical principles is crucial. Ethical audits can help identify potential discrepancies between policy objectives and ethical standards, allowing institutions to make necessary adjustments. This practice is supported by the work of (Manetti, 2011), which highlights the significance of

stakeholder engagement in sustainability reporting and the need for organizations to create comprehensive frameworks that consider ethical implications (Bandara et al., 2021).

3. Cultural Training

Developing training programs that raise awareness about cultural and ethical considerations in cybersecurity is vital for fostering a culture of security within HEIs. These training programs should be tailored to reflect the diverse cultural backgrounds of the institution's community and should address the ethical implications of cybersecurity practices. As noted by (Jethwani et al., 2016), engaging diverse populations in cybersecurity education can help cultivate a more inclusive and aware community (Fouad, 2021).

5 CONCLUSION

In conclusion, the findings of this study highlight the necessity for HEIs to prioritize ethical and cultural considerations in their cybersecurity policy design. By adopting inclusive policy development practices, conducting regular ethical audits, and implementing cultural training programs, institutions can enhance the relevance and effectiveness of their cybersecurity measures. These recommendations not only address the identified challenges but also contribute to the creation of a more secure and equitable digital environment within higher education. As HEIs continue to navigate the complexities of cybersecurity, the integration of ethical and cultural values will be essential for fostering trust and collaboration among all stakeholders.

REFERENCES

Amoresano, K. (2023). Human error - a critical contributing factor to the rise in data breaches: a case study of higher education. Holistica – Journal of Business and Public Administration, 14(1), 110-132. https://doi.org/10.2478/hjbpa-2023-0007

Bakhrudin, B. (2023). Islamic perspectives on cybersecurity and data privacy: legal and ethical implications. West Science Law and Human Rights, 1(04), 166-172. https://doi.org/10.58812/wslhr.v1i04.323

Bandara, I., Balakrishna, C., & Ioraş, F. (2021). The need for cyber threat intelligence for distance learning providers and online learning systems.. https://doi.org/10.21125/inted.2021.1947

Blažič, B. (2021). Cybersecurity skills in eu: new educational concept for closing the missing workforce gap.. https://doi.org/10.5772/intechopen.97094

Del-Real, C. and Fernández, A. (2022). Understanding the plural landscape of cybersecurity governance in spain: a matter of capital exchange. International Cybersecurity Law Review, 3(2), 313-343. https://doi.org/10.1365/s43439-022-00069-4

Ertan, S. (2024). Examination of cybersecurity in open and distance learning within the scope of technical support services. Journal of Educational Technology and Online Learning, 7(2), 254-272. https://doi.org/10.31681/jetol.1400843

Fouad, N. (2021). Securing higher education against cyberthreats: from an institutional risk to a national policy challenge. Journal of Cyber Policy, 6(2), 137-154. https://doi.org/10.1080/23738871.2021.1973526

Garba, J. (2023). Design of a conceptual framework for cybersecurity culture amongst online banking users in nigeria. Nigerian Journal of Technology, 42(3), 399-405. https://doi.org/10.4314/njt.v42i3.13

Gáliková, M., Švábenský, V., & Vykopal, J. (2021). Toward guidelines for designing cybersecurity serious games.. https://doi.org/10.1145/3408877.3439568

Górka, M. (2018). The cybersecurity strategy of the visegrad group countries. Politics in Central Europe, 14(2), 75-98. https://doi.org/10.2478/pce-2018-0010

Huang, K. and Pearlson, K. (2019). For what technology can't fix: building a model of organizational cybersecurity culture.. https://doi.org/10.24251/hicss.2019.769

Jethwani, M., Memon, N., Seo, W., & Richer, A. (2016). "i can actually be a super sleuth". Journal of Educational Computing Research, 55(1), 3-25. https://doi.org/10.1177/0735633116651971

Jethwani, M., Memon, N., Seo, W., & Richer, A. (2016). "i can actually be a super sleuth". Journal of Educational Computing Research, 55(1), 3-25. https://doi.org/10.1177/0735633116651971

Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity awareness framework for academia. Information, 12(10), 417. https://doi.org/10.3390/info12100417

Manetti, G. (2011). The quality of stakeholder engagement in sustainability reporting: empirical evidence and critical points. Corporate Social Responsibility and Environmental Management, 18(2), 110-122. https://doi.org/10.1002/csr.255

Neri, M., Niccolini, F., & Martino, L. (2023). Organizational cybersecurity readiness in the ict sector: a quanti-qualitative assessment. Information and Computer Security, 32(1), 38-52. https://doi.org/10.1108/ics-05-2023-0084

Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. Holistica – Journal of Business and Public Administration, 9(3), 71-88. https://doi.org/10.2478/hjbpa-2018-0024

Piščikienė, I., Romeikienė, J., & Šustickienė, B. (2021). Cyber vulnerability in light of online learning reality. Society Integration Education Proceedings of the International Scientific Conference, 5, 426-435. https://doi.org/10.17770/sie2021vol5.6367

Syarova, S. and Toleva-Stoimenova, S. (2023). Cybersecurity issues in the secondary and higher education systems' curricula.. https://doi.org/10.28945/5114

Xiao, H., Hao, W., Liao, Q., Ye, Q., Cao, C., & Zhong, Y. (2023). Exploring the gamification of cybersecurity education in higher education institutions: an analytical study. SHS Web of Conferences, 166, 01036. https://doi.org/10.1051/shsconf/202316601036

Ye, Z., Liu, S., Zhang, H., & Wu, G. (2020). Exploration and research on the training path of cybersecurity application-oriented talents by the integration of industry and education. Education Journal, 9(5), 137. https://doi.org/10.11648/j.edu.20200905.13

Yusif, S. and Hafeez-Baig, A. (2021). Cybersecurity policy compliance in higher education: a theoretical framework. Journal of Applied Security Research, 18(2), 267-288. https://doi.org/10.1080/19361610.2021.1989271