A QUALITATIVE INQUIRY INTO THE ROLE OF CORPORATE CYBERSECURITY INITIATIVES IN ENHANCING MSI AUDIT PREPAREDNESS

by

SHAUNYA C. ISHMAEL

BS, Clark Atlanta University, 1989

MS, Tuskegee University, 1991

A Research Paper Submitted to the School of Computing Faculty of

Middle Georgia State University in

Partial Fulfillment for the Requirements for the Degree

DOCTOR OF SCIENCE IN INFORMATION TECHNOLOGY

MACON, GEORGIA

2026

A qualitative inquiry into the role of corporate cybersecurity initiatives in enhancing MSI audit preparedness

SHAUNYA ISHMAEL, *Middle Georgia State University,* Shaunya.Ishmael@mga.edu

Abstract

As Minority-Serving Institutions (MSIs) navigate an increasingly hostile cybersecurity landscape, they face a paradox: the mandate for stringent regulatory compliance often outpaces their limited resources. Corporate partnerships can bridge critical capability gaps and enhance audit preparedness. This qualitative multiple-case study investigates the influence of external corporate cybersecurity initiatives on the audit preparedness and cybersecurity posture of seven MSIs. Utilizing Resource Dependence Theory (RDT) as a framework, the research explores how these institutions navigate significant resource constraints, including limited financial, human, and technical capital, by engaging Corporation X's (a pseudonym for a global Fortune 50 technology company) Cyber Maturity program. Through semi-structured interviews and document analysis, the study reveals a fundamental shift from a reactive posture to a security-focused one. Findings indicate that while these programs are vital for meeting stringent regulatory requirements, such as the National Institute of Standards and Technology NIST SP 800-171, they also introduce operational friction and raise concerns about long-term sustainability. According to the research, the most effective partnerships evolve from transactional exchanges to long-term relational collaborations, providing MSIs the strategic legitimacy needed to secure internal executive support and institutionalize cybersecurity as a core value.

Keywords: Cybersecurity, Minority-Serving Institutions (MSIs), Audit Preparedness, Resource Dependence Theory (RDT), Higher Education Institutions (HEIs)

Introduction

Higher Education Institutions (HEIs) are caretakers of highly sensitive and valuable data, including educational records, medical information, and the personal data of students, faculty, and staff (AL-Nuaimi, 2022). To maintain eligibility for Title IV federal funding, these institutions must adhere to rigorous regulatory standards, like the National Institute of Standards and Technology (NIST SP 800-171) and Gramm-Leach-Bliley (GLBA) guidelines (Wertheim, 2019; Federal Student Aid, 2020). Minority-serving institutions (MSIs), including Historically Black Colleges and Universities (HBCUs), face unique challenges in meeting these complex requirements due to significant financial and personnel resource constraints (Lamar, 2022; Khairi, 2024).

These limitations highlight a critical aspect of organizational behavior, explained by Resource Dependence Theory (RDT), which suggests organizations, particularly those with limited internal resources, must partner with external entities to ensure their survival, achieve strategic objectives, and navigate environmental uncertainty (Pfeffer & Salancik, 1978; Hillman et al., 2009). RDT emphasizes how institutional behavior remains constrained by power dependencies and the need for external capital, making it a suitable lens for examining how MSIs leverage corporate partnerships to mitigate resource scarcity. For

MSIs, specialized cybersecurity capabilities and compliance expertise constitute scarce, yet vital, internal resources (Fraczkiewicz-Wronka & Szymaniec, 2012). To bridge these gaps, some MSIs have engaged with external corporate initiatives, such as the Cyber Maturity program delivered by Corporation X (a pseudonym for a global Fortune 50 company), which offered a comprehensive suite of enhanced resources and support to bolster NIST SP 800-171 self-assessments and GLBA audit scores, including donated security products and services, a specialized Cyber Audit program, and direct access to compliance expertise (Corporation X, n.d.).

While existing literature documents the cybersecurity challenges facing HEIs and the importance of meeting compliance standards, a qualitative research gap remains regarding the lived experiences, perceptions, and nuanced implementation of targeted external programs within MSIs. Previous research has not adequately explored the specific mechanisms, perceived successes, or operational frictions personnel encountered during their engagement with such corporate initiatives.

This study adopts an interpretive approach to address this gap, examining how those involved understood and interpreted their experiences. By analyzing these experiences through an RDT lens, this research provides rich contextual insights to guide future support strategies, mitigate risks to federal funding, and enable policymakers and leaders to accurately assess the value of corporate partnerships in enhancing cybersecurity readiness at under-resourced institutions.

The purpose of this qualitative study was to explore and understand the lived experiences and perceptions of key institutional personnel regarding the influence of Corporation X's Cyber Maturity programs on their institution's cybersecurity posture and audit preparedness. The research will answer the following question:

RQ1: What overall themes will emerge from the Minority Serving Institution participants on how they perceive, experience, and interpret the value, effectiveness, and challenges of Corporation X's Cyber Maturity program in strengthening their institution's cybersecurity posture and audit preparedness?

The insights provided by this research contribute to a more nuanced understanding of the effectiveness of these external programs, inform future strategies to strengthen cybersecurity posture in under-resourced institutions, and highlight the potential gains enabled by strategic partnerships between corporations and HEIs.

Review of Literature

HEIs operate within a dynamic environment marked by competing priorities, particularly concerning the protection of data privacy for faculty, staff, and students. Cybersecurity at HEIs extends well beyond administrative compliance. Robust adherence to cybersecurity standards is essential for preserving institutional reputation and ensuring smooth, uninterrupted operations (AL-Nuaimi, 2022).

These institutions gather and manage large volumes of highly sensitive data, including educational and academic records, medical information, personal and health insurance data, and valuable intellectual property and research outputs (AL-Nuaimi, 2022; Amine, 2023; Othman, 2023; Yusif & Hafeez-Baig, 2023). This wealth of information makes them attractive targets for cybercriminals and other malicious actors (Lallie et al., 2023; Lallie et al., 2025; Yusif & Hafeez-Baig, 2023). The rapid transition to online

learning during the global pandemic further widened the attack surface for HEIs, leading to an increase in data breaches and exploitation (AL-Nuaimi, 2022).

Universities serve a diverse and transient user base comprised of students, faculty, researchers, staff, and visitors. These groups are frequently targeted by phishing and other cybersecurity attacks (Amine, 2023; Lallie et al., 2023; Wang, 2024). The core value of openness and academic freedom, while central to HEIs, can sometimes conflict with the security controls mandated by regulatory frameworks and industry standards (Ulven & Wangen; Kam et al., 2022). Additionally, the complexity of university network environments is heightened by users connecting from multiple locations and devices with varying security levels (Lallie et al., 2023; Lallie et al., 2025). Decentralized information technology (IT) management further complicates the security landscape, often leaving institutions insufficiently prepared to manage and mitigate IT risks (Ulven & Wangen, 2019; Amine, 2023).

Given these challenges, HEIs must prioritize and reinforce their cybersecurity posture, particularly regarding data management and Bring Your Own Device (BYOD) policies (Amine, 2023). Proactive and coordinated IT management is necessary to safeguard institutional networks, intellectual assets, and the personal data of all university stakeholders (Othman, 2023). Addressing these challenges is fundamental to maintaining their operational integrity and public trust (AL-Nuaimi, 2022; Amine, 2023).

The custodial role assumed by HEIs, while crucial for maintaining institutional reputation and operational efficiency, often leaves many of them ill-prepared to address IT risks (AL-Nuaimi, 2022). While the literature details these technical and structural issues, a qualitative research approach is essential for understanding the life experiences of personnel grappling with these complex risks and their perceptions of mitigation strategies.

The Regulatory and Threat Landscape for HEIs

HEIs manage large volumes of sensitive data, including educational records, medical information, and valuable intellectual property. Othman (2023) identifies eight recurring attack types, including malware, ransomware, website defacement, and denial-of-service attacks. Phishing and social engineering are especially prevalent, frequently targeting individuals with access to confidential or strategic data (Amine, 2023; Lallie et al., 2023; Wang, 2024). Ransomware has emerged as a leading cause of disruption, often compromising email accounts, personally identifiable information (PII), technical resources, and sensitive research assets (Lallie et al., 2023). The frequency and scale of data breaches in the education sector are also notable. Between 2005 and 2021, the sector experienced 1,850 data breaches, exposing over 28.6 million records, with universities accounting for approximately 87% of these compromised records (Wang, 2024).

The increasing reliance on third-party service providers for essential academic and administrative functions introduces additional vulnerabilities. Attacks on these providers can have direct and severe implications for university operations and data integrity (Lallie et al., 2025). From an RDT perspective, this reliance on external entities highlights the strategic risks of dependence on external resources and services. RDT suggests that as HEIs engage more with third-party vendors to meet critical needs, they become increasingly exposed to risks arising from these dependencies, which can undermine their ability to control and secure their own information assets (Pfeffer & Salancik, 1978; Lallie et al., 2025).

As cybersecurity threats and legal requirements continue to evolve, HEIs must navigate a landscape shaped by intersecting federal, state, and industry mandates. Compliance is not only a legal obligation but, for institutions receiving federal funding, is also essential to safeguarding sensitive personal, financial, and research data (Delaney, 2025; Price, 2022). Key regulations such as the Family Educational Rights and Privacy Act (FERPA), the GLBA, and the Privacy Act of 1974, along with state-specific privacy and breach-notification laws, create a complex compliance environment for HEIs (FSA, 2020; Price, 2022). For example, the GLBA Safeguards Rule directly links information security to eligibility for federal aid. Failure to comply can result in severe penalties, including financial sanctions or loss of Title IV funding (Delaney, 2025; Federal Student Aid, 2020). In response to these requirements, institutions are encouraged to adopt comprehensive technical standards such as ISO/IEC 27001, the NIST Cybersecurity Framework, and NIST SP 800-171 R2, which provide structured approaches to risk management and data protection (Amine et al., 2023; Apthorpe et al., 2024). Effective compliance involves regular auditing, measuring policy effectiveness, assigning clear responsibilities, and ongoing adaptation to new threats and technologies (Apthorpe et al., 2024; Alwahaibi et al., 2022).

Cybersecurity Strategies and Technology in HEIs

Effective cybersecurity in HEIs requires a comprehensive, institution-wide strategy that extends beyond the IT department. Strengthening governance is critical, with senior leadership responsible for elevating cybersecurity as a top institutional priority (Cheng & Wang, 2022). Developing clear cybersecurity policies, guidelines, and procedures demonstrates organizational commitment and provides IT personnel with well-defined roles and responsibilities. These policies must strike a balance between robust security controls and user accessibility to ensure successful adoption and compliance (Cheng & Wang, 2022).

RDT provides insight into the challenges HEIs face in implementing and maintaining effective cybersecurity measures. Institutions often rely on external resources, such as regulatory guidance, vendor solutions, or philanthropic support (e.g., technology donations), to bridge gaps in their security posture. Targeted interventions, such as corporate donation programs, may help address resource disparities but also require careful integration with institutional priorities and risk management frameworks.

Adopting technological standards and best practices is fundamental to building a resilient cybersecurity defense. Routine actions such as keeping operating systems up to date, installing and maintaining antivirus software, performing regular data backups, implementing strong password policies, and enabling multi-factor authentication (MFA) are essential (Nassoura, 2022). Modern strategies, such as Single Sign-On (SSO), Virtual Private Networks (VPNs), Virtual Desktop Infrastructure (VDI), and encryption, provide additional protection, yet adoption remains inconsistent across the sector (Cheng & Wang, 2022; Apthorpe et al., 2024). As artificial intelligence (AI) becomes both a tool for attackers and defenders, HEIs will need to prepare for AI-driven threats and integrate AI-based solutions with appropriate oversight (Cheng & Wang, 2022). As a result, HEIs are increasingly transitioning from a “maturity-based” to a “risk-based” approach to cybersecurity, emphasizing continuous, organization-wide risk management rather than simply achieving compliance milestones (Cheng & Wang, 2022).

Human Behavior and Cybersecurity Culture

While traditional approaches to cybersecurity in HEIs have focused on mitigating risks associated with human error, recent advancements highlight the potential of leveraging human behavior as a proactive defense mechanism. Innovative strategies, such as behavioral analytics, are increasingly used to identify

anomalies in user activity that may signal a security threat, enabling early intervention without relying solely on technical controls. Rather than attributing breaches solely to human error, scholars advocate a socio-technical perspective that considers the interactions among users, institutional culture, and technical systems (Almuhammadi & Alsaleh, 2017; Parsons et al., 2017). This approach recognizes that policy effectiveness depends on how well security procedures align with user workflows, academic values, and the broader organizational climate.

Higher education's core values and culture can sometimes make it challenging to implement stringent security practices (Kam et al., 2022). The emphasis on academic freedom, openness, autonomy, and collaboration distinguishes HEIs from industry settings where trade secrets are protected at all costs (Ulven & Wangen, 2019). Kam et al. (2022) propose a flexible approach to information security management, emphasizing open communication, collaboration, and team spirit, which may align better with the culture of higher education than a purely controlled approach focused on top-down decision-making and policy enforcement. However, policy development remains a crucial step in demonstrating commitment and setting a clear plan (Cheng & Wang, 2022). Ultimately, human behavior and organizational culture are key drivers of compliance with security policies, influencing whether users adhere to measures designed to protect institutional resources (Yusif & Hafeez-Baig, 2023). Yusif and Hafeez-Baig (2023) found that factors such as unfair procedures and outcomes, slow rule enforcement, lack of accountability, and unfavorable organizational culture can lead to violations of information security policies. Their research states the primary goal of building a cybersecurity culture is to shape how people and groups think, act, and feel about cybersecurity when using information technology.

Leadership engagement and visible support for cybersecurity initiatives are critical for success, as they help integrate security into the institutional identity and normalize secure practices as part of daily operations (Almuhammadi & Alselah, 2017). From an RDT perspective, institutions with greater access to expertise and funding are better equipped to invest in advanced, adaptive training and culture-building interventions. At the same time, resource-constrained HEIs may struggle to sustain such programs (Pfeffer & Salancik, 1978).

Auditing and Assessment Practices

Auditing and assessment practices are essential components of a comprehensive cybersecurity strategy in higher education, serving as mechanisms to evaluate the effectiveness of controls and identify emerging vulnerabilities (Wertheim, 2019; Sabillon et al., 2024). The evolving perception of cybersecurity as a core business risk requires institutional governance to prioritize regular, risk-based audits and to integrate findings into broader decision-making processes (Wertheim, 2019).

However, audit effectiveness is frequently constrained by challenges in defining audit scope and capturing the full range of institutional risks, including human and cultural factors that technical assessments alone may overlook (Sabillon et al., 2024; Delaney, 2025). While frameworks such as NIST SP 800-171 provide structure for technical evaluations, there remains a lack of consensus on which specific domains and controls to prioritize, resulting in inconsistent audit practices across institutions (Sabillon et al., 2024).

From the perspective of RDT, the effectiveness and comprehensiveness of cybersecurity audits in HEIs are strongly influenced by the institution’s access to external expertise, funding, and technological resources. Resource-constrained institutions often rely more heavily on external vendors or third-party auditors, which can shape both the scope and depth of cybersecurity assessments (Hillman et al., 2009; Pfeffer & Salancik,

1978). This reliance may introduce risks such as over-standardization, reduced contextual awareness, or potential misalignment with the institution's unique culture and risk profile, ultimately impacting audit outcomes (Hillman et al., 2009).

Unique Challenges for Minority Serving Institutions

MSIs, including HBCUs, face intensified and distinct cybersecurity and data governance challenges rooted in persistent resource limitations and historical inequities (Khairi, 2024; Burnett, 2020). Compared to larger, predominantly white institutions (PWIs), HBCUs often operate with constrained financial resources, limiting their ability to fund specialized cybersecurity staff, implement modern tools, and maintain up-to-date IT infrastructure (Khairi, 2024; Lamar, 2022). This financial disparity often results in gaps in data quality, security, and compliance and forces existing personnel to juggle multiple roles, detracting from consistent policy enforcement and focused risk management (Khairi, 2024).

Technological fragmentation is another recurring issue. Outdated and decentralized IT systems across departments create data silos, complicating integration and standardization efforts, and amplifying the risk of breaches due to inconsistent or insufficient controls (Khairi, 2024). Budget constraints and limited technical expertise further hinder efforts to establish centralized, secure, and well-governed data environments.

Cultural commitments and historical missions also shape cybersecurity priorities at HBCUs. A strong emphasis on protecting student privacy and serving marginalized communities can sometimes take precedence over formalized governance or rigorous security implementation (Khairi, 2024). Engaging diverse internal stakeholders, each with different priorities and varying levels of security awareness, also adds another layer of complexity to governance initiatives.

Competing institutional priorities, such as addressing the immediate needs of student success and academic programming, often take precedence over long-term cybersecurity investments. This dynamic, combined with regulatory compliance requirements and the expectation of accountability from accrediting bodies and funding agencies, creates significant pressure on already stretched resources (Khairi, 2024; Burnett, 2020). Accreditation challenges are especially acute for HBCUs. A disproportionate number of these institutions have faced heightened risk of accreditation loss, often linked to chronic underfunding and broader financial instability (Burnett, 2020). Loss of accreditation can trigger a cascade of consequences, including loss of Title IV eligibility and access to federal funding, further compounding institutional vulnerabilities (Federal Student Aid, 2020).

Political and external pressures also play a significant role. HBCUs' heavy reliance on public funding exposes them to political shocks at the state and federal levels. It attempts to control external operations, potentially disrupting resource allocation for cybersecurity and related priorities (Coupet, 2017). Although federal funding has been designated for HBCUs and Tribal institutions, restrictive usage policies and insufficient oversight often prevent these funds from fully addressing underlying resource inequities (Coupet, 2017).

These persistent and multifaceted resource constraints reinforce a central argument of RDT. Organizations facing resource gaps must turn to external entities to acquire the support necessary for survival and compliance (Pfeffer & Salancik, 1978). For MSIs, particularly for HBCUs, this frequently means seeking partnerships with external organizations and with industry to access technology, expertise, and funding

essential to meeting cybersecurity and regulatory demands. Understanding how MSI personnel experience and interpret these dependencies and partnerships provides a vital lens for assessing the effectiveness and sustainability of such collaborations.

Resource Dependence Theory (RDT) in Higher Education

RDT provides a framework for understanding how HEIs manage environmental uncertainty by acquiring external resources. Johnson (1995) applied RDT to examine how universities manage relationships with external stakeholders, noting how dependence on specific funding sources influences institutional decision-making and strategic planning. This perspective views the university as an open system where power dynamics between the institution and its resource providers shape academic and administrative goals.

Slaughter and Leslie (1997) further utilized RDT to analyze how universities shifted toward entrepreneurial activities to secure external revenue. In their view, universities have become increasingly dependent on corporate and private funding to maintain research missions, illustrating how shifts in public funding force institutions to seek external partners. This shift changes internal priorities to align with those partners' interests.

Morphew (2009) applied RDT to explain why institutions engage in inter-institutional collaborations. These partnerships allow colleges to pool resources, reducing environmental uncertainty and ensuring long-term institutional survival. The research highlights how institutions with limited internal capital seek alliances with peers to gain economies of scale and improve their competitive position within the higher education landscape.

Hatch (2013) explored how smaller, tuition-dependent institutions use mergers to mitigate resource scarcity. Using RDT, the study explains how the threat of closure drives institutions to seek external partners for financial stability. This research underscores the role of resource dependence in driving structural changes in higher education, where survival necessitates surrendering some institutional autonomy in exchange for fiscal security. These applications of RDT demonstrate its utility in explaining how resource-constrained institutions navigate external pressures to maintain operational integrity.

External Support and Partnerships

External support and industry-academia partnerships offer avenues to enhance cybersecurity posture by providing access to best practices, technology, and funding (Towhidi & Pridmore, 2023). Corporation X's Cyber Maturity program, for example, provides resources such as security software, installation services, training, and compliance expertise that directly address the identified resource dependencies (Corporation X, n.d.). Other examples of such partnerships include initiatives by organizations such as the National Cybersecurity Alliance and vendor programs for educational institutions. By expanding access to expertise and technology, these initiatives can effectively reduce the "transaction costs" identified in RDT and associated with the development of internal cybersecurity capabilities (Feng et al., 2025). While these partnerships are increasingly vital, their real-world implementation and perceived impact, particularly from the perspective of institutional personnel, remain underexplored, creating an experiential research gap.

The literature review suggests that while governance strategies and best practices continue to evolve, under-resourced institutions, such as MSIs, often struggle to implement them consistently. While the literature touches on aligning cybersecurity efforts with industry needs (Towhidi & Pridmore, 2023) and highlights

collaborative pathways between industry and academia (Zafar et al., 2024), it falls short of examining how these partnerships are experienced by institutional personnel and what specific elements contribute to their success in achieving regulatory or audit outcomes. This gap is where RDT offers a robust framework for interpreting narratives of how measurable improvements in the organization's outcomes and capabilities can be achieved through interventions by external partners (Pfeffer & Salancik, 1978). This study tested the theory by examining, through qualitative inquiry, whether Corporation X's Cyber Maturity initiatives enhanced audit readiness, regulatory compliance, and the closure of cybersecurity gaps identified at MSIs, from the perspective of key personnel.

Methodology

The research used a qualitative multiple-case study to explore the impact of Corporation X's Cyber Maturity Program on MSIs' cybersecurity posture and audit preparedness. To facilitate institutional cybersecurity improvements, Corporation X collaborated with participating institutions by pairing them with a dedicated partner to guide self-assessments and conduct gap analyses aligned with NIST standards. Through a commitment of more than $100 million, Corporation X provided five years of complimentary security software, installation support, training, optimization, and adoption services (Corporation X, n.d.). This approach was chosen to provide a rich, in-depth understanding of the complex interplay of factors within specific institutional contexts. The initiative also provided a one-year software license for a centralized repository to compile, manage, and store audit compliance data. The multiple-case study design was particularly suitable for exploring contemporary phenomena in real-life contexts, especially when the boundaries between the phenomenon and its context are unclear (Yin, 2018). Each MSI interviewed as part of the study served as an individual case, enabling cross-case analysis to identify patterns and variations (Stake, 1995; Merriam & Tisdell, 2016).

The researcher, serving as both the designer and implementer of the program, acknowledged an active role in the interpretive process. With expertise in Cybersecurity, Project and Program Management, and a significant professional focus on MSIs, particularly HBCUs, the researcher brought considerable theoretical sensitivity to the study. This background enabled a nuanced understanding of the technical and regulatory complexities inherent in MSI audits. To mitigate potential personal bias during data collection and analysis, the researcher maintained a reflexive journal throughout the research process.

Research Paradigm and Positionality

The research was guided by RDT, which fits best with a postpositivist view of the theory. It was applied within an interpretivist research paradigm, consistent with Creswell and Poth's (2018) guidance on the flexible use of theory in qualitative inquiry. RDT serves as the ideal theoretical framework for this study because it explicitly addresses the power imbalances and resource scarcities inherent in the MSI landscape. While other organizational theories focus on internal processes, RDT prioritizes the external pressures forcing institutions to seek partnerships for survival. By adopting this framework, the study captures the structural reality of resource-constrained institutions attempting to meet federal mandates. This theory provides a mechanism for interpreting the lived experiences of personnel as they navigate dependencies between their institutions and external corporate entities (Pfeffer & Salancik, 1978).

From an epistemological perspective, RDT seeks to explain how organizations manage uncertainty by acquiring and leveraging external resources. Knowledge is generated through participants' interpretations of their experiences navigating these dependencies, aligning with an interpretivist epistemology (Creswell & Poth, 2018). In terms of axiology, the study acknowledges the role of values in qualitative inquiry. Given the historical underfunding and marginalization of MSIs, considerations of equity, access to resources, and institutional survival influence the interpretation of the findings. Researcher positionality and reflexive journaling support analytic transparency, rigor, and credibility.

Methodological Alignment

RDT aligns with the qualitative multiple-case study design by providing a structured way to interpret the strategic value of external support. This theory is particularly well-suited to answer the research question, as it provides a framework for analyzing the transaction costs and power dynamics involved in corporate-academic partnerships. By viewing the Cyber Maturity program as a resource injection, the study evaluates how these institutions manage environmental uncertainty while balancing the potential loss of autonomy (Hillman et al., 2009). This approach allows for a deeper understanding of how institutional leaders leverage prestige and resources to influence internal decision-making processes.

RDT also provides an analytic lens for examining challenges associated with integrating external support, consistent with the research question, and interpreting the strategic value of corporate partnerships within resource-constrained environments. This multiple-case study design remains appropriate for examining complex organizational phenomena in the real world (Yin, 2018). RDT ensures the research remains grounded in the structural realities of institutional behavior, providing a robust framework for assessing the effectiveness of corporate-academic partnerships.

Case Selection and Participant Sampling

MSIs were selected using a criterion-based sampling strategy for in-depth analysis at the individual institutional level, which served as the primary unit of analysis (Merriam & Tisdell, 2016; Yin, 2018). The participant pool and the designation of small, medium, and large institutions were strictly based on the participant universe for the Corporation X Cyber Maturity Program (Corporation X, n.d.). Eligible cases were drawn from institutions officially designated as MSIs that actively participated in Corporation X's Cyber Maturity Program. To capture a diverse range of perspectives from the eligible pool across varying resource levels and organizational complexities, the final sample comprised seven institutions: two small, two medium, and three large MSIs. This specific distribution of institutional sizes was intentionally selected to ensure a robust cross-case analysis. By capturing institutions across this spectrum, the study accounted for varying degrees of resource dependency and administrative complexity inherent in the MSI landscape. The sample size of seven was determined by the principle of data saturation, in which the depth of information gathered from each case provided sufficient insight to identify recurring patterns and thematic variations, without the need for further data collection (Merriam & Tisdell, 2016; Yin, 2018). To ensure anonymity, institutions were assigned codes as outlined in Table 1.

Participant selection employed maximum-variation purposive sampling, targeting eight individuals with direct experience in the program's assessment, audit, training, and implementation phases (Creswell & Poth, 2018). This focus ensured that participants could offer informed and relevant perspectives on the program's outcomes and challenges. Snowball sampling was employed to broaden the participant pool, as illustrated by the inclusion of two interviews from one university (Medium A1 and Medium A2), where an initial

participant identified another key team member involved in the implementation (Creswell & Poth, 2018). This dual approach was particularly suited to capturing a comprehensive, nuanced understanding of how the program functioned across different institutional contexts (Stake, 1995; Yin, 2018).

Table 1: Participant and Case Overview

Case ID	Institution Size	Participant Role	Sampling Method
Small A	(0 - 3,500)	Former Provost	Criterion-based Purposive
Small B	(0 - 3,500)	IT Oversight/Administration	Criterion-based Purposive
Medium A1	(3,500 - 7,000)	Chief Information Officer	Criterion-based Purposive
Medium A2	(3,500 - 7,000)	AVP Information Management	Snowball (via Medium A1)
Medium B	(3,500 - 7,000)	Chief Information Security Officer (CISO)	Criterion-based Purposive
Large A	(7,000+)	Vice President of IT	Criterion-based Purposive
Large B	(7,000+)	Director of IT Infrastructure	Criterion-based Purposive
Large C	(7,000+)	Security Manager/Faculty	Criterion-based Purposive

Data Collection

The primary data was collected through semi-structured interviews conducted via Webex secure video conferencing. This format ensured consistency through a standardized interview protocol while allowing the flexibility to probe emerging insights (Cresswell & Poth, 2018). The interview protocol was grounded in RDT, specifically examining how external resources, such as software, expertise, and training, mitigated internal resource scarcity and environmental uncertainty.

Interviews lasted 30-60 minutes and were recorded and transcribed with participants' consent. To enhance data richness, institutional cybersecurity policies and, where available, redacted audit self-assessments were reviewed to provide contextual triangulation.

Data Analysis Strategy

The findings were analyzed using Thematic Analysis, following the six-phase recursive process outlined by Braun and Clarke (2006). Utilizing this approach allowed themes to emerge directly from the data. Cross-case analysis procedures involved comparing themes and patterns across the selected MSI cases to identify commonalities, differences, and unique insights, thereby enhancing the depth and breadth of understanding. To ensure the rigor and trustworthiness of the findings, strategies such as credibility through triangulation and member checking, transferability through rich descriptions, dependability through an audit trail, and confirmability through data grounding were employed.

The steps the researcher used in the analysis are listed below (Braun & Clarke, 2006).

1. Familiarization or immersion in the data through repeated reading of transcripts.
2. Initial Coding, which included generating shorthand labels for data segments.
3. Theme Development, where codes were clustered into potential themes related to RDT.
4. Reviewing Themes and checking them against the entire data set.

5. Defining and naming to refine the basics of each theme.
6. Reporting and linking findings back to the research question and literature.

Trustworthiness and Rigor

To ensure the trustworthiness of the findings (Lincoln & Guba, 1985), the study employed the following checks and balances.

- Credibility through member checking, where participants reviewed their transcripts for accuracy.
- Transferability through detailed "thick" descriptions of the institutional contexts and implementation challenges.
- Dependability through the maintenance of a detailed research log (audit trail using reflexive journaling) documenting all analytical decisions.
- Confirmability using a reflexive journal was maintained to help mitigate researcher bias. For example, initial coding categorized feedback regarding the program's time-sensitive nature as an administrative hurdle. Reflexive analysis revealed this to be a minimization of the participant's experience, which subsequently led to the coding framework being adjusted to include "Operational Friction" as a theme.

Results

The data from the participating MSIs revealed several interconnected themes regarding the implementation and perceived impact of Corporation X's Cyber Maturity Program. These findings, interpreted through the lens of RDT, illustrate how institutions navigate internal resource scarcities, such as financial, human, and knowledge capital, by leveraging strategic external partnerships. The results were organized into themes derived from the qualitative codebook and were directly mapped to the study's research question.

Institutional Transformation

The study examined how key institutional personnel described perceived changes in their institution's cybersecurity posture and audit preparedness following participation in Corporation X's Cyber Maturity program. In response, the data revealed a significant cultural transformation. Participants described moving from a reactive "check-the-box" compliance mentality to a proactive security culture. Participant Large A described this shift vividly, noting that previously: "The mindset was this Corporation X equipment is really expensive…we're just going to kind of check the box. [Now] it is eyes-wide-open. Where are we vulnerable?" Participant Small B reflected on the "wake-up call" provided by the program, stating: "We had policies that did not exist…now we are realizing that we need to put something together."

Beyond these, participant Medium A2 pointed out a noticeable change in institutional feeling: "I guess security was kind of thought about, but…it just seemed like now it is just more evident that, you know, people are paying attention. I mean, you can just feel the like, it's a fundamental shift." Similarly, participant Large C emphasized how the technical stack validated their efforts: "Coupled with our work and everything else, we were able to sit down in all those audits and have an answer for the technical controls…having the technical controls in place is a piece of it."

Resource Scarcity and Dependency

The research examined how MSI personnel perceived the applicability and effectiveness of the software, training, and compliance expertise provided by Corporation X's Cyber Maturity program in enhancing audit preparedness. The analysis highlighted that while software and hardware were highly applicable, their effectiveness was often mediated by human capital gaps. Participant Small A emphasized this critical dependency, stating: "We would not have been able to afford to do it without having support from Corporation X…the hardware…was one-fourth of our budget." Participant Large B articulated the struggle of managing high-end donations without a dedicated team: "I do not have a security team on campus. It is great to get the donations, but how do we manage this?"

The data further illustrated how these resources filled gaps that the institutions could not address due to market conditions. Participant Medium B explained: "Hiring personnel is always a challenge. Our pay is not aligned with the market rate. These tools and resources have allowed us to do more with high confidence." Participant Medium A1 summarized the eagerness for such partnerships: "We are underfunded and understaffed, so anytime we get to partner with a reputable company like you, we are chomping at the bit."

Operational Friction

An analysis of the data revealed significant operational friction. Large institutions struggled with "tool sprawl", characterized by redundant or unmanaged systems, which created inefficiencies. This phenomenon stems from reactive management, in which institutions address cybersecurity vulnerabilities only as funding permits, rather than adopting a holistic, strategic view of the institutional cybersecurity environment. Participant Large A identified: "nine different pieces of services…actually those nine together cost more than the one Corporation X tool." Conversely, medium-sized institutions highlighted the "hidden cost" of staff time as a primary barrier to effective program use. Participant Medium A2 noted: "The biggest drawback was the time commitment…trying to find the time to even get this done." This implementation burden represented a high internal cost of managing external resource interventions.

Other forms of hidden friction included the complexity of knowledge management and geographic isolation. Participant Large C noted the difficulty in accessing timely support compared to larger peers: "You're sitting down, and you're waiting on our turn while [larger state universities] are getting serviced." For participant Small B, environmental factors added to the friction: "Finding the time to continue with the project was another thing. We just did not have the time. We lost power [due to an internet cable cut], and then we had to focus on making sure that students were still able to have continuity of service."

Strategic Alliances and External Pressure

The study examined how personnel interpreted the program's overall value within their specific institutional contexts. The data indicated that the program's value extended beyond technical tools to include strategic legitimacy. IT leaders used the prestige of Corporation X and the Cyber Maturity program's objective findings as ammunition to influence internal university politics. Participant Medium B described the audit reports as "additional ammo to get what I needed approved", illustrating how external assessments are used to gain internal power and secure executive buy-in. Participant Medium A1 observed: "[the partnership] has definitely shifted from standing in the gap to what we look at as more of a long-term…more relational than transactional."

This strategic value was also felt in the boardroom. Participant Small A noted that the program changed the conversation with executive leadership: “When I had to go to the president and say, ok, I need a hundred thousand dollars to do this, it wasn’t as hard to fall on [deaf] ears because they understood differently.” Participant Large B echoed this sentiment of long-term commitment: “I wouldn’t allow anybody to bring another product in here besides Corporation X. For us, it’s a partnership, and it’ll take a lot for that partnership to dissolve.” Figure 1 illustrates MSIs' leverage of external resources to bolster their cybersecurity efforts.

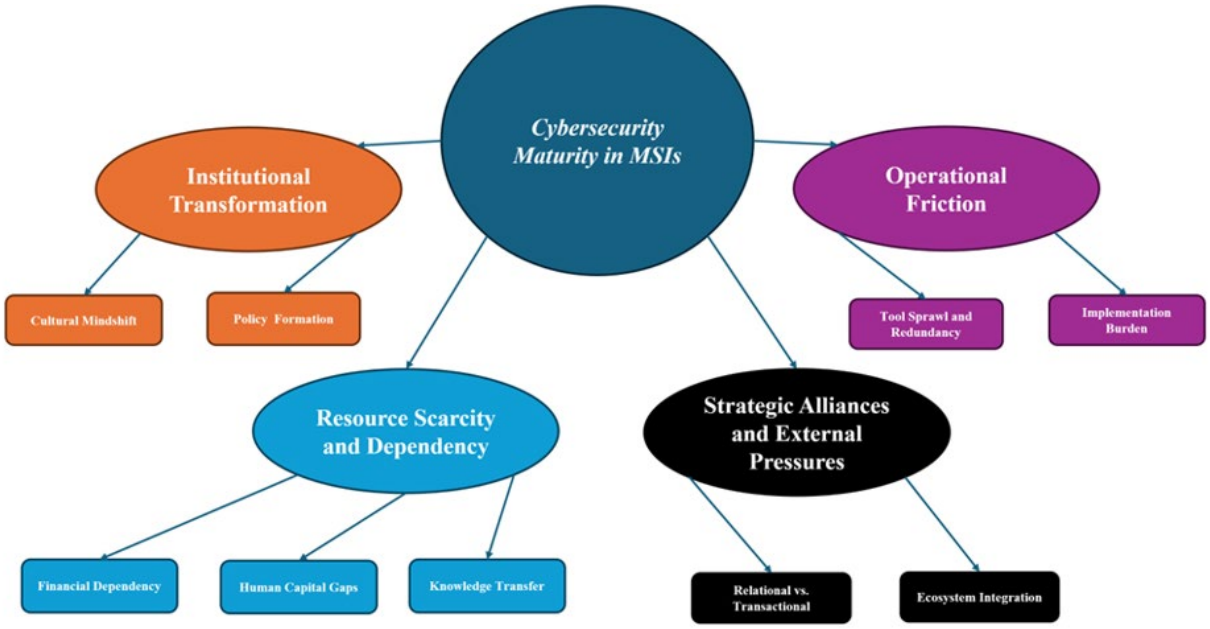

Figure 1: Thematic Visualization

The lived experiences of personnel and the specific ways they addressed the research question varied significantly by institutional scale, as summarized in Table 2.

Table 2: Summary of Comparative Findings by Institution Size

Comparative Theme	**Small Institution Perspective**	**Medium Institution Perspective**	**Large Institution Perspective**
Primary Friction	Geographic & Resource Isolation	"Shadow IT" & Departmental Silos	Legacy Culture & Internal Politics
View of AI	Not yet on the radar	A threat to be controlled	A visibility metric for audits
Staffing Concern	"We don't have a manager."	"We don't have enough time."	"We have the wrong mindset."
Partnership Goal	To be "Seen and Heard"	To gain "Legitimacy & Ammo."	To "Consolidate & Optimize"

Power Imbalance and Sustainability

A reflexive analysis of the findings revealed a nuanced power imbalance inherent in these corporate-academic partnerships. While institutions expressed deep gratitude, there was a palpable underlying anxiety regarding sustainability and "vendor lock-in." Participants Large A and Large B both expressed concern that, once the "free" period ends, the high licensing costs could bankrupt the budgets they are currently trying to fix.

The nature of skepticism varied by institutional context. Small and rural institutions, such as Small B, have historically been skeptical of the "photo op", fearing that partners might provide a gift for social media visibility and then disappear. For these institutions, the program's value was interpreted through a humanitarian lens. They acknowledged "being seen and heard" in a landscape where they are often ignored. In contrast, large institutions viewed the partnership through a surgical lens, utilizing it as a political tool to remove deep-seated organizational inefficiencies. As these reflexive insights emphasized, the perceived value of the program was not a static metric but a socially constructed one, shaped by the institution's socioeconomic and organizational position.

Discussion

Theoretical Implications

This qualitative inquiry explored the lived experiences of MSI personnel regarding the impact of the Corporation X Cyber Maturity program on institutional cybersecurity preparedness. External corporate initiatives provided a vital lifeline for resource-constrained institutions, while simultaneously introducing complex tensions over long-term sustainability and organizational autonomy. The study extends RDT by applying it to the specific socio-technical context of MSI cybersecurity, demonstrating how external partnerships function as both technical conduits and political tools for institutional legitimacy. By examining these dynamics, this research bridges the gap between organizational theory and the practical realities of cybersecurity in under-resourced higher education environments.

Navigating Resource Dependencies

The findings align with Pfeffer and Salancik (1978) on the necessity of acquiring external resources for organizational survival. However, the operational friction observed, specifically tool sprawl, illustrates the hidden costs of dependency. While institutions secure vital assets, they simultaneously inherit management burdens, corroborating Hillman et al.'s (2009) assertion of potential reduced organizational autonomy. The data suggests dependency on external vendors creates a contradictory state. Institutions gain the technical capability to meet federal requirements while also increasing their administrative workload.

From Compliance to a Security-First Culture

The shift toward a security-first culture reflects the socio-technical integration proposed by Almuhammadi and Alsaleh (2017). By leveraging external expertise, MSI personnel successfully navigated the unfavorable organizational culture identified by Yusif and Hafeez-Baig (2023). This transformation demonstrates how external partnerships provide the necessary social capital to institutionalize cybersecurity practices. Rather

than viewing security as a peripheral IT concern, these institutions integrated external guidance into their core institutional identity, effectively mitigating the human-centric risks described by Al-Nuaimi (2022).

Leveraging External Validation for Institutional Support

External audits function as political instruments within the MSI context. As Wertheim (2019) notes, cybersecurity risk assessment constitutes a core business function. The findings suggest that MSI leaders use external validation to secure executive buy-in, thereby transforming technical compliance into institutional power. This strategic maneuver aligns with the power dynamics in RDT, where organizations seek legitimacy to influence internal resource allocation. This finding extends the work of Sabillon et al. (2024) by demonstrating that audits provide not only technical data but also the leverage required to elevate cybersecurity within the institutional hierarchy.

Sustainability and the "Fiscal Cliff"

The anxiety regarding the fiscal cliff after the program concluded emphasizes the risks of temporary injections. Coupet (2017) points out the strings attached to the external revenue sources, which can significantly disrupt long-term planning. Without sustained capacity building, these institutions remain vulnerable to the accreditation risks described by Burnett (2020). For partnerships to be effective, they must evolve from transactional, short-term support models into relational collaborations, as advocated by Zafar et al. (2024).

Incorporating Vendor Lock-In

The fear of vendor lock-in expressed by participants reflects broader economic concerns in IT procurement, where the initial cost savings from external partnerships are ultimately offset by the high switching costs of proprietary systems (Tadelis, 2012).

Limitations of the Study

While this study offered a comprehensive qualitative analysis of the case studies presented, it was subject to some limiting factors, which should be considered when interpreting the results. As a qualitative multiple-case study of a limited population within HEIs, the findings may not be generalizable to other institutions outside this targeted group. Cybersecurity programs represent a heavy burden to institutions. The difficulty in quantifying the "hidden costs", which included the administrative burden, the time diverted from other institutional goals, may have been underrated in the final analysis.

Recommendations for Future Research

Future studies should compare institutions that use external cybersecurity support with those that rely solely on their own internal resources. The scope should also be expanded beyond MSIs and include all HEIs in the United States. Finally, future research should show how external support in the United States differs from corporate-academic relationships in other countries, and how different regulations affect those relationships.

Conclusion

Strategic partnerships offer a viable pathway for MSIs to address persistent cybersecurity challenges, provided these collaborations evolve beyond transactional resource exchanges. Through the lens of Resource Dependence Theory, the Corporation X Cyber Maturity Program served as a critical resource injection, enabling these institutions to navigate complex regulatory landscapes, improve their technical posture, and foster a culture of security awareness.

For MSIs, cybersecurity is not only a technical concern but a fundamental institutional requirement for survival. The success of these initiatives suggests that when corporate partners provide training, knowledge transfer, and the strategic partnership needed to institutionalize cybersecurity, along with tools and funding, the result is a long-term shift in institutional capability. Moving toward a collaborative model of shared knowledge and collective action will be essential for these institutions to maintain their resilience in the face of an ever-changing threat landscape.

References

Almuhammadi, S., & Alsaleh, M. (2017). Information security awareness in higher education: An exploratory study. *Procedia Computer Science, 124*, 803–808. https://doi.org/10.1016/j.procs.2017.12.214

Al-Nuaimi, M. (2022). Human and contextual factors influencing cybersecurity in organizations, and implications for higher education institutions: A systematic review. *Global Knowledge, Memory and Communication, 73*(1), 1–23. https://doi.org/10.1108/gkmc-12-2021-0209

Alwahaibi, A., Hassa, W., Ismail, W., & Almamari, M. (2022). A systematic literature review on IT security standards for higher education institutions. *Journal of Tianjin University Science and Technology, 55*(7), 194–213. https://doi.org/10.17605/OSF.IO/F935H

Amine, A., Chakir, E., Issam, T., & Khamlichi, Y. (2023). Review of cybersecurity management standards applied in higher education institutions. *International Journal of Safety and Security Engineering, 13*(6), 1109–1116. https://doi.org/10.18280/ijsse.130602

Apthorpe, N., Beavers, B., Shvartzshnaider, Y., & Frischmann, B. (2024). *Measuring NIST authentication standards compliance by higher education institutions*. [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2409.00546

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101.

Burnett, C. A. (2020). Diversity under review: HBCUs and regional accreditation actions. *Innovative Higher Education, 45*(1), 3–15. https://doi.org/10.1007/s10755-019-09482-w

Cheng, E. C. K., & Wang, T. (2022). Institutional strategies for cybersecurity in higher education institutions. *Information, 13*(4), 192. https://doi.org/10.3390/info13040192

Corporation X. (n.d.). *Action 8 brief: Commit to HBCUs and the surrounding communities* [Internal corporate document].

Coupet, J. (2017). Strings attached? Linking historically black colleges and universities' public revenue sources with efficiency. *Journal of Higher Education Policy and Management, 39*(1), 40–57. https://doi.org/10.1080/1360080X.2016.1254427

Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among the five approaches* (4th ed.). Sage.

Delaney, P. (2025). *Assessing cybersecurity awareness implementation in higher education institutions: A qualitative analysis* [Doctoral dissertation, South College]. ProQuest Dissertations & Theses Global.

Federal Student Aid. (2020). *Protecting student information: Compliance with CUI and GLBA*. https://fsapartners.ed.gov/knowledge-center/library/electronic-announcements/2020-12-18/protecting-student-information-compliance-cui-and-glba

Feng, X., Zhao, D., Ma, X., & Lei, J. (2025). How does digital transformation affect cross-boundary innovation? Evidence from China. *Applied Economics*. https://doi.org/10.1080/00036846.2025.2535550

Frączkiewicz-Wronka, A., & Szymaniec, K. (2012). Resource based view and resource dependence theory in decision making process of public organisation - research findings. *Management, 16*(2), 16–29. https://doi.org/10.2478/v10286-012-0052-2

Hatch, D. K. (2013). The role of inter-institutional collaboration in the survival of small, private colleges. *Journal of Higher Education Management, 28*(1), 74–89. https://www.aaua.org/journals/jhem/jhem_28-1.pdf

Hillman, A. J., Withers, M. C., & Collins, B. J. (2009). Resource dependence theory: A review. *Journal of Management, 35*(6), 1404–1427. https://doi.org/10.1177/0149206309343469

Johnson, B. L., Jr. (1995). *Resource dependence theory: A political economy model of organizations*. ERIC Clearinghouse on Educational Management. https://eric.ed.gov/?id=ED387871

Kam, H. J., Kim, D. J., & He, W. (2022). Should we wear a velvet glove to enforce information security policies in higher education? *Behaviour & Information Technology, 41*(10), 2259–2273. https://doi.org/10.1080/0144929X.2021.1917659

Khairi, M. (2024). Comprehensive data governance for historically black colleges and universities in Texas: Survey and focus group analysis. *International Journal of Business Research and Information Technology, 11*(1). https://www.iabpad.com/comprehensive-data-governance-for-historical-black-colleges-and-universities-in-texas-survey-and-focus-group-analysis/

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

Lallie, H. S., Thompson, A., Titis, E., & Stephens, P. (2023). *Understanding cyber threats against the universities, colleges, and schools*. [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2307.07755

Lamar, S. (2022, March 18–19). *Managing cyber hygiene at a higher education institution in the United States* [Conference presentation]. Southern Association for Information Systems Conference, Myrtle Beach, SC, United States. https://aisel.aisnet.org/sais2022/

Lincoln, Y. S., & Guba, E. G. (1985). Naturalistic inquiry. Sage.

Merriam, S. B., & Tisdell, E. J. (2016). *Qualitative research: A guide to design and implementation* (4th ed.). Jossey-Bass.

Morphew, C. (2009). Conceptualizing change in the institutional diversity of U.S. colleges and universities. *The Journal of Higher Education, 80*(3), 243–269. https://doi.org/10.1080/00221546.2009.11779012

Nassoura, A. (2022). Cybersecurity technologies and practices in higher education institutions: A systematic review. *Webology, 19*(3), 1152–1167. https://doi.org/10.14704/web/v19i3/web19295

Othman, Z. (2023). Sustainability of higher education institutions: A case study on cyber attacks. *Global Business Management Review, 15*(1), 24–38. https://doi.org/10.32890/gbmr2023.15.1.2

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2017). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security, 67*, 35–46. https://doi.org/10.1016/j.cose.2016.10.002

Pfeffer, J., & Salancik, G. R. (1978). *The external control of organizations: A resource dependence perspective*. Harper & Row.

Price, J. (2022). *Data security in higher education: Protecting confidential financial aid data* [Doctoral dissertation, Northeastern University]. ProQuest Dissertations & Theses Global.

Sabillon, R., Higuera, J., Cano, J., Higuera, J., & Montalvo, J. (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

Slaughter, S., & Leslie, L. (1997). *Academic capitalism: Politics, policies and the entrepreneurial university*. Johns Hopkins University Press.

Stake, R. E. (1995). *The art of case study research*. Sage.

Tadelis, S. (2012). Public procurement design: Lessons from the private sector. International Journal of Industrial Organization, 30(3), 297–302. https://doi.org/10.1016/j.ijindorg.2012.02.002

Towhidi, G., & Pridmore, J. (2023). Aligning cybersecurity in higher education with industry needs. *Journal of Information Systems Education, 34*(1), 70–83. https://doi.org/10.30654/jise.4.2023.4

Ulven, J. B., & Wangen, G. (2019). A systematic review of cybersecurity risks in higher education. *Future Internet, 13*(2), 39. https://doi.org/10.3390/fi13020039

Wang, M. (2024). The lack of responsibility of higher education institutions in addressing phishing emails and data breaches. *Drexel Law Review, 23*(3). https://heinonline.org/HOL/LandingPage?handle=hein.journals/dltr23&div=3&id=&page=

Wertheim, S. (2019). Auditing for cybersecurity risk. *The CPA Journal, 89*(6), 68–72. https://www.cpajournal.com/2019/06/19/auditing-for-cybersecurity-risk/

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). Sage.

Yusif, S., & Hafeez-Baig, A. (2023). 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

Zafar, H., Hollingsworth, C., Bandyopadhyay, T., & Randolph, A. (2024). Collaborative pathways to cybersecurity excellence: Insights from industry and academia in the southeastern U.S. *Journal of Cybersecurity Education, Research and Practice, 23*(1), 1–9. https://doi.org/10.62915/2472-2707.1183