Paradigm-shifting back to the future: Evolutionary vs revolutionary shifts in cybersecurity best practices for U.S. colleges

by

Jim Lilly

B.S., University of Phoenix, 2012
M.S., Western Governors University, 2020

AN ABSTRACT OF A DISSERTATION

submitted in partial fulfillment of the requirements for the degree

DOCTOR OF EDUCATION

Department of Education Leadership
College of Education

KANSAS STATE UNIVERSITY
Manhattan, Kansas

2025

Abstract

This qualitative multi-case study examines the impact of cybersecurity insurance, third-party providers, and endpoint protection on U.S. colleges' cybersecurity policies while highlighting the importance of internal IT skill growth and community involvement as a frontline defense. The Qualitative Case Study Research Design and the National Institute of Standards and Technology (NIST) CSF 2.0 are used as frameworks to explore U.S. colleges' cybersecurity risk management policies and practices. This study emphasizes fostering internal IT expertise, preventing IT staff deskilling, and enhancing the effectiveness of cybersecurity measures. The insights gained will inform best practices, policy development, and risk management strategies for cybersecurity in higher education.

The findings indicate that leveraging the latest cybersecurity solutions, such as NIST CSF 2.0 and HEISC, is crucial for establishing a robust defense strategy. However, an over-reliance on third-party cyber vendors and cybersecurity insurance may be counterproductive due to minimal return on investment and substantial premiums. Instead, institutions should prioritize direct investments in cybersecurity measures, such as ongoing staff training and IT skill development, as evidenced by successful programs incorporating regular hands-on training sessions at larger institutions. Continuous risk assessments, adaptive best practices, and a focus on internal IT growth were identified as effective strategies, particularly for colleges that regularly updated their policies in alignment with NIST and HEISC frameworks. The study also emphasizes the deskilling IT personnel, which can occur when institutions overly depend on third-party providers or insurance. Participants engaging with state and federal cybersecurity programs was shown to be valuable for enhancing security beyond relying on insurance. These findings underscore the importance of proactive internal measures to strengthen resilience.

Paradigm-shifting back to the future: Evolutionary vs revolutionary shifts in cybersecurity best practices for U.S. colleges

by

Jim Lilly

B.S., University of Phoenix, 2012
M.S., Western Governors University, 2020

A DISSERTATION

submitted in partial fulfillment of the requirements for the degree

DOCTOR OF EDUCATION

Department of Education Leadership
College of Education

KANSAS STATE UNIVERSITY
Manhattan, Kansas

2025

Approved by:

Major Professor
Dr. Terry Calaway

Copyright

Abstract

This qualitative multi-case study examines the impact of cybersecurity insurance, third-party providers, and endpoint protection on U.S. colleges' cybersecurity policies while highlighting the importance of internal IT skill growth and community involvement as a frontline defense. The Qualitative Case Study Research Design and the National Institute of Standards and Technology (NIST) CSF 2.0 are used as frameworks to explore U.S. colleges' cybersecurity risk management policies and practices. This study emphasizes fostering internal IT expertise, preventing IT staff deskilling, and enhancing the effectiveness of cybersecurity measures. The insights gained will inform best practices, policy development, and risk management strategies for cybersecurity in higher education.

The findings indicate that leveraging the latest cybersecurity solutions, such as NIST CSF 2.0 and HEISC, is crucial for establishing a robust defense strategy. However, an over-reliance on third-party cyber vendors and cybersecurity insurance may be counterproductive due to minimal return on investment and substantial premiums. Instead, institutions should prioritize direct investments in cybersecurity measures, such as ongoing staff training and IT skill development, as evidenced by successful programs incorporating regular hands-on training sessions at larger institutions. Continuous risk assessments, adaptive best practices, and a focus on internal IT growth were identified as effective strategies, particularly for colleges that regularly updated their policies in alignment with NIST and HEISC frameworks. The study also emphasizes the deskilling IT personnel, which can occur when institutions overly depend on third-party providers or insurance. Participants engaging with state and federal cybersecurity programs was shown to be valuable for enhancing security beyond relying on insurance. These findings underscore the importance of proactive internal measures to strengthen resilience.

Table of Contents

List of Figures

List of Tables

Acknowledgements

I would like to express my heartfelt gratitude to those who supported me throughout this dissertation. First, I am deeply thankful to my dissertation chair, Dr. Terry Calaway, for his mentorship, wisdom, and constant guidance. This work would not have been possible without your encouragement and expert advice.

I am also grateful to my committee members Dr. Margaretta B. Mathis, Dr. Steven Gonzales, Dr. Greg Peterson, and Dr. Jim Martin—for their valuable feedback and insights and for challenging me to think critically at every stage of this research.

To the study participants, thank you for sharing your time and experience and providing the essential foundation for this research.

I would also like to acknowledge my colleagues, classmates, and the broader academic community at Kansas State University for fostering growth and learning. Special thanks to the IT staff and administration for their technical support and for making the process smoother.

Lastly, a huge thanks to my family and friends for their patience and support throughout this journey. Your belief in me has been my greatest source of strength.

Dedication

I dedicate this work to my family, whose constant, positive support and encouragement have been my foundation throughout this journey. Thank you to my close friends for your patience and understanding along the way.

Most importantly, I dedicate this dissertation to Kathryn Enciso, a fellow classmate in this doctoral journey, whose untimely passing reminds us of the preciousness of life and the importance of cherishing those who walk alongside us. Kat, you are very much missed, and thank you for your mentorship.

Preface

This dissertation emerged from my growing interest in cybersecurity's evolving and increasingly complex landscape, particularly the unique challenges U.S. colleges face. As institutions are entrusted with vast amounts of sensitive information, U.S. colleges often operate with limited resources while shouldering the responsibility of maintaining high levels of security. My professional experience in information security, especially within educational institutions, has exposed me to these colleges' vulnerabilities. This exposure sparked my desire to explore how they navigated cybersecurity risks and how effectively their strategies mitigated these threats. The complexities and challenges I encountered firsthand, particularly during multiple security incidents, underscored the urgent need for robust cybersecurity solutions, fueling my determination to contribute meaningfully to this critical field.

Finally, this journey began when I pursued my master's degree in Cybersecurity and Information Assurance. During that time, I witnessed firsthand the consequences of ransomware attacks, including overreliance on cybersecurity insurance companies and third-party applications. Few individuals within the organization understood how to mitigate such incidents internally. These experiences sparked my desire to explore how institutions—especially U.S. colleges and universities—can strengthen their internal defenses in an increasingly complex threat landscape. This dissertation is the culmination of these insights and my ongoing commitment to advancing cybersecurity solutions for educational institutions.

Through this research, I sought to delve deeply into the intersection of resource limitations, evolving cyber threats, and the need for institutional resilience. Understanding that U.S. colleges are not immune to the sophisticated attacks seen in larger organizations, I was driven to uncover strategies that balance affordability with comprehensive protection. This study also addressed the critical role and

integration of internal policies and practices with third-party solutions, exploring how these institutions can enhance their cybersecurity posture.

My work in this field underscores the importance of continuous learning, adaptation, and collaboration. This research contributes to a growing body of knowledge aimed at helping educational institutions, especially U.S. colleges, better protect themselves in an ever-changing digital landscape.

By grounding this study in both theoretical and practical insights from key stakeholders, I hope to offer valuable recommendations that can inform institutional decision-making and policy development in cybersecurity. Through the lessons learned from this research, I sincerely hope that U.S. colleges can better prepare for and respond to daily cyber threats, ensuring the continued protection of their data and the integrity of their systems.

Chapter 1 - Introduction

Premium Cyber-Attacks

Since 2019, cyberattacks and reliance on technology platforms have raised concerns regarding cybersecurity (Burt, 2021). Community colleges and universities across the United States are at risk of such attacks because of the sensitive and personal data stored in the student and employee information systems. Such attacks can result in financial losses, data breaches, and reputational damage to U.S. colleges. While U.S. colleges were expected to implement measures to mitigate these risks, such as using third-party applications, internal policies, procedures, or cyber insurance, it remained to be seen to what extent these security measures were employed or how effective they were in addressing cybersecurity threats. However, more information was needed to determine how much U.S. colleges utilized these measures and their overall impact on security.

Problem Statement

U.S. Community colleges and universities face an increasing threat from cyber-attacks and data breaches, which compromise sensitive information and critical systems. Many of these institutions rely heavily on third-party applications and cyber insurance, which can expose them to additional risks such as vendor vulnerabilities and delayed incident responses. This reliance creates a gap in their overall cybersecurity posture as institutions may not regularly conduct comprehensive external and internal audits to assess their security needs or explore open-source solutions that offer greater control and flexibility. The absence of a balanced and adaptable cybersecurity strategy heightens the vulnerability of institutional data and systems to evolving cyber threats. While each measure, such as third-party tools, protocols, policies, or insurance, may contribute to improving cybersecurity, it is crucial to understand how these measures work together to comprehensively enhance overall security. This qualitative multi-case study examined the effectiveness and impact of different cybersecurity measures within U.S.

colleges, specifically analyzing how third-party applications and internal policies and procedures contributed to mitigating cybersecurity risks (Woods et al., 2017).

Background of the Problem

Over the past decade (2010-2022), technology has become ubiquitous in higher education. U.S. colleges increasingly relied on digital strategies to support their operations, administration, and student services. Unfortunately, this trend made U.S. colleges vulnerable to cybercriminals and threat actors who exploited system vulnerabilities and security gaps (New Cybersecurity Resources for Institutes of Higher Education Available | Knowledge Center, 2023). As a result, cyber-attacks have caused substantial financial losses, data breaches, and reputational harm to U.S. colleges and similar institutions. In response to these risks, many U.S. colleges have implemented cybersecurity practices, including adopting third-party applications and developing internal policies and procedures.

Research was needed to determine how much U.S. colleges relied on security measures and their overall impact on security. Several factors, such as the size and type of college, level of coverage, and perceived benefits and drawbacks, influenced the adoption and effectiveness of these measures. Additionally, affordability was a significant concern, as U.S. colleges often struggled to find cost-effective solutions that addressed their unique security needs.

While cybersecurity measures, including third-party applications and internal policies and procedures, have helped mitigate cyber threats, no single action has provided complete protection. U.S. colleges have recognized the importance of a comprehensive approach to cybersecurity, incorporating strong security policies and procedures, regular risk assessments, staff training on cybersecurity best practices, and data backup strategies. Higher education leaders have strengthened their institutions' resilience against cyber-attacks and data breaches by continuously improving internal procedures and

adhering to state-mandated guidelines.

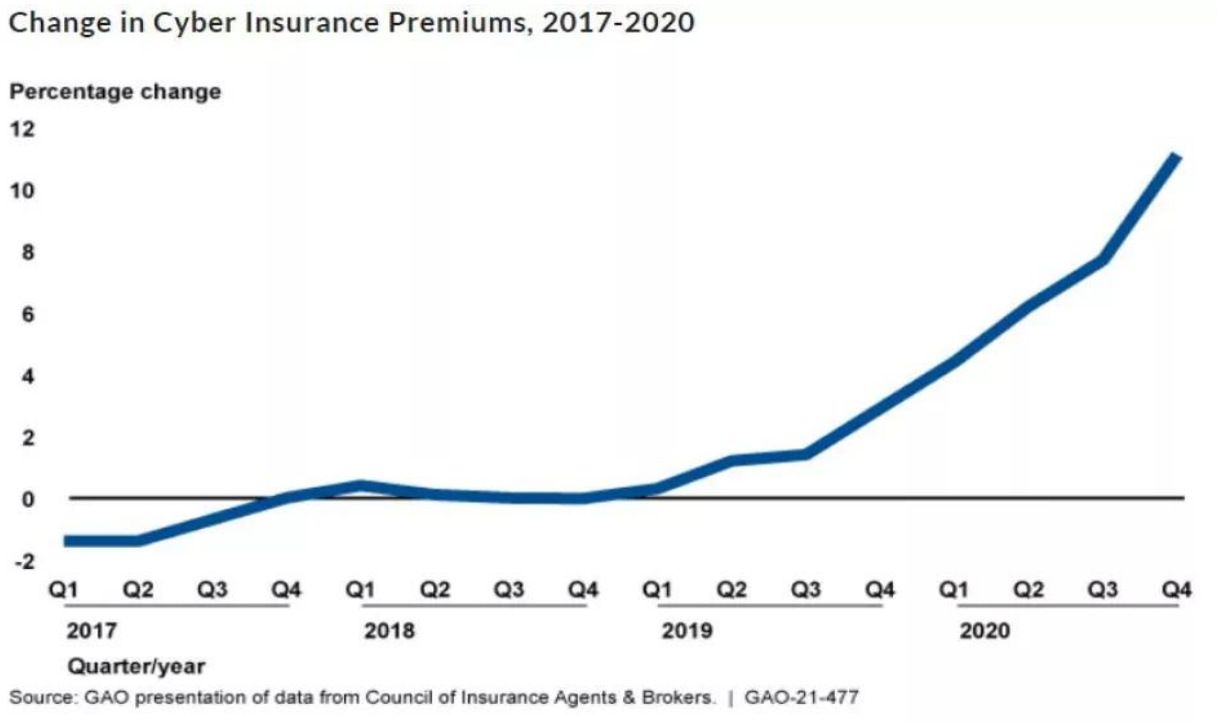

Figure 1:Rising Cybersecurity Insurance Costs

As Figure 1 shows, the cost of cyber insurance premiums increased by 20 percent over the past four years. This rise in premiums contributed to a parallel increase in market uncertainty. This dissertation scrutinized the challenges of pricing cyber risk and offering coverage in an environment characterized by escalating cyber threats.

The study, guided by a qualitative case study approach, involved data analysis and case studies that explored how the frequency, severity, and cost of cyber-attacks significantly influenced the cost of cyber insurance. The ambiguity surrounding future threats steered insurers towards a more cautious strategy, limiting coverage and increasing premiums for higher-risk sectors, such as academia, healthcare, and public services.

Insurers resorted to more stringent policy terms and conditions to mitigate the unforeseen losses from cyber incidents. Previously, commercial property and casualty policies provided limited

cyber-coverage. However, insurers have since excluded cyber coverage from these policies, positioning it as a stand-alone product. This shift left policyholders with fewer coverage options, higher standards, and more exclusions.

Moreover, the federal government's potential role in managing cyber insurance challenges warrants further attention. Large-scale cyber-attacks on critical infrastructure could significantly impact the U.S. economy and national security.

The Federal Terrorism Risk Insurance Program (TRIP), designed to cover terrorism-related losses on eligible cyber policies, often did not apply to cyber-attacks due to their non-violent nature. This study also explored how federal entities, such as the Federal Insurance Office (FIO) under the Treasury Department and the Cybersecurity and Infrastructure Security Agency (CISA) under the Department of Homeland Security, began examining the landscape, but had yet to devise an adequate federal response to a catastrophic cyber event.

This research proposed that the FIO and CISA conduct an in-depth assessment of potential federal responses, analyzing relevant data and considering various possible outcomes. This study examined the evidence suggesting the need for federal involvement in cyber insurance and identified specific steps to address this issue.

As this dissertation explored these insights, the researcher comprehensively analyzed the current market scenario and necessary federal actions.

Purpose Statement

The purpose of this study was to explore best practices in cybersecurity standards adopted by U.S. colleges, including reliance on security firms, third-party software, endpoints, and cybersecurity insurance. This study aimed to examine specific best practices, such as the use of security firms, third-

party software, endpoints, cybersecurity insurance, and the role of internal IT staff or cybersecurity teams, both in isolation and in their collective influence on the overall security posture of these institutions. It assessed the cumulative impact of these benchmarks on mitigating cyber risk. It found effective and affordable cybersecurity practices that U.S. colleges should adopt to safeguard their digital assets and protect sensitive information.

Research Questions

1. What are the best practices in the U.S. college environment for the use of security firms, third-party software, endpoints, and cybersecurity insurance?

2. What is their influence on the overall security posture of U.S. colleges?

3. How can U.S. colleges evolve their cybersecurity strategies to anticipate and counter emerging cyber threats based on historical trends and expert insights?

Conceptualizing the Theory

1. This study is grounded in Resource Dependency Theory (RDT), which serves as the primary theoretical lens for understanding how U.S. colleges manage cybersecurity risks in resource-constrained environments. Developed by Pfeffer and Salancik (1978), RDT emphasizes that organizations depend on external resources to achieve their objectives, especially when internal capacities are limited. For U.S. colleges, which often face budget constraints, relying on third-party services and external cybersecurity solutions is a strategic necessity. By examining these dependencies, this study sought to understand how colleges leverage external resources to strengthen their cybersecurity infrastructure. In conjunction with the RDT, the NIST Cybersecurity Framework (CSF 2.0) provides a practical framework for addressing cybersecurity challenges in educational institutions. NIST CSF focuses on identifying, assessing, and managing

risks through a structured approach, allowing organizations to enhance their resilience against cyber threats. Integrating the NIST framework with RDT offers a dual perspective: it highlights the strategic use of external partnerships and guides the prioritization of cybersecurity measures based on risk assessments.

2. Furthermore, the study employs Social Cognitive Theory (Bandura, 1986) to explore the role of training and awareness programs in fostering cybersecurity compliance among staff members. Social Cognitive Theory posits that learning occurs through social interactions and observation, making it particularly relevant in training initiatives designed to improve cybersecurity behaviors. This study identified strategies for enhancing institutional cybersecurity practices by understanding how training influences staff compliance. Lastly, the Technology Acceptance Model (TAM) is used to analyze the factors affecting the adoption of new cybersecurity technologies within U.S. colleges. According to Davis (1989), TAM focuses on perceived ease of use and perceived usefulness as critical determinants of technology adoption. This model is crucial for understanding how U.S. colleges, which may face resistance to technological change, can improve the integration of cybersecurity tools. By identifying barriers to adoption, this study provides insights into the promotion of effective technology use in educational institutions. These theoretical frameworks collectively offer a comprehensive understanding of how U.S. colleges can manage cybersecurity challenges. Integrating RDT, NIST CSF, Social Cognitive Theory, and TAM enables a multifaceted analysis of the complex dynamics involved in resource allocation, staff training, and technology adoption, thus offering actionable recommendations for enhancing cybersecurity in higher education.

Conceptualizing and Working the Frame

The conceptual framework for this study was based on risk management methodology and the need for protection against potential cyber threats. According to this theory, U.S. colleges rely on security firms, third-party software, endpoints, and cybersecurity insurance to mitigate risks and improve their overall security posture. Higher education leaders generally recognize the increased frequency and sophistication of cyber-attacks and understand the financial and reputational consequences of a successful attack. Consequently, they purchased cybersecurity insurance and adopted other protection strategies to manage and mitigate the risk of such attacks. These strategies provided them with a safety net in the case of a breach and helped transfer financial and reputational risks to the insurance company. Additionally, purchasing cybersecurity insurance signaled to stakeholders, such as students, employees, and the public that higher education took cybersecurity seriously and was committed to protecting sensitive information.

Through the risk management lens, U.S. colleges' reliance on cybersecurity insurance, security firms, third-party software, and endpoints also helped build stakeholder trust. This demonstrated that higher education took cybersecurity seriously and proactively implemented measures to protect sensitive information. This helped mitigate potential reputational damage from a breach and build confidence in the college's data privacy and security commitments.

The study employed the NIST CSF 2.0 (Force, 2018) and the Cybersecurity Framework for HEISC (New Cybersecurity Resources for Institutes of Higher Education Available | Knowledge Center, 2023) as separate but complementary frameworks to guide the research. While the NIST Cybersecurity Framework provided a foundation for risk management, the HEISC Framework was explicitly tailored for higher education, adding dimensions for deeper analysis. By examining the effectiveness of policies and procedures within the scope of these frameworks, the study aimed to provide recommendations for improving U.S. colleges' cybersecurity posture and ensuring compliance with applicable regulations. Furthermore, the frameworks were used to analyze the risks associated with the college's reliance on

cybersecurity insurance, security firms, third-party software, and endpoints. This multifaceted approach contributes to the literature on cybersecurity risk management policies in U.S. colleges and offers valuable insights for enhancing cybersecurity strategies and risk management efforts.

Methodology

This study employed a qualitative strategy, using the case study methodology as the primary design. The case study methodology allowed for an in-depth exploration of the complexities within the cybersecurity domain in U.S. colleges. It proved beneficial for capturing emergent patterns, themes, and concepts and informing and modifying existing frameworks and theories. The methodology enabled a contextually rich exploration of specific instances, offering a nuanced view of cybersecurity practices in U.S. colleges.

Chapter 2 details the intricacies of this methodological tool, enhancing the theoretical frameworks of RDT and NIST CSF 2.0. This approach allowed for iterative analysis of qualitative data, such as interviews and document reviews. This study explored how U.S. colleges managed cybersecurity risks, relied on external resources such as third-party applications and services, cybersecurity firms, insurance, and vendors, and identified cost-effective, scalable, and secure solutions. The case study design allowed for an in-depth examination of multiple instances, offering a more nuanced and comprehensive understanding of the cybersecurity landscape in U.S. colleges. The findings offered valuable insights into the cybersecurity strategies adopted by these institutions, contributing to broader knowledge of cybersecurity management in educational settings.

The multi-case study research design was selected because it provided an in-depth understanding of the research problem by exploring U.S. colleges' experiences, attitudes, and practices concerning their reliance on cybersecurity insurance. Additionally, it enabled the examination of the risk

management processes employed by colleges and how these processes influenced their reliance on cybersecurity insurance (Yin, 2017).

The researcher collected data through semi-structured interviews with key stakeholders from four U.S. colleges, including administrators, IT staff, and risk management professionals. A document analysis of relevant policies, plans, and reports complemented the data gathered through interviews, providing a broader perspective on the research problem. The collected data were analyzed using thematic analysis to identify patterns, themes, relationships, and best practices related to cybersecurity risk management. The researcher securely stored all interview recordings, transcripts, and documents on a USB thumb drive with fingerprint authentication and in a OneDrive Vault with biometric access to ensure data security, confidentiality, integrity, and availability. I restricted my access to myself as a researcher.

NIST CSF 2.0 (NIST CSF) guided the data analysis, focusing on how U.S. colleges identified, assessed, and responded to cyber risks. NIST CSF 2.0 also explored how these institutions financed these risks through cybersecurity insurance. The HEISC Cybersecurity Framework for Higher Education provided additional dimensions tailored to higher education, contributing to a more nuanced understanding of risk management practices within U.S. colleges.

This methodology ensured that U.S. colleges effectively managed their cyber risks and protected themselves against potential threats. By employing a step-by-step approach, the study examined the types of cyber risks faced by colleges, assessed their likelihood and impact, and evaluated how policies and processes reduced these risks. Additionally, it considered how these institutions financed and monitored their cyber risk environments (Force, 2018). The qualitative case study design enabled the identification of best practices and strategies for higher education leaders to mitigate risk. While this

study aligns with NIST CSF 2.0, it also integrates a traditional risk management approach to further explore institutional cybersecurity practices.

This study employed the following risk management methodology:

- **Risk Identification**: This process identified the diverse types of cyber risks U.S. colleges face, such as data breaches, malicious attacks, and ransomware. A risk assessment considers the institutions' assets, operations, and systems, helping to pinpoint areas of vulnerability.

- **Risk Analysis**: A qualitative risk analysis estimated the likelihood and impact of each identified risk, helping prioritize which risks to address first and how to manage them.

- **Risk Control**: Security measures, including encryption protocols, firewalls, intrusion detection/prevention systems, and administrative controls, were implemented to protect against cyber threats and reduce the likelihood of incidents.

- **Risk Financing**: Cybersecurity insurance was examined to provide financial protection against potential cyber risk. The study analyzed the cost-effectiveness of different coverage options and their benefits for U.S. colleges.

- **Risk Monitoring**: The Colleges regularly monitor their cyber risk environments to adapt to evolving threats. This study evaluated the effectiveness of the policies and processes against new cyber threats (Chapter 4-Security Management, From Safeguarding Your Technology, National Center for Education Statistics (NCES) Publication 98-297, n.d.).

In conclusion, the data gathered through this methodology provided a comprehensive understanding of U.S. colleges' reliance on cybersecurity preparedness and the role of cybersecurity insurance. The qualitative case study design and NIST CSF 2.0s offered insights that would help U.S.

colleges better manage and respond to cyber threats. The findings aimed to enhance the institution's ability to manage cyber risks and inform strategies to improve its overall security posture. Additionally, historical studies were incorporated to provide a robust understanding of cybersecurity preparedness and risk management in U.S. colleges. These studies reviewed past and existing cybersecurity policies and incidents, offering insights into how risk-management strategies have evolved. Historical data sources included past security policies, incident reports, institutional protocols, and relevant public records.

Alignment Table

The alignment table demonstrated the relationship between the various elements of the research.

This section explored many facets of the study's broader aim, specifically evaluating the impact and role of third-party applications and the lack of protocols, policies, and cybersecurity insurance within the range of cybersecurity practices adopted by U.S. colleges. This purpose was aligned with NIST CSF 2.0, which is a widely used cybersecurity framework. The framework for managing cyber risks involved five core components: Risk Identification, Risk Analysis, Risk Control, Risk Financing, and Risk Monitoring, elaborated in the previous section. Collectively, these components offered a holistic approach to cyber risk management, with each building on the other to ensure a robust strategy. These components were crucial for ensuring that U.S. colleges were equipped to mitigate cyber risks and improve their overall security posture. In addition, the HEISC Cybersecurity Framework for Higher Education was employed to tailor the study's focus on the unique cybersecurity needs and challenges faced by higher education institutions. Appendix A in Figure A.2 presents an alignment table illustrating how the framework was applied to identify and address these challenges.

Delimitations and Assumptions

Delimitating the Study

This study examined the impact of cybersecurity insurance and NIST CSF 2.0, on cybersecurity risk management policies at U.S. colleges in the United States over the past seven years (2015-2022). The study focused on a small sample of U.S. colleges in the United States that had identified and implemented best practices in cybersecurity protection using NIST CSF 2.0. The methodology for this study followed a qualitative approach, employing a multi-case study research design to obtain a broad understanding. Data were collected and analyzed based on the criteria outlined in the NIST and HEISC frameworks. The HEISC framework was specifically used to evaluate measures tailored for educational institutions, such as compliance with higher education and academic regulations and staff and student training programs. U.S. colleges with a minimum enrollment of 2,000 students and at least two years of implementation of these cybersecurity measures were included in the study. Where available, data spanning a seven-year period were analyzed to assess the long-term impact. This study focused on the effects of these interventions on the following criteria of cybersecurity risk management policies: risk assessment, risk mitigation, risk monitoring, and risk communication.

Assumptions

The study included U.S. colleges that had implemented cybersecurity insurance and NIST CSF 2.0 to enhance their cybersecurity risk management policies, with the assumption that the impact of these interventions on cybersecurity risk management policies would be significant and observable. Colleges that relied solely on cybersecurity insurance as their risk management strategy often found it ineffective in preventing attacks (Yeo & Yeo, 2023). This approach frequently created a false sense of security, leading to the development and implementation of inadequate cybersecurity risk management policies.

It was also assumed that U.S. colleges in the sample had the necessary resources, expertise, and capacity to implement and sustain the interventions. Additionally, the study assumed that the selected higher education leaders would be willing to share information and cooperate with the researcher honestly, and that the study findings would apply to other U.S. colleges in the United States that had implemented or were considering implementing cybersecurity insurance and NIST CSF 2.0.

These assumptions reflected the expectation that implementing cybersecurity insurance and NIST CSF 2.0 would positively impact cybersecurity risk management policies in U.S. colleges, while acknowledging the potential negative impact of relying solely on cybersecurity insurance. The assumptions also considered the availability of resources and expertise required for the successful implementation of these interventions and the willingness of U.S. colleges to cooperate with the study.

Significance of the Study

This study is significant for several reasons. First, U.S. colleges are responsible for protecting sensitive student and institutional data, yet they are often overlooked in the literature on cybersecurity risk management and risk management policies. This study provides essential insights into the impact of relying on cybersecurity insurance, third-party security companies, and software, as well as implementing the NIST CSF 2.0 on cybersecurity risk management policies in U.S. colleges, which inform policy and practice in this area.

This study aimed to improve the security of higher education institutions by highlighting the importance of U.S. colleges in cybersecurity risk management policies and examining the impact of cybersecurity insurance, third-party security companies and software, and NIST CSF 2.0.

Additionally, this study addressed a critical gap in the literature on the effectiveness of cybersecurity insurance, third-party security companies, and software as a risk management strategy. While cybersecurity insurance, third-party security companies, and software have become popular

solutions for managing cyber risks, more research is needed on their effectiveness in improving cybersecurity risk-management policies. By providing valuable information on the impact of relying on cybersecurity insurance, third-party security companies and software, and the NIST CSF 2.0 on the risk management policies of U.S. colleges, this study informed best practices and policy development in this area.

Finally, the study has practical implications for U.S. colleges that have implemented or are considering implementing cybersecurity insurance, third-party security companies, software, and NIST CSF 2.0. By assessing the impact of these interventions on cybersecurity risk management policies in U.S. colleges, the study provided insights into how to leverage these interventions to improve cybersecurity risk management practices, procedures, and policies. As a result, U.S. colleges could better protect sensitive data and prevent cyber incidents, ultimately improving the security of the higher education sector.

Additionally, this study delved into the cybersecurity risk management practices and challenges of U.S. colleges, aiming to identify potential solutions to enhance their cybersecurity posture. This explored the best practices for managing cybersecurity risks and the factors determining their success or failure, offering practical guidance to U.S. colleges to bolster their cybersecurity readiness.

While much of the existing research on higher education cybersecurity has centered on four-year institutions, U.S. colleges have played a pivotal role in the educational landscape. Their growing importance in the sector underscored the need to understand their unique cybersecurity challenges and opportunities. This research provided insights into the factors that shaped their cybersecurity stance and effective strategies for risk management.

Additionally, the study explored collaborative approaches for U.S. colleges to engage with policymakers and other institutions to strengthen cybersecurity practices. Such insights could guide the creation of new policies and initiatives to enhance cybersecurity across the higher education sector.

This research bridged the gap between theory and practice by contributing to cybersecurity literature and emphasizing the role of U.S. colleges. It aimed to inform future studies and the development of robust cybersecurity policies and programs in higher education, ultimately enhancing the cybersecurity posture of U.S. colleges and the broader educational environment.

Definitions of Terms

1. Best Practices: The most effective and efficient way of doing something based on research, experience, and industry standards (Computer Security Resource Center (CSRC) content editor, n.d.-a).

2. Cyberattacks: Intentional malicious actions that target computers, networks, or data systems (CSRC Content Editor, n.d. b.).

3. Cybersecurity: The protection and mitigation of Internet-connected systems, including hardware, software, and data, from cyberattacks, theft, or damage (CSRC Content Editor, n.d.).

4. Cybersecurity Insurance: A type of insurance that provides financial protection for an organization in the case of a cyber incident (Cyber Insurance 2021).

5. Data Breaches: Unauthorized access, disclosure, or theft of sensitive or confidential data (CSRC Content Editor, n.d.-a.).

6. Data Redundancy: Refers to a situation where the identical dataset is duplicated in several locations, while data inconsistency refers to the same data appearing in various formats across multiple tables. Regrettably, the presence of data redundancy can trigger data consistency, potentially supplying an organization with unreliable information that requires a more meaningful context (Selman, 2022).

7. Educational Institutions: Organizations that provide educational services, including schools, universities, and community colleges (Definition & Meaning Educational Institution, n.d.).

8. Family Educational Rights and Privacy Act (FERPA): The Family Educational Rights and Privacy Act (FERPA) is a federal law that affords parents the right to have access to their children's education records, the right to seek to have the records amended, and the right to have some control over the disclosure of personally identifiable information from the education records. When a student turns 18 years old or enters a post-secondary institution at any age, the rights under FERPA transfer from the parents to the student ("eligible student"). The FERPA statute is found at 20 U.S.C. § 1232 g, and the FERPA regulations are found at 34 CFR Part 99 (What is FERPA? | Protecting Student Privacy, n.d.).

9. Higher Education Institutions: Organizations that provide post-secondary education, including universities and community colleges (What Is Higher Education Institution | IGI Global, n.d.).

10. Immutable Backups: Data storage copies that cannot be altered, deleted, or modified once created. Designed to protect data integrity, they serve as a secure safeguard against ransomware and unauthorized access by ensuring that the backup files remain unchanged. This immutability feature helps institutions maintain data reliability and meet

regulatory compliance requirements by providing a reliable restoration option in the event of a cyberattack or data corruption (HornetSecurity, 2024).

11. NIST: A U.S government branch that promotes technology, standards, and best practices in various areas, including cybersecurity (Mohajeryami, 2023).

12. NIST CSF 2.0: The NIST Cybersecurity Framework (CSF) builds on established standards, guidelines, and practices to help organizations manage and reduce cybersecurity risks. It is widely used across sectors worldwide. As a living document, the CSF will continue to evolve to address growing cybersecurity risks, emerging technologies, and best practices. NIST plans to engage in public-private dialogue to guide ongoing updates (NIST CSF 2.0, 2024).

13. Personal Identifiable Information (PII): Information that can be used by institutions on its own or with other data to identify, locate, contact, or locate a single person, or to identify an individual (CSRC Content Editor, n.d. -h).

14. Risk Assessment: The process of analyzing and evaluating potential risks to an organization (CSRC Content Editor, n.d.-d).

15. Risk Management: Identifying, assessing, and mitigating risks in an organization (CSRC Content Editor, n.d.-b).

16. Risk Management Framework: A structured approach to risk management that includes identifying risks, assessing the likelihood and impact of risks, developing risk-mitigation strategies, and monitoring and reviewing risks (CSRC Content Editor, n.d.-c).

17. Risk Mitigation: The process of analyzing, reducing, or eliminating the impact of a risk on an organization (CSRC Content Editor, n.d.-g).

18. Risk Monitoring: The ongoing process of observing and reviewing risks and risk management strategies to ensure that they are effective (Cyber Risk Monitoring | BitSight, n.d.).

19. Security Posture: The security status of an enterprise's networks, information, and systems based on information assurance resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and react as the situation changes. Synonymous with security status.

20. Security Information and Event Management (SIEM): A security solution that aggregates and analyzes activities from various resources across the IT infrastructure. SIEM systems collect security event logs and other relevant data from networks, devices, servers, and applications and then analyze this information to identify and respond to potential security threats in real time. SIEM tools are essential for monitoring, detecting, and responding to cybersecurity threats across large and complex environments, helping organizations meet compliance requirements and maintain a robust security posture (*Cybersecurity Master's Degree, Online, NYU Tandon School of Engineering*, n.d.).

21. Sensitive Information: Data that require extra protection due to its potential to cause harm to individuals or organizations if it is exposed or accessed by unauthorized parties (CSRC Content Editor, n.d.-f).

22. The Security Operations Center (SOC) is a centralized unit responsible for continuously monitoring, detecting, analyzing, and responding to cybersecurity threats. SOC teams are often staffed either internally or through third-party providers (Managed Security Service Providers - MSSPs) to provide 24/7 threat management, incident response, and security operations (CompTIA, n.d.).

23. Taguette: An open-source tool for qualitative research that allows users to quickly **code** and analyze text-based data such as interview transcripts or field notes. This enables researchers to tag sections of their data with thematic **codes**, facilitating the identification of patterns and insights. Taguette is user-friendly, supports various file formats, and is accessible through a web browser, making it ideal for collaborative research projects (Rampin & Rampin, n.d.).

24. Wazuh: An open-source security monitoring platform that provides capabilities, such as threat detection, integrity monitoring, vulnerability detection, and incident response. It integrates various systems and platforms, collecting and analyzing log data to detect and alert potential security threats. Wazuh can also be used for configuration assessments, compliance management, and cloud security monitoring. It is particularly valuable for organizations seeking cost-effective and scalable security monitoring solutions (Wazuh, n.d.).

25. Extended Detection and Response (XDR): An integrated cybersecurity approach that goes beyond traditional endpoint detection and response (EDR) by combining data from various security products, including networks, emails, and cloud environments. It enables security teams to detect, investigate, and respond to threats more efficiently by correlating data across different security layers, thereby providing a holistic view of security incidents. The goal of XDR is to improve detection accuracy and streamline response efforts by reducing the time and complexity involved in managing security threats across multiple domains (*What Is XDR? | Microsoft Security*, n.d.).

Chapter Summary

The growing concern over cybersecurity has been particularly acute in the context of U.S. colleges. Due to their increasing reliance on technology, U.S. colleges urgently needed additional

resources to protect their institutions from cyber-attacks. These attacks have led to significant financial losses, data breaches, and reputational damage. To address these security risks, U.S. colleges have explored a range of cybersecurity solutions, including third-party security companies and software, endpoint protection, and cybersecurity insurance.

However, there was a need for more information on how U.S. colleges utilized cybersecurity insurance, among the other strategies listed above, to mitigate cyber risks. Therefore, this chapter presented three research questions: (1) What are the best practices in the U.S. college environment in using security firms, third-party software, endpoints, and cybersecurity insurance? (2) What was their influence on the overall security posture of U.S. colleges? (3) How could U.S. colleges evolve their cybersecurity strategies to anticipate and counter emerging cyber threats based on historical trends and expert insights?

To address these research questions, this study adopted a methodological approach based on a qualitative case study research design and NIST CSF 2.0. These frameworks were relevant to the research questions and provided a comprehensive and practical approach for data collection, analysis, and interpretation. The frameworks helped offer a systematic and structured approach to data collection, analysis, and understanding, offering valuable insights into the effectiveness of cybersecurity insurance, third-party security companies and software, endpoints, and the NIST CSF 2.0 in improving U.S. colleges' cybersecurity risk management policies.

The chapter also emphasized the study's practical implications for U.S. colleges, cybersecurity insurance providers, and policy development in the higher education sector. The insights gained from this study inform the best practices, policy development, and cybersecurity risk management practices, procedures, and policies in the context of higher education. By leveraging the latest cybersecurity solutions, including cybersecurity insurance, third-party security companies and software, endpoints,

and NIST CSF 2.0, U.S. colleges could better protect sensitive data and prevent cyber incidents, ultimately improving the security of the higher education sector.

Organization of the Study

The remainder of this study was organized into four additional chapters, each addressing a specific aspect of the research.

Chapter 2 is devoted to a literature review and examines prior research on cybersecurity risk management policies. The literature review identified key themes, concepts, and gaps in the literature, providing a foundation for the study's research questions. This chapter also reviews the literature on cybersecurity insurance adoption and impact, NIST CSF 2.0, and best practices in the higher education sector.

Chapter 3 presented the research methodology for the study, including the research design, data collection methods, and data analysis methods. This chapter also provides an overview of the sample selection, data sources, and ethical considerations. The Qualitative Case Study Research Design and the NIST CSF 2.0 guided the study's methodology.

Chapter 4 reports the findings of the study, which were organized according to the two research questions. This chapter provides an in-depth analysis of the impact of relying on cybersecurity insurance and NIST CSF 2.0, on cybersecurity risk management policies in U.S. colleges. Additionally, this chapter explored how U.S. colleges' cybersecurity insurance impacted their ability to protect sensitive data. Qualitative data collected from semi-structured interviews and document analyses were used to answer the research questions.

Section 5 summarizes the study's main findings and implications for policy and practice. This chapter also discusses the study's delimitations, identifies areas for future research, and concludes the

paper. The chapter also provides a practical guide for U.S. colleges, cybersecurity insurance providers, and policy developers in the higher education sector. This study's theoretical and practical contributions to the literature on cybersecurity risk management policies in U.S. colleges are also discussed.

Chapter 2 - Literature Review

Introduction

This literature review explores current research and best practices associated with strategic risk management and cybersecurity in U.S. colleges. The review contextualized current strategies and policies in cybersecurity risk management within U.S. colleges, highlighting areas where existing research is either lacking or inconsistent. Various sources were consulted, including academic journals, books, and industry reports. Several online databases such as JSTOR, ProQuest, and Google Scholar were used to conduct the search.

Diverse keywords were employed, including "strategic risk management," "cybersecurity," "community colleges,", “universities”, “AI and colleges”, "best practices," and "emerging technologies." The search was limited to English-language sources published within the last decade and focused on research conducted in the United States. The review process involved examining more than 100 sources, particularly peer-reviewed academic journals. Sources were selected based on their relevance to the research question, quality, and contribution to understanding strategic risk management and cybersecurity in U.S. colleges.

The literature review was organized thematically, with each section addressing a specific aspect of risk management and cybersecurity within the broader context of higher education. The review also incorporated cybersecurity best practices from other sectors, such as business, which provided valuable insights into improving cybersecurity in educational institutions (Cybersecurity Best Practices | Cybersecurity and Infrastructure Security Agency CISA, n.d.).

Background and Conceptual Framework

US Colleges have played a crucial role in providing diverse populations with opportunities for higher education and workforce training. These institutions face various risks, including cybersecurity threats, which compromise the confidentiality, integrity, and availability of sensitive staff, student information, financial data, and disrupted operations. Strategic risk management and cybersecurity practices have helped U.S. colleges mitigate these security risks and ensure the continued delivery of high-quality education to their communities.

The frameworks employed in this study extend beyond the conventional applications. Initially formulated by Pfeffer and Salancik (1978), RDT serves as a lens for understanding organizational behavior in resource-constrained environments. In the context of this research, it was particularly relevant for dissecting the allocation and management strategies of cybersecurity resources in U.S. colleges.

The Cybersecurity Framework for Higher Education, developed by the HEISC (New Cybersecurity Resources for Institutes of Higher Education Available | Knowledge Center, 2023), was instrumental in this study. It addressed sector-specific nuances of cybersecurity risk management and filled gaps, including compliance and governance issues, which are often overlooked in generalized frameworks.

In addition to the HEISC Cybersecurity Framework, this study also originally considered the NIST Risk Management Framework (RMF), a widely adopted tool that provides a structured approach for categorizing, assessing, and monitoring security controls. RMF has historically been instrumental in helping institutions manage cybersecurity risks systematically and comply with regulatory standards, especially in higher education. However, in light of recent updates, NIST introduced Cybersecurity Framework 2.0 (CSF 2.0), which expands on RMF's foundational elements and offers a broader, adaptable approach suited to today's dynamic cybersecurity landscape. This new framework also

introduces a "Govern" function, highlighting strategic oversight and governance as central components of effective cybersecurity.

Given these advancements, this study incorporates NIST CSF 2.0, rather than RMF, to ensure alignment with the latest standards. CSF 2.0, which includes six core functions—Identify, Govern, Protect, Detect, Respond, and Recover— provides a more exhaustive risk management and governance model that addresses the unique needs of U.S. colleges.

NIST CSF 2.0 (NIST, n.d.) is a more general yet robust tool commonly applied across various sectors. Its inclusion in this study added a layer of rigor and enabled a more exhaustive risk assessment and management plan for the sampled U.S. colleges. The framework comprises a structured five-step process that allows the categorization, assessment, selection, implementation, and monitoring of security controls.

This study synthesized RDT with the HEISC Cybersecurity Framework and NIST CSF 2.0, to provide a comprehensive and multifaceted approach to understanding and addressing cybersecurity challenges in U.S. colleges.

Role of Case Study Methodology in Cybersecurity Research

A case Study is a research methodology frequently used in qualitative research to construct a theory from systematically obtained data. Its utility in this study was to help understand the complex nature of cybersecurity practices in U.S. colleges.

Owing to the field's ever-evolving nature, the case study methodology is particularly suited to cybersecurity research. This approach allowed for the discovery of new concepts, themes, and patterns that may not have readily appeared in existing theories or frameworks. This is critical in fields such as

cybersecurity, where threats and responses continually evolve, and insights need to be derived from real-world experiences and practices.

In this study, a case study methodology was applied by collecting and analyzing interview data from various stakeholders within U.S. colleges, including IT managers, cybersecurity officers, and other relevant personnel. The data obtained were analyzed iteratively, allowing themes, patterns, and theories to emerge naturally.

This approach, combined with the theoretical lens of RDT and the practical guidance of the HEISC Cybersecurity Framework and NIST CSF 2.0 (NIST CSF 2.0), provided a comprehensive understanding of the cybersecurity landscape in U.S. colleges.

The selection of a case study approach is driven by its capacity to offer an intricate, contextually rich understanding of complex issues (Baxter & Jack, 2015). Cybersecurity in U.S. colleges is a multifaceted problem encompassing technological, human, and organizational variables. A case study methodology was best suited to explore these variables in detail, allowing the researcher to understand U.S. colleges' cybersecurity experiences, attitudes, and practices (Creswell and Poth 2017).

Case studies are beneficial for exploring how and why phenomena occur, providing a level of detail that might have been overlooked in other research methodologies (Baxter & Jack, 2015). Therefore, employing a case study design effectively achieved a nuanced understanding of U.S. colleges' risk-management processes and how these organizations made resource-dependent decisions on cybersecurity measures.

This research methodology also opened opportunities for employing case study methodology techniques. The case study methodology complemented case studies by enabling inductive data collection and analysis, potentially leading to new theoretical insights (Creswell & Poth, 2017). This ensured that the study was empirically grounded and theoretically informed.

RDT

The RDT, initially formulated by Pfeffer and Salancik in 1978, served as a significant theoretical lens for this study. This was particularly relevant for understanding how U.S. colleges, often operating under constrained resources, managed and allocated their cybersecurity resources. According to Pfeffer and Salancik (1978), organizations are not fully autonomous; they depend on external resources, which affect their behavior and decision-making processes. For U.S. colleges, this dependency is manifested in relationships with third-party security firms, software licenses, and cybersecurity insurance policies. The RDT was crucial in shaping this study's research questions and methodology because it provided a framework for examining the complex interdependencies that these educational institutions had with various stakeholders in cybersecurity (Pfeffer & Salancik, 1978).

Best Practices in Cybersecurity Risk Management

Section 1: Strategic Risk Management

Cybersecurity has become a top priority for colleges in today's digital era as they increasingly rely on information systems to conduct their operations. Protecting against potential cyber threats requires a proactive approach to manage risks and vulnerabilities achieved through strategic risk management. The literature emphasizes the importance of risk assessment in strategic planning and the need for a systematic approach to risk management (Ashraf et al., 2021).

One framework that gained widespread recognition for its effectiveness in managing cybersecurity risks was the NIST CSF 2.0 (NIST CSF 2.0) (NIST, n.d.). This study discussed the benefits of using NIST CSF 2.0, as a guideline for implementing comprehensive, organization-wide protection. NIST CSF 2.0 offered a structured and flexible means for analyzing and alleviating risks arising from college information systems. Its six-step process enables the categorization, assessment, selection,

implementation, and monitoring of security controls, providing a comprehensive approach to managing cybersecurity risks.

In addition to providing a structured approach to managing risks, NIST CSF 2.0 helped colleges comply with various security standards and regulations, including the Health Insurance Portability and Accountability Act (HIPAA), the Family Educational Rights and Privacy Act (FERPA), and the Gramm-Leach-Bliley Act (GLBA). Compliance with these standards is essential for colleges that handle sensitive information, such as personal health information, student records, and financial data. The literature emphasizes the importance of compliance and the need for colleges to stay up-to-date with evolving security standards and regulations. The NCES provides comprehensive guidelines on security management in educational settings, emphasizing the importance of compliance with relevant policies and standards (NCES, n.d.).

Literature on managing cybersecurity risks, including Bandura's Social Cognitive Theory (1986), advocates a proactive strategy. According to Bandura, organizations can learn and adapt through observation and experience, making strategic risk management an essential practice. NIST CSF 2.0 provided a framework for colleges to achieve this goal, emphasizing risk assessment, compliance, and a systematic approach to managing risks.

An essential aspect of strategic risk management is the development of a security-aware organizational culture that empowers individuals at all levels to take responsibility for securing information and systems. Fostering a culture of collaboration and information sharing among faculty, staff, and students helped create an environment in which cybersecurity was prioritized. In addition, promoting a continuous learning atmosphere ensured that all college members remained current with emerging threats and best practices. "The use of artificial intelligence (AI), the spear-phishing that seems

highly successful for many faculty and staff to fall prey to... AI will also be used against us in the attacks so that it may be a zero-sum game in the end' (Participant 1, personal communication, July 2024).

Bandura's Social Cognitive Theory (1986) provided an important foundation for understanding the proactive approach to cybersecurity risk management. According to Bandura, human behavior is influenced by a dynamic interplay between individual cognitive factors, environmental influences, and the behavior itself. The theory posits that individuals can learn new information and behaviors by observing others, which is particularly relevant when fostering a culture of cybersecurity awareness within U.S. colleges.

NIST CSF 2.0 became even more critical within the context of Bandura's theory. The proactive approach to managing cybersecurity risks, underpinned by Bandura's Social Cognitive Theory and structured through NIST CSF 2.0, formed the basis for a comprehensive strategy emphasizing risk assessment, compliance, and systematic risk management. This strategy highlights the importance of cultivating a security-aware culture within colleges, where individual behavior significantly impacts cybersecurity.

Personal factors refer to individual attitudes and knowledge about cybersecurity, while the environment encapsulates regulatory standards and NIST CSF 2.0. Behaviors pertain to the actions taken by individuals in college to manage cybersecurity risks. This interplay, as outlined by Bandura's theory, was central to fostering security-aware culture.

An essential step was cultivating a culture that promotes collaboration, information sharing, and continuous learning about emerging threats and best practices. This proactive environment empowers individuals at all levels to take responsibility for securing information and systems, aligning well with Bandura's concept of observational learning.

Thus, applying Bandura's Social Cognitive Theory enriched the understanding of the human factors involved in implementing NIST CSF 2.0 and managing cybersecurity risks, making cybersecurity in colleges more comprehensive and effective.

Regular security awareness training for all employees, including faculty and staff, is vital for maintaining a college's cybersecurity posture. This training covered the latest threats, mitigation strategies, and everyone's role in securing the colleges' digital assets.

Section 2: Cybersecurity Threats and Risk Management

US Colleges across America were not immune to the growing threat of cyberattacks; in many ways, these institutions became targets for hackers. Greenwald (2014) highlighted that cyber-attacks significantly threaten U.S. prosperity, with cybersecurity risks prevalent nationwide. Colleges and universities, which hold valuable information, such as financial and personal data, research, and intellectual property, have become prime targets for cybercriminals.

Effective risk management practices are critical for mitigating these risks, as emphasized by various scholars and industry bodies. According to the NIST, U.S. colleges were encouraged to continuously monitor and assess vulnerabilities to identify and remediate potential security gaps (CSRC Content Editor, n.d.-d). Alawida et al. (2022) advocated for a proactive approach to risk management, helping institutions detect and address vulnerabilities before attackers could exploit them. The NCES guidelines also stressed the importance of establishing incident response plans and training employees to respond to cyber incidents (Chapter 4-Security Management, from Safeguarding Your Technology, NCES Publication 98-297). Eling and Schnell (2016) argued that security plans should be regularly tested to ensure their effectiveness.

Cyber insurance also mitigates these risks. Companies that follow cybersecurity best practices and maintain cyber insurance are expected to benefit from lower insurance rates (Senthilkumar &

Easwaramoorthy, 2017). However, Eling and Schnell (2016) cautioned that cyber insurance should not substitute for a robust cybersecurity risk management strategy.

Effective cybersecurity practices require the implementation of both short-term and long-term goals aligned with the college's overall risk management strategy (CSRC Content Editor, n.d.-b; Cybersecurity Best Practices | Cybersecurity and Infrastructure Security Agency CISA, n.d.). Alawida et al. (2022) suggested specific steps U.S. colleges could take to implement short-term and long-term cybersecurity goals effectively. The following section explores strategies that U.S. colleges could employ to manage cybersecurity risks effectively, divided into short-term actions, offering immediate security improvements, and long-term goals that contribute to developing a sustainable cybersecurity infrastructure.

When discussing cybersecurity threats faced by U.S. colleges, it is crucial to consider the specific threat actors targeting these institutions, such as nation-state hackers, cybercriminals, hacktivists, and insider threats. These actors had various motivations, including financial gain, espionage, or disruption, but all could inflict significant damage on an institution under attack (Alawida et al., 2022).

Information sharing and collaboration also played a vital role in strengthening U.S. colleges' cybersecurity. This involved participating in industry-specific information-sharing organizations and partnering with local, state, and federal law enforcement agencies to exchange threat intelligence and best practices.

Ashraf et al. (2021) and Xie et al. (2020) emphasized the importance of a systematic and structured approach to managing cybersecurity risks. Ashraf et al. (2021) highlighted the benefits of using the NIST CSF 2.0 (NIST CSF 2.0) as a guideline for implementing comprehensive protection across an institution. On the other hand, Xie et al. (2020) proposed a conceptual framework for cyber risk scoring and mitigation that institutions could use to manage their cyber risks and optimize their cyber insurance policies. Their framework is based on four components: identification, assessment, treatment,

and monitoring. Both studies underscored the importance of identifying potential cyber risks, assessing them, developing treatment strategies, and monitoring the effectiveness of the implemented controls.

Senthilkumar and Easwaramoorthy (2017) also highlighted the benefits of cyber insurance in mitigating cybersecurity risks but cautioned that it should never be considered a substitute for a comprehensive cybersecurity risk management strategy. These scholars agreed on the importance of taking a proactive approach to managing cybersecurity risks, continuously monitoring and assessing vulnerabilities, and promoting a culture of collaboration and information-sharing among all college members.

Long-Term Goals

Long-term cybersecurity goals were designed to establish a sustainable cybersecurity stance that evolved with a changing threat landscape. These goals must align with the college's overall risk-management strategy and evaluate emerging threats and technologies. The long-term objectives included the following (EDUCAUSE, n.d.):

- **Implementing a cybersecurity NIST CSF 2.0**: NIST CSF 2.0 provides a structured approach to identifying, assessing, and managing cybersecurity risks.
- **Establishing a cybersecurity governance structure**: This structure is intended to define cybersecurity roles and responsibilities and provide an overview of cybersecurity practices.
- **Developing a cybersecurity awareness program**: An ongoing cybersecurity awareness program covers essential topics such as social engineering, phishing, and ransomware.
- **Conducting regular security assessments**: Regular assessments identify old and new vulnerabilities and ensure the continued effectiveness of existing security measures.

- **Implementing emerging technologies**: Emerging technologies such as AI and machine learning offer new opportunities for threat detection and incident response (EDUCAUSE, n.d.).

The successful implementation of short-term and long-term cybersecurity goals depends on several key factors. The importance of executive leadership support in effective risk management was highlighted in NIST CSF 2.0 (Force, 2018). Adequate budget allocation was also crucial, as demonstrated in Orlando's study on Cyber Risk Quantification (Orlando, 2021). Additionally, involving stakeholders from various departments in risk management fostered a holistic IT approach to cybersecurity, as recommended by the ISACA (Holistic IT governance, risk management, security, and privacy, n.d.). These elements provide the necessary resources and commitment to help colleges achieve their cybersecurity objectives.

The continuous review and evaluation of implemented security measures remain paramount to ensure their relevance and effectiveness in the face of evolving threats. This requires using metrics to measure the success of security initiatives and conducting regular reviews and audits to ensure compliance with industry standards and regulations (Holistic IT Governance, Risk Management, Security, and Privacy: Needed for Effective Implementation and Continuous Improvement, n.d.).

Short- and long-term cybersecurity goals are critical for U.S. colleges to protect themselves against cyber threats. Short-term objectives have laid the foundation for building long-term security standards that could adapt to the evolving threat landscape. Therefore, U.S. colleges need to establish goals aligned with their risk management strategies while considering emerging threats and new technologies.

In conclusion, cybersecurity risk management remains crucial for institutions, including U.S. colleges, to protect themselves against cyber threats. According to the National Institute of Standards

and Technology's NIST CSF 2.0 (NIST, n.d.), a strategic approach to risk management is essential for reducing vulnerabilities. Griffith (2022) further corroborated this by emphasizing that effective risk-mitigation practices could minimize risk exposure and safeguard sensitive information.

Third-Party Cyber Risk Management Section 3: Cyber Risk Management and Insurance

Effective cyber risk management and insurance safeguard institutions against potential cyber threats. Xie et al. (2020) proposed a conceptual framework for cyber risk-scoring and mitigation. Organizations utilize this framework to effectively manage cyber risks and optimize their cyber insurance policies. According to Xie et al. (2020), the conceptual framework for cyber risk management comprises four essential components: identification, assessment, treatment, and monitoring. Institutions have identified cyber risks threatening their information systems, including data breaches and cyber-attacks. An evaluation gauged the likelihood and potential impact of each identified risk. Based on these assessments, organizations strategized treatment plans that involved implementing controls such as firewalls and intrusion detection systems to mitigate these risks. The last component, monitoring, involved regular checks on the effectiveness of these controls to ensure that they continued to provide sufficient protection against evolving cyber threats. While the study primarily focused on banking, the framework underscored the importance of utilizing risk management methodologies to address cyber risk across various sectors, including educational institutions.

Eling and Schnell (2016) specifically explored the role of risk management frameworks in banking, emphasizing their utility in identifying and assessing cyber risks. They also advocated the development and implementation of adequate controls such as firewalls and intrusion detection systems to safeguard against potential threats. Force (2018) extended this argument by focusing on how these frameworks continuously monitor an institution's cybersecurity posture.

Adane (2020) took a slightly different approach by providing an empirical analysis that used probit regressions to study cyber risk management in the insurance sector. The study revealed that insurance companies that invested in robust cyber risk management practices and implemented adequate risk controls experienced lower rates of cyber losses and were better equipped to manage cyber risk.

These studies collectively highlight the essential nature of adopting a comprehensive risk management strategy that includes identification, assessment, treatment, and ongoing monitoring to effectively mitigate cyber risk in financial institutions.

Section 4: Third-Party Cyber Risk Management

Keskin et al. (2021) delved into the risks associated with institutions relying on third-party vendors and partners for essential services. This reliance has often opened new avenues for cybercriminals to exploit vulnerabilities. Keskin and colleagues explored using non-intrusive methods for conducting Cyber Third-Party Risk Management (C-TPRM) as a more efficient means of assessing the cybersecurity risks posed by these external partners. Their research compared the existing C-TPRM methods developed by different organizations to identify commonly used indicators and assessment criteria. The study emphasized the need for a structured and systematic approach to third-party risk assessment, which includes identifying and categorizing third-party vendors, thoroughly evaluating their cybersecurity posture, and implementing controls to mitigate associated risks.

In conclusion, effective cyber risk management remains indispensable for institutions, including U.S. colleges, which aim to protect themselves against ever-increasing cyber threats. According to the NIST CSF 2.0 set forth by the NIST (Force, 2018), a comprehensive and strategic approach to risk management was not just recommended but essential. This viewpoint was further corroborated by Griffith (2022), who emphasized that specific risk-mitigation practices could significantly reduce an

institution's risk exposure and enhance the protection of sensitive information. Keskin et al. (2021) highlighted the importance of assessing the cybersecurity risks posed by third-party vendors and partners, suggesting a structured approach for Cyber Third-Party Risk Management (C-TPRM). By incorporating these expert insights and adopting a proactive stance on cyber risk management and insurance, institutions have markedly reduced their susceptibility to cyber threats.

Conceptual Frameworks for Cyber Risk Scoring and Mitigation

Xie et al. (2020) proposed a conceptual framework for cyber risk scoring and mitigation, emphasizing the importance of risk assessment and control measures in managing cyber risks. They argued that implementing the NIST CSF 2.0s helped institutions identify potential cyber threats, develop effective controls, and monitor their cybersecurity posture over time. The authors conducted a broader empirical analysis with probit regressions on cyber risk management in insurance, highlighting the importance of investing in cyber risk management and implementing risk controls to lower the rates of cyber losses and better manage cyber risks. Keskin et al. (2021) also stressed the importance of a systematic approach for assessing third-party risks in institutions. They compared the existing methods for Cyber Third-Party Risk Management (C-TPRM) used by different companies to identify commonly used indicators and assessment criteria. The authors emphasized the need to identify and categorize third-party vendors, evaluate their cybersecurity posture, and implement risk-mitigation controls. Thus, both Xie et al. (2020) and Keskin et al. (2021) highlight the importance of a structured and flexible approach to assess and mitigate risks, implement controls, and monitor their effectiveness, whether for cyber risk management or third-party cyber risk management.

Emerging Cybersecurity Threats

Effective cyber risk management and insurance safeguard institutions against potential cyber threats. Xie et al. (2020) proposed a conceptual framework for cyber risk-scoring and mitigation.

Organizations utilize this framework to effectively manage cyber risks and optimize their cyber insurance policies. According to Xie et al. (2020), the conceptual framework for cyber risk management comprises four essential components: identification, assessment, treatment, and monitoring. Institutions have identified cyber risks threatening their information systems, including data breaches and cyber-attacks. An evaluation gauged the likelihood and potential impact of each identified risk. Based on these assessments, organizations strategized treatment plans that involved implementing controls such as firewalls and intrusion detection systems to mitigate these risks. The last component, monitoring, involved regular checks on the effectiveness of these controls to ensure that they continued to provide sufficient protection against evolving cyber threats. While the study primarily focused on banking, the framework underscored the importance of utilizing risk management methodologies to address cyber risk across various sectors, including educational institutions.

Eling and Schnell (2016) specifically explored the role of NIST CSF 2.0s in banking, emphasizing their utility in identifying and assessing cyber risks. They also advocated the development and implementation of adequate controls such as firewalls and intrusion detection systems to safeguard against potential threats. Force (2018) extended this argument by focusing on how these frameworks continuously monitor an institution's cybersecurity posture.

Adane (2020) took a slightly different approach by providing an empirical analysis that used probit regressions to study cyber risk management in the insurance sector. The study revealed that insurance companies that invested in robust cyber risk management practices and implemented adequate risk controls experienced lower rates of cyber losses and were better equipped to manage cyber risk.

These studies collectively highlight the essential nature of adopting a comprehensive risk management strategy that includes identification, assessment, treatment, and ongoing monitoring to effectively mitigate cyber risk in financial institutions.

Section 4: Third-Party Cyber Risk Management

Keskin et al. (2021) delved into the risks associated with institutions relying on third-party vendors and partners for essential services. This reliance has often opened new avenues for cybercriminals to exploit vulnerabilities. Keskin and colleagues explored using non-intrusive methods for conducting Cyber Third-Party Risk Management (C-TPRM) as a more efficient means of assessing the cybersecurity risks posed by these external partners. Their research compared the existing C-TPRM methods developed by different organizations to identify commonly used indicators and assessment criteria. The study emphasized the need for a structured and systematic approach to third-party risk assessment, which includes identifying and categorizing third-party vendors, thoroughly evaluating their cybersecurity posture, and implementing controls to mitigate associated risks.

In conclusion, effective cyber risk management remains indispensable for institutions, including U.S. colleges, which aim to protect themselves against ever-increasing cyber threats. According to NIST CSF 2.0, established by the National Institute of Standards and Technology (Force, 2018), a comprehensive and strategic approach to risk management is essential. This viewpoint was further corroborated by Griffith (2022), who emphasized that specific risk-mitigation practices could significantly reduce an institution's risk exposure and enhance the protection of sensitive information. Keskin et al. (2021) highlighted the importance of assessing the cybersecurity risks posed by third-party vendors and partners, suggesting a structured approach for Cyber Third-Party Risk Management (C-TPRM). By incorporating these expert insights and adopting a proactive stance on cyber risk management and insurance, institutions have markedly reduced their susceptibility to cyber threats.

Conceptual Frameworks for Cyber Risk Scoring and Mitigation

Xie et al. (2020) proposed a conceptual framework for cyber risk scoring and mitigation, emphasizing the importance of risk assessment and control measures in managing cyber risks. They argued that implementing NIST CSF 2.0s helped institutions identify potential cyber threats, develop effective controls, and monitor their cybersecurity posture over time. The authors conducted a broader empirical analysis with probit regressions on cyber risk management in insurance, highlighting the importance of investing in cyber risk management and implementing risk controls to lower the rates of cyber losses and better manage cyber risks. Keskin et al. (2021) also stressed the importance of a systematic approach for assessing third-party risks in institutions. They compared the existing methods for Cyber Third-Party Risk Management (C-TPRM) used by different companies to identify commonly used indicators and assessment criteria. The authors emphasized the need to identify and categorize third-party vendors, evaluate their cybersecurity posture, and implement risk-mitigation controls. Thus, both Xie et al. (2020) and Keskin et al. (2021) highlight the importance of a structured and flexible approach to assess and mitigate risks, implement controls, and monitor their effectiveness, whether for cyber risk management or third-party cyber risk management.

2.5 Emerging Cybersecurity Threats

US Colleges faced significant cybersecurity threats, as they handled a large amount of sensitive data and were increasingly targeted by cybercriminals (OIG-23-01 - DHS OIG - Homeland Security, n.d.). Among the emerging threats, ransomware attacks have become more frequent, where attackers gain unauthorized access to college systems and demand payment to release encrypted data. Social engineering techniques, particularly phishing attacks, have become increasingly sophisticated and difficult to detect. Additionally, insider threats posed challenges, as insiders had legitimate access to the systems they exploited. To remain informed of the latest cybersecurity threats, U.S. colleges monitored

threat intelligence sources, collaborated with other institutions, and conducted regular security assessments and penetration testing (Griffith, 2022; Fujs et al., 2019).

US Colleges adopted comprehensive risk management strategies to effectively manage these emerging cybersecurity threats. The National Institute of Standards and Technology's CSF 2.0 emphasized actively monitoring threat intelligence sources as part of a robust cybersecurity strategy (Force, 2018). Collaboration with other institutions and industry groups is also recommended to stay ahead of evolving cyber threats (Griffith 2022). Regular security assessments and penetration testing have proven crucial for identifying vulnerabilities and enhancing security measures (Fujs et al., 2019). Cybersecurity training and awareness programs for faculty, staff, and students are deemed necessary to improve an institution's overall cybersecurity posture (IBM Thought Leadership, n.d.).

Furthermore, implementing access controls to limit unauthorized access to sensitive data has become a standard risk-management practice (Landoll, 2020). Monitoring the network activity for potential attacks has also emerged as a key component of cybersecurity frameworks (ISO/IEC JTC 1/SC 27, 2023). U.S. colleges manage risks effectively by implementing these measures, safeguarding sensitive data, and maintaining stakeholder trust (Keskin et al., 2021).

In addition to ransomware, phishing, and insider threats, U.S. colleges faced other significant risks that impacted their operations and reputations. For example, distributed denial-of-service (DDoS) attacks overloaded college networks, rendering them inaccessible to users and causing substantial disruptions (NCES, n.d., Chapter 5 - Protecting Your System: Physical Security from Safeguarding Your Technology). U.S. colleges have increasingly become targets for advanced cyber-attacks, including Advanced Persistent Threats (APTs). These sophisticated attackers have deployed advanced tactics to gain unauthorized access to educational systems and exfiltrate-sensitive data (Griffith, 2022; Eling & Schnell, 2016). This elevated risk necessitates the implementation of state-of-the-art cybersecurity

measures. U.S. colleges employ cybersecurity tools and technologies to effectively counter these threats, including next-generation firewalls, intrusion detection and prevention systems (IDPS), and SIEM solutions. According to Force (2018), a layered security architecture integral to NIST CSF 2.0 was recognized as the best practice for safeguarding information systems. Moreover, the use of these tools improves detection and prevention capabilities and enhances visibility of network activities, allowing for timely monitoring and response to security incidents (Simos, 2021; NIST, n.d.).

Consistent with existing research, adopting established cybersecurity frameworks, such as the NIST Cybersecurity Framework and ISO/IEC 27001, proved beneficial for U.S. colleges (Force, 2018; ISO/IEC JTC 1/SC 27, 2023). These frameworks offer structured methods for managing cybersecurity risks (NIST et al.; Insurance et al. No. 2, 2021). Implementing such standards enables educational institutions to proactively develop effective risk-management strategies and identify vulnerabilities before they are exploited (Keskin et al., 2021; Eling & Schnell, 2016).

Finally, as suggested by the Ponemon Institute's report on "The Cyber Resilient Organization: Learning to Thrive Against Threats," U.S. colleges were highly recommended to form partnerships with cybersecurity experts and industry organizations. These collaborations facilitated information sharing and best practices, enabled participation in threat intelligence programs, and promoted cooperative efforts in cybersecurity research and development. These partnerships serve as valuable resources, allowing colleges to stay ahead of emerging threats and maintain a robust cybersecurity posture (Ponemon Institute, n.d.).

Consistent with existing research, adopting established cybersecurity frameworks, such as the NIST Cybersecurity Framework and ISO/IEC 27001, can be beneficial for U.S. colleges (Force, 2018; ISO/IEC JTC 1/SC 27, 2023). These frameworks offer structured methods to manage cybersecurity risks (NIST CSF 2.0, n.d.). Insurance Circular Letters No. 2, 2021). Implementing such standards allows

educational institutions to proactively develop effective risk management strategies and to identify vulnerabilities before they become exploitable (Keskin et al., 2021; Eling & Schnell, 2016).".

Lastly, as suggested by the Ponemon Institute's report on The Cyber Resilient Organization: Learning to Thrive Against Threats, it is highly recommended that U.S. colleges consider forming partnerships with cybersecurity experts and industry organizations. Such collaborations can facilitate the sharing of information and best practices, enable participation in threat intelligence programs, and promote cooperative efforts in cybersecurity R&D. These partnerships could serve as valuable resources, allowing colleges to stay ahead of emerging threats and maintain a robust cybersecurity posture (Ponemon Institute n.d.).

AI Influence

AI has attracted significant attention in cybersecurity in recent years. This trend of AI's growing role is expected to continue, as highlighted in the National Security Commission on NSCAI's Final Report (n.d., Section on AI and Cybersecurity). AI-based cybersecurity solutions allow institutions to detect and prevent cyber threats in real-time. They worked by analyzing large volumes of data and identifying patterns and anomalies that human operators might have overlooked otherwise. AI's capabilities extend to automating various aspects of cybersecurity protocols, including threat intelligence gathering and incident response, thereby elevating the efficiency and effectiveness of cybersecurity operations (NSCAI Final Report, n.d., Section on AI and Cybersecurity).

One area where AI has shown significant promise is the detection of malware and other types of cyber threats. Machine learning algorithms analyze substantial data and identify patterns and behaviors indicative of malicious activities. This method helps institutions detect and prevent cyber-attacks before they cause considerable damage (Musser & Garriott, 2021).

AI has also affected the development of predictive analytics. By analyzing large datasets, AI identifies potential vulnerabilities and uses these data to predict where future attacks might occur. As a result, AI has helped institutions prioritize their cybersecurity efforts and allocate resources more effectively (Franzke et al., 2021).

In addition, AI contributes to automating the incident response process by providing real-time alerts and automating specific response actions, such as isolating infected systems and containing the spread of malware (Musser & Garriott, 2021). This methodology helps institutions respond to cyber-attacks more quickly and effectively, minimizing the impact on their operations and data (Musser & Garriott, 2021).

The rapid integration of AI technologies in educational institutions has transformed the cybersecurity landscape. AI-driven tools such as automated threat detection systems and predictive analytics substantially enhance security measures. However, as these institutions increasingly adopt AI, there are growing concerns about its ethical and legal implications, particularly related to handling Personally Identifiable Information (PII).

According to a recent BBC report (2024), many organizations are adopting AI solutions without fully understanding their legal responsibilities regarding data privacy. For educational institutions that handle sensitive information such as student records, financial details, and health data, the misuse or mishandling of PII can lead to significant legal consequences, especially under regulations such as the General Data Protection Regulation (GDPR) and the Family Educational Rights and Privacy Act (FERPA).

Researchers have highlighted the importance of conducting privacy impact assessments before deploying AI tools to ensure compliance with data protection laws. For instance, Perna (2024) highlighted that while AI systems can automate many processes, they also introduce risks if privacy

safeguards are not adequately considered. The literature emphasizes the need for continuous governance and audits of AI tools to assess compliance and minimize potential data breaches.

Although AI has the potential to revolutionize cybersecurity, it also presents certain challenges and risks. One concern was that cybercriminals could use AI to develop more sophisticated and effective attacks, making it more difficult for institutions to defend themselves against them (IBM Thought Leadership, n.d.). Additionally, using AI in cybersecurity could lead to false positives or false negatives, potentially resulting in security breaches or excessive security measures being taken (Musser & Garriott, 2021).

Despite these challenges, the potential benefits of AI in cybersecurity remain significant. As the number and complexity of cyber threats grow, AI-based solutions help institutions stay ahead of the curve and protect their sensitive data and assets (Griffith, 2022).

Legal and Ethical Challenges of AI Adoption

In recent years, there has been a significant push for organizations, including educational institutions, to adopt AI technologies to enhance their efficiency and streamline operations. However, as AI adoption accelerates, many institutions have overlooked critical legal and ethical issues, particularly concerning the handling of Personally Identifiable Information (PII).

According to recent reports, while AI-driven tools can optimize processes, such as automated data analysis and threat detection, they can also inadvertently expose sensitive information if not properly managed (BBC, 2024). As highlighted by Perna (2024), organizations often prioritize the immediate benefits of AI, such as increased productivity and cost savings, while neglecting compliance with privacy regulations such as the General Data Protection Regulation (GDPR)and Family Educational Rights and Privacy Act (FERPA).

The lack of adequate safeguards for PII is a significant concern, especially for educational institutions that handle vast amounts of sensitive data, including student records, health information, and financial details. Failure to protect these data risks legal penalties and damages institutional trusts and reputations. As AI tools become more integrated into cybersecurity strategies, institutions must implement privacy impact assessments and regular audits to ensure compliance with the existing regulations.

Related Variables

Numerous studies have highlighted the importance of several variables related to strategic risk management and cybersecurity that are considered necessary for effective risk management (NIST, n.d.). These variables include security risk assessment, incident response planning, employee training, and cyber-insurance.

Security risk assessment was identified as a critical part of strategic risk management. It involves identifying, evaluating, and prioritizing risks based on their likelihood and potential impact (Musser & Garriott, 2021). Practical security risk assessments helped institutions develop and implement risk management strategies tailored to their specific needs and vulnerabilities (The Cyber Resilient Organization: Learning to Thrive Against Threats: Ponemon Institute, n.d.). By conducting regular security risk assessments, institutions can identify potential security weaknesses and implement proper risk-mitigation measures to protect against cyber threats (IBM Thought Leadership, n.d.).

Incident response planning is another essential variable that involves developing a plan to respond to and recover from cybersecurity incidents (Musser and Garriott 2021). Such planning has helped institutions minimize the impact of security breaches and quickly resume normal operations (The Cyber Resilient Organization: Learning to Thrive Against Threats: Ponemon Institute, n.d.). The incident response plan included the roles and responsibilities of key personnel, procedures for detecting and

responding to incidents, and guidelines for communicating with stakeholders (IBM Thought Leadership n.d.).

Employee training has emerged as a vital factor for effective risk management. A study by Orlando (2021) showed that many cybersecurity incidents are attributable to human errors or behaviors, underscoring the crucial role of employee training in averting cyber threats. This study explored the need for employees to undergo regular training sessions, covering topics such as identifying potential threats, recognizing phishing attempts, averting social engineering attacks, and promptly reporting suspicious activities.

Beyond regular training sessions, institutions have fostered a culture of cybersecurity awareness among their employees. According to Cerra (2019), creating a cybersecurity culture involves advocating best practices in password management, data protection, and secure communication. Providing employees with channels to anonymously report security incidents was found to be effective in identifying and mitigating potential threats before escalating.

Practical employee training also involves gamification and simulation-based training methods, which engage employees and make the training more interactive and memorable. The simulations provided realistic scenarios that allowed employees to identify and respond to cyber threats in a safe environment.

Institutions also consider providing targeted training for employees in specific roles or with access to sensitive information (Senthilkumar & Easwaramoorthy, 2017). This includes training on secure data handling practices for developers or proper data handling and storage for employees with sensitive data (Franzke et al., 2021).

Evaluating the effectiveness of these training programs is essential to ensure that employees are adequately prepared to mitigate cyber risks (IBM Thought Leadership, n.d.). This evaluation involved

monitoring employee behavior and conducting regular assessments to identify areas where additional training might have been necessary (New Cybersecurity Resources for Institutes of Higher Education, 2023).

Research has shown that integrating continuous evaluation and adaptive training programs significantly improves the effectiveness of employee cybersecurity training. Institutions that incorporate metrics-based approaches, such as tracking response times to simulated phishing attacks and adherence to security protocols, can address specific vulnerabilities better (IBM Thought Leadership, n.d.). By tailoring training initiatives based on these insights, institutions strengthen their risk management strategies, ensuring that resources are focused on where they are most needed (New Cybersecurity Resources for Institutes of Higher Education, 2023).

Cybersecurity insurance, for instance, is a financial safety net and a driver for adherence to better security practices. Given U.S. colleges' constrained budgets, understanding the utility and effectiveness of such insurance policies offers the necessary policy guidance (Spitzner, 2022).

Additionally, this study addresses a critical gap in the existing research concerning the effectiveness of these tools and strategies in managing cybersecurity risks. While cybersecurity insurance, third-party security companies, and specialized software have all gained popularity, their efficacy within U.S. colleges is yet to be adequately researched.

Research on cybersecurity insurance, third-party security services, and NIST CSF 2.0 has shown varied levels of effectiveness when applied in higher education settings (Franzke et al., 2021; Senthilkumar & Easwaramoorthy, 2017). Studies indicate that, while these measures can enhance security postures, their success is often contingent upon how well they are integrated into the institution's overall risk management strategy (Orlando, 2021). For instance, institutions that proactively align their policies with NIST guidelines tend to demonstrate improved resilience against cyber threats,

whereas those relying heavily on third-party solutions without sufficient internal capacity may face increased vulnerabilities (Cerra 2019).

Themes

The literature on strategic risk management and cybersecurity has several themes. These themes included the need to adhere to NIST CSF 2.0, continuous monitoring and vulnerability assessments, incident response planning, employee training and awareness, and emerging trends in cyber insurance (Insurance et al. No. 2, 2021). The literature highlights the need for a strong organizational security culture, starting with leadership's commitment to cybersecurity by allocating resources and setting policies. Collaboration and communication between departments were emphasized to ensure a coordinated approach to risk management.

Existing research highlights the increasing adoption of emerging technologies, such as AI, machine learning, and blockchain, to enhance cybersecurity measures within educational institutions (Orlando, 2021; Franzke et al., 2021). While these technologies offer advanced capabilities for monitoring and threat detection, studies indicate that institutions face challenges in implementation, particularly related to integration with existing systems and the need for specialized expertise (Senthilkumar & Easwaramoorthy, 2017). Furthermore, the literature emphasizes the importance of maintaining human oversight and judgment when employing these technologies to avoid over-reliance and ensure effective decision making in dynamic threat environments (Cerra 2019).

Conclusion

The reviewed literature indicates that strategic risk management and cybersecurity are essential for U.S. colleges. NIST CSF 2.0 provided a structured and flexible means for implementing organizational-wide protection against cyber threats. Effective risk management practices include continuous

monitoring, vulnerability assessments, and incident response planning, while preparing for emerging security threats. Cyber insurance was increasingly seen as an intelligent move in risk mitigation, supported by research from Xie, Lee, and Eling (2020), which showed how it promoted good security behavior among institutions. However, more work remains, as researchers such as Orlando (2021) and Woods et al. (2017) have stressed the importance of studying this across different industries. As for third-party cyber risk management (C-TPRM), efficient and non-intrusive methods need exploration, a point emphasized by recent work by Yeo and Yeo (2023).

The literature on cybersecurity in higher education frequently highlights the importance of standardized frameworks, such as NIST CSF 2.0, and the HEISC Cybersecurity Framework for Higher Education. These frameworks provide institutions with structured guidance on implementing best practices and addressing risks unique to the higher education environment. The NIST framework emphasizes comprehensive risk management across all stages of a cybersecurity incident, while the HEISC framework offers tailored strategies that accommodate the particular needs and constraints of U.S. colleges. These approaches underscore the value of adopting proven frameworks to improve the security posture of higher education institutions.

The review underscored a notable gap in the literature: the need for comprehensive research tailored explicitly to the cybersecurity needs and challenges of the U.S. college sector. This study addressed this void by providing an in-depth analysis focused on implementing strategic risk management and cybersecurity best practices within U.S. colleges.

Chapter 3 - Methodology

Study Framework Outline

The researcher built upon the theoretical foundations established in Chapter 1 to apply Resource Dependency Theory (RDT) and the NIST Cybersecurity Framework (CSF 2.0) to guide the research design. The RDT provided a lens for understanding how U.S. colleges, often constrained by limited internal resources, strategically leveraged external partnerships, such as third-party cybersecurity firms and insurance providers, to strengthen their security measures. This theoretical framework informed the selection of case studies, focusing on institutions that rely heavily on external resources to manage cybersecurity risks.

The NIST CSF Framework was crucial in structuring the data collection process, mainly in assessing how U.S. colleges identified, protected, detected, responded to, and recovered from cyber threats. This framework ensured that the interview questions and document analysis aligned with the key cybersecurity domains, enabling a more comprehensive evaluation of institutional practices.

The researcher integrated the Social Cognitive Theory (Bandura, 1986) into the research design to evaluate the effectiveness of staff training and awareness programs in fostering compliance with cybersecurity protocols. This study identified the best practices that enhanced cybersecurity awareness and reduced vulnerabilities by examining how training initiatives shaped staff behaviors.

The Technology Acceptance Model (TAM) was applied to understand the factors influencing the adoption of new cybersecurity technologies within these institutions. This framework guided the analysis of the interview data related to staff perceptions of ease of use and usefulness, which are critical factors in technology adoption. By focusing on the practical applications of these theoretical

models, this study provides actionable insights into the factors that impact cybersecurity practices and adoption in resource-constrained educational environments.

This integrated approach ensured a robust analysis of how external dependencies, internal training programs, and technology adoption collectively influenced the cybersecurity strategies of U.S. colleges. The frameworks guided the methodology and enhanced the interpretation of the findings, offering practical recommendations for improving cybersecurity in higher education.

Purpose of the Study

This study explored the best practices in cybersecurity standards adopted by U.S. colleges, including reliance on security firms, third-party software, endpoints, and cybersecurity insurance. In line with the cybersecurity standards proposed by the NIST CSF 2.0 (NIST, n.d.) and guided by recent developments in cybersecurity resource availability for institutes of higher education (New Cybersecurity Resources for Institutes of Higher Education Available, 2023), this study comprehensively examined the current cybersecurity landscape in U.S. colleges. The objective was to identify the effectiveness of varying layers of cybersecurity measures—from adopting third-party security solutions to cybersecurity insurance—in mitigating risks and vulnerabilities. The study evaluated the security firms' role and the effectiveness of endpoint solutions. Furthermore, the study explored how U.S. colleges can evolve these strategies to anticipate and counter emerging cyber threats by leveraging historical trends and expert insights to enhance their cybersecurity.

Research Questions

This study was guided by the following research questions:

1. What are the best practices in the U.S. college environment for the use of security firms, third-party software, endpoints, and cybersecurity insurance?
2. What is their influence on the overall security posture of U.S. colleges?
3. How can U.S. colleges evolve their cybersecurity strategies to anticipate and counter emerging cyber threats based on historical trends and expert insights?

Theoretical and Conceptual Frameworks

The overarching theoretical framework, Resource Dependency Theory (RDT), and two primary conceptual frameworks—the NIST CSF 2.0 (NIST CSF 2.0) and the Cybersecurity Framework for Higher Education developed by the Higher Education Information Security Council (HEISC)—guided this research. Before delving into these conceptual frameworks, it is essential to first discuss RDT, which serves as an overarching lens through which the research questions were formulated. According to Pfeffer and Salancik (2003), organizations are only partially self-sufficient and must engage in transactions with other entities to obtain essential resources. For U.S. colleges, these transactions often include contracts with third-party security firms, software licenses, and cybersecurity insurance policies. RDT elucidates how dependence on external resources affects organizational behavior and decision-making processes in the context of cybersecurity.

Understanding this dependency became vital when assessing the unique cybersecurity challenges U.S. colleges faced. These institutions often operate with limited budgets and resources, making them dependent on various external entities to meet their cybersecurity needs. Thus, RDT

provides a valuable perspective for analyzing U.S. colleges' trade-offs and decisions in their cybersecurity strategies.

Building upon this theoretical foundation, this study employed two specific conceptual frameworks to examine the cybersecurity measures adopted by U.S. colleges. These frameworks provide a comprehensive understanding of educational institutions' unique cybersecurity challenges and solutions.

The NIST CSF 2.0 (NIST CSF 2.0) is a widely recognized and adopted framework that provides a structured and flexible approach to managing cybersecurity risks within an institution. NIST CSF 2.0, comprised of six core functions:

- Govern: Establish organizational governance structures to manage cybersecurity risk.
- Identify: Develop an understanding of the organization's cybersecurity risks.
- Protect: Implement safeguards to ensure the delivery of critical services.
- Detect: Develop activities to identify the occurrence of cybersecurity events.
- Respond: Implement actions to address detected cybersecurity incidents.
- Recover: Develop plans to maintain resilience and restore capabilities impaired by cybersecurity incidents.

By following NIST CSF 2.0, U.S. colleges systematically identified, evaluated, and mitigated the risks associated with their information systems.

This study references the Higher Education Information Security Council (HEISC) framework, which provides cybersecurity resources and guidance specifically for the higher education sector.

Although the HEISC does not formally define its own set of core functions, it aligns with principles similar to those found in the NIST Cybersecurity Framework. HEISC resources help institutions, particularly those facing resource limitations such as U.S. colleges, prioritize cybersecurity efforts in line with widely accepted practices (EDUCAUSE, n.d.).

Complementary Role with NIST CSF 2.0

While the NIST Cybersecurity Framework 2.0 (CSF 2.0) includes six core functions—Identify, Govern, Protect, Detect, Respond, and Recover— offers a structured approach for managing cybersecurity risks across sectors, HEISC focuses specifically on applying cybersecurity best practices within the unique context of higher education. By combining NIST CSF 2.0's structured framework with HEISC's sector-specific insights, this study uses a dual approach that addresses both general cybersecurity risks and the particular challenges faced by U.S. colleges.

While NIST CSF 2.0 is procedural and prescriptive, guiding institutions through a step-by-step process to manage cybersecurity risks, the HEISC Cybersecurity Framework offers a strategic approach that emphasizes a comprehensive and adaptable set of practices aligned with the Five Core Functions, which allows for a multifaceted understanding of the cybersecurity landscape in U.S. colleges, enriching the study's findings and recommendations.

This study utilized NIST CSF 2.0 and the HEISC Cybersecurity Framework, which incorporates the Five Core Functions, to provide a comprehensive overview of the cybersecurity measures in U.S. colleges. NIST CSF 2.0 informed the evaluation of the specific controls and processes in place, offering a step-by-step procedural approach. At the same time, the Five Core Functions integral to the HEISC Cybersecurity Framework served as an overarching guide to assess the strategic aspects of cybersecurity programs. Employing these two interconnected frameworks allowed for a multifaceted understanding of the cybersecurity landscape in U.S. colleges, enriching the study's findings and recommendations.

The Cybersecurity Framework for Higher Education, developed by HEISC, offers guidance and best practices tailored specifically to the higher education sector. This framework emphasizes the importance of a robust cybersecurity posture in protecting sensitive information and maintaining uninterrupted operations. The HEISC Cybersecurity Framework was organized around Six Core Functions: (1) Govern, (2) Identify, (3) Protect, (4) Detect, (5) Respond, and (6) Recover. By aligning with these core functions, U.S. colleges have developed and implemented effective cybersecurity strategies that address their unique needs and vulnerabilities (Tabassi, 2023).

Incorporating RDT as the overarching theoretical framework and NIST CSF 2.0, and the HEISC Cybersecurity Framework as conceptual lenses allowed for a comprehensive and multifaceted approach to understanding and addressing cybersecurity challenges in U.S. colleges. By integrating these frameworks, this study provides valuable insights and practical recommendations for improving cybersecurity risk management practices in the U.S. college context.

Research Design Within Theoretical Context

This study used a qualitative multi-case study methodology to explore complex relationships and understand the nuances of real-world settings (Yin, 2018). Such an approach provides an in-depth examination of cybersecurity risk management practices in U.S. colleges, guided by Resource Dependency Theory (RDT) and the cybersecurity frameworks utilized in the study. Employing case studies offers insights into the dynamics of specific contexts, making it a suitable method for exploring how U.S. colleges manage cybersecurity risks with limited resources and external dependencies.

Aligned with Yin's work on case studies (Yin, 2017), the qualitative approach involves collecting non-numerical data through in-depth interviews (Kvale & Brinkmann, 2015), historical (archival) documents (Krueger & Casey, 2014), and document analysis (Bowen, 2009). This approach allowed the

study to explore how the principles of RDT and the HEISC Cybersecurity Framework, including the Six Core Functions, were applied or manifested in practice.

For data collection and analysis, this study employed a combination of thematic analysis (Braun & Clarke, 2006), content analysis (Krippendorff, 2018), and case study methodology (Glaser & Strauss, 1967). These methods were integrated into the research design to align with the theoretical frameworks, ensuring that the collected data were systematically examined and interpreted. By grounding the data analysis in these established approaches, the study maintained consistency with its theoretical basis, which supports its overall credibility and methodological rigor (Creswell and Poth 2017).

This integrated approach allowed for a comprehensive and nuanced understanding of cybersecurity risk management in U.S. colleges and facilitated the triangulation of findings from different data sources. This addressed potential limitations and biases, ultimately enhancing the credibility and validity of the study's findings.

Selection of RDT

This study adopted a qualitative research approach, inspired by the theoretical frameworks presented in Chapter 1—RDT (Pfeffer & Salancik, 1978) and Cybersecurity Frameworks (NIST, 2018; Tabassi, 2023). The qualitative methodology was purposefully chosen to align with the exploratory nature of this research, which aimed to identify effective cybersecurity practices in U.S. colleges (Fujs et al., 2019; Yin, 2014). By integrating this approach, this study comprehensively explored the complex dynamics within these institutions.

The RDT (Pfeffer & Salancik, 1978) guided the exploration of U.S. colleges' reliance on various resources for cybersecurity measures, reinforcing the methodology's alignment with the theoretical framework. The Cybersecurity Frameworks, including the NIST CSF 2.0 (NIST, 2018) and the Six Core

Functions (Tabassi, 2023), provided normative guidelines that informed the evaluation of cybersecurity practices, ensuring rigor and relevance in the analysis.

Moreover, the qualitative approach is highly suited for uncovering social processes and patterns of interaction—precisely, the types of processes and interactions involved in adopting and implementing cybersecurity standards (Kvale & Brinkmann, 2015; Krueger & Casey, 2014).

To delve into these complexities, this study employed systematic yet flexible procedures to gather and analyze data (Braun & Clarke, 2006; Krippendorff, 2018). This approach aligns with RDT's emphasis on the dynamic relationships between organizations and their environments (Hillman et al., 2009), enabling a deeper exploration of how U.S. colleges interact with external stakeholders and resources for cybersecurity.

Finally, the research design was iterative, allowing continuous data collection and analysis (Glaser and Strauss 1967). This process has enabled a more nuanced understanding of the complex and dynamic nature of cybersecurity practices in U.S. colleges (Creswell & Poth, 2017).

Based on the research questions, the focus on social processes, and the goal of developing a comprehensive understanding rooted in empirical data (Yin, 2014), a qualitative research approach underpinned by RDT and Cybersecurity Frameworks emerged as the most suitable methodology for this study (Creswell & Poth, 2017).

Beyond the selection of the case study methodology as an overarching methodology, the study was further guided by several theoretical frameworks. These frameworks informed the research questions and objectives, and provided valuable lenses for interpreting the data collected. These sub-frameworks include the following:

• **TAM (Davis, 1989)**: As a supporting theoretical perspective, the TAM helped explore the factors influencing technology adoption in cybersecurity measures, complementing the study's main frameworks. While the Technology Acceptance Model (TAM) highlights that the perceived usefulness and ease of use of AI tools drive their adoption, a growing body of literature points out the potential challenges related to privacy and compliance. According to recent findings, institutions adopting AI-driven tools often prioritize efficiency over legal safeguards, which can lead to breaches of privacy (BBC 2024). Ensuring that these technologies align with data protection laws is essential to gaining user trust and widespread acceptance within educational settings.

• **RDT (Pfeffer & Salancik, 1978)**: This theory was central to examining power dynamics and external dependencies, directly informing the methodological approach.

• **NIST CSF 2.0 (NIST, n.d.)**: This comprehensive framework guided the study's focus on risk management practices specific to U.S. colleges.

• **Cybersecurity Insurance Framework (Insurance et al. No. 2, 2021)**. As a sub-framework, it outlined the best practices for financial risk management, contributing to the study's evaluation of cybersecurity insurance policies.

• **Coopetition Theory (Brandenburger & Nalebuff, 1996)**: This theory provides a lens for examining collaboration and information sharing among institutions, relevant to the study's focus on U.S. colleges' cooperation in cybersecurity.

• **Social Cognitive Theory (Bandura, 1986)**: This framework supports the exploration of cybersecurity awareness and training programs by understanding how new behaviors are learned and adopted.

Each sub-framework informed the research questions and objectives and the analysis and interpretation of the data collected.

Integration of RDT in the Research Design

The qualitative methodology used in this study is closely integrated with RDT (Pfeffer & Salancik, 1978), which serves as the theoretical foundation. The RDT provides a framework for examining how U.S. colleges depend on external resources for their cybersecurity measures. The RDT aligns with the research questions and social processes explored in this study by focusing on the dynamic relationships between these institutions and their environments. This integration ensures that the study remains grounded in a theory that is directly relevant to the challenges faced by U.S. colleges in managing cybersecurity.

Research Design

To better understand how U.S. colleges handle cybersecurity and how these practices affect their security posture, a qualitative case study approach was used. This method ties closely with the theoretical foundations of the study, such as Resource Dependency Theory (RDT) and established cybersecurity guidelines, to keep the research grounded. By collecting and analyzing qualitative data, the study was able to closely examine the reliance on different cybersecurity strategies, leading to practical recommendations for improvement. This structured method, supported by well-known frameworks and detailed analysis, helps ensure that the findings are accurate, trustworthy, and relevant.

Qualitative Research Techniques

This study utilized a **qualitative case study approach** to explore cybersecurity practices within U.S. colleges. This approach allowed for an in-depth exploration of the strategies employed and their

impact on the security posture of institutions. Qualitative data collection techniques, such as interviews, multi-case studies, and the analysis of historical documents, provide comprehensive insights into the factors contributing to effective cybersecurity measures. By examining these cases, the research identified patterns and recommendations for improvement, ensuring a detailed understanding of the challenges and solutions faced by U.S. colleges (Baxter & Jack, 2015; Yazan, 2015).

This case study approach also facilitated the exploration of complex issues that are not readily quantifiable, aligning with the study's objective of assessing the effectiveness of cybersecurity strategies. The findings contribute to a holistic understanding of the institutional factors influencing cybersecurity practices, thereby enriching the analysis and providing practical recommendations for improvement.

Study Settings

This study was conducted using a sample of three U.S. colleges in different states throughout the United States. The three colleges that participated in the study were selected based on their geographic location, size, history of cyber incidents, organizational structure, resources, and approaches to handling cybersecurity risks. The selection was intentional, as it provided an opportunity to explore the unique aspects of cybersecurity in diverse geographical and socioeconomic environments, reflecting the various nature of the U.S. higher education system.

By examining cybersecurity risk management practices at the chosen U.S. colleges, this study aimed to shed light on the challenges faced by these institutions while tackling cybersecurity threats. This study also suggests potential strategies for effectively managing these risks. Furthermore, the study setting helped identify similarities and differences in cybersecurity risk management practices across various colleges/institutions, providing valuable information for policymakers, staff, faculty, students, and educational leaders seeking to enhance cybersecurity posture within the higher education sector.

Study Participants

The study participants were carefully selected based on specific criteria to ensure that they had comprehensive knowledge and involvement in their respective U.S. colleges' cybersecurity risk management practices. The participants included U.S. college administrators, IT staff, and faculty members who were directly engaged in decision-making and implementing cybersecurity policies and procedures. A purposeful sampling strategy was employed to identify and recruit participants with a substantial understanding of their institutions' cybersecurity environments.

Higher-education administrators

These individuals play a pivotal role in cybersecurity decision-making processes. Their insights provided an understanding of the strategies and policies at the institutional level. Administrators were selected based on their involvement in cybersecurity decision making and their years of service in administrative roles.

IT Staff:

IT personnel are directly involved in implementing and monitoring cybersecurity measures. They provided a hands-on perspective on the current practices' challenges, effectiveness, and gaps. Participants in this category were selected based on their role in cybersecurity management and their experience in the field.

Process for Selecting the Involved Participants

1. Reaching out to the administrative offices of U.S. colleges to request a list of potential participants who hold critical roles in cybersecurity risk management.

2. The roles and responsibilities of the listed individuals are reviewed to ensure that they possess adequate knowledge and experience in cybersecurity risk management.

3. Extending invitations to selected individuals, outlining the purpose of the study and their expected involvement, and requesting their consent to participate.

4. Interested participants were followed up to confirm the availability and schedule of data collection sessions.

Instrumentation

Qualitative research tools were used for Data collection, including semi-structured questionnaire interviews, case study methodology, and historical studies. This approach ensured that the study provided a comprehensive and in-depth understanding of cybersecurity risk management practices in selected U.S. colleges.

Review of Historical Studies: This study reviewed past and existing cybersecurity policies and incidents at U.S. colleges to understand how risk management strategies have evolved. This method provided a context for current practices and helped identify enduring challenges and successful strategies. The research began by examining cybersecurity policies and incidents in selected U.S. colleges. The intent was to explore the evolution of risk-management strategies over time and their impact on current practices. This study delved into the changes in cybersecurity measures, considering technological advancements and the increasing sophistication of cyber threats. Additionally, this retrospective analysis highlighted the enduring challenges faced by these institutions, pinpointing areas where improvement was necessary, and successful strategies that resulted in effective cybersecurity risk management.

Historical data sources included past security policies, incident reports, institutional protocols, and relevant public records.

RDT and the Cybersecurity Framework for Higher Education: The RDT and the Cybersecurity Framework for Higher Education guided the data collection and analysis processes, as outlined in the framework and methodology sections. This approach enabled the exploration of U.S. colleges' dependencies on external resources and cybersecurity measures.

Data Collection:

- **In-depth interviews**: Semi-structured interviews were conducted with U.S. college IT personnel and cybersecurity officers. These interviews aimed to gather insights into the cybersecurity strategies employed and challenges faced. Depending on participant preferences, interviews were held in person, over the phone, or via video conferencing.

- **Archival Document Analysis**: To complement the interviews, relevant archival documents, such as institutional reports, cybersecurity policies, and historical data on cybersecurity incidents, were reviewed. These documents provided an additional context and supported the analysis of the interviews.

- **Step-by-step Approach**: Participants were selected based on their roles within their institutions, and interview questions were tailored to explore their specific experiences with cybersecurity. Archival documents were sourced from college records and external reports, following a systematic review process to ensure consistency.

Data Analysis:

- **Iterative Analysis**: The data collected were analyzed iteratively, allowing themes, patterns, and theories to emerge naturally. The RDT and Cybersecurity Framework for Higher Education served as underpinning theories for this analysis.
- **Refining Interviews**: As interviews progressed, questions were refined to explore the evolving themes and patterns more deeply.

This method allowed for a more nuanced understanding of how U.S. colleges depended on various resources and frameworks for cybersecurity measures. It also aligned with the exploratory nature of this research, allowing for the emergence of unique insights into real-world experiences and practices of cybersecurity management in U.S. colleges.

These methodologies aimed to uncover an in-depth understanding of participants' experiences, opinions, and insights regarding cybersecurity risk management procedures. The study employed data collection tools and approaches to gather comprehensive and detailed information on cybersecurity risk management practices at selected U.S. colleges (Cyber Skills for All: Community Colleges Lead the Way, n.d.).

Data Collection and Sources

Data collection for this study employed a combination of primary and secondary sources to provide a comprehensive and nuanced understanding of cybersecurity risk management practices at selected U.S. colleges. The mixed-methods approach included semi-structured interviews, observations, and historical document analysis complemented by secondary data from college websites, cybersecurity reports, and related materials.

Primary Data Sources

Observations:

Observations were conducted to gain firsthand insights into how U.S. colleges manage and implement cybersecurity measures. These observations covered critical activities, such as incident handling, training sessions, and daily cybersecurity practices. The data collected from these observations helped contextualize the findings from the interviews and document analysis.

Interviews and Semi-Structured Interviews:

In-depth questionnaire interviews with critical stakeholders—administrators, IT staff, and risk management professionals—were conducted at selected U.S. colleges. These Semi-structured interviews allowed flexibility in addressing emergent themes, while focusing on core research objectives. These interviews provided rich data on decision-making processes and the real-world application of cybersecurity strategies in U.S. colleges.

Document Analysis:

Document analysis involved reviewing cybersecurity policies, strategic plans, incident reports, and other institutional documents to gain deeper insights into cybersecurity governance, practices, and challenges. These documents provided an additional layer of understanding, confirming the data gathered from the interviews and observations.

Secondary Data Sources

College Websites:

Publicly available information from the official websites of U.S. colleges was reviewed to gather data on their cybersecurity posture, services, and resources.

Cybersecurity Reports:

Reports on cybersecurity trends and practices in higher education were examined to draw comparisons and identify commonalities in the cybersecurity challenges faced by U.S. colleges.

Related Materials:

To strengthen the secondary data pool, academic papers, government publications, and institutional studies relevant to cybersecurity in higher education were included.

Observations

Observations were conducted at selected U.S. colleges to provide direct insights into the implementation of cybersecurity measures. These included live observations of incident management procedures, training sessions, and application of different cybersecurity tools and technologies.

Number of Colleges for Observation

Based on logistical constraints and stakeholder availability, three colleges were selected for observation, which included both in-person visits and virtual sessions via platforms such as Zoom.

Criteria for Selection:

- **Geographic Location:** Colleges were selected based on geographic diversity, with a mix of institutions within a reasonable distance and others accessible through virtual observations.
- **Size of Institution:** Both small and large colleges were included in the study to ensure a diverse sample.

- **Cybersecurity Incidents:** Preference was given to colleges that had recently experienced cybersecurity incidents, as this allowed for a real-world analysis of challenges and responses.

- **Availability of Stakeholders:** Institutions where key stakeholders were available for participation, whether in person or virtually, were prioritized.

Interviews

Multiple questionnaires were used to conduct interviews with key stakeholders including IT managers, cybersecurity officers, and other relevant personnel.

Member Checking:

Participants were provided with interview transcripts to review and verify the accuracy of their statements, a process known as member checking, to ensure the validity of the collected data and minimize researcher bias.

Triangulation

To ensure the reliability and validity of the study, triangulation was employed using multiple methods of data collection.

- **Document Analysis:** Institutional policies and reports were analyzed to corroborate the interview data.

- **Observations:** Firsthand observations of cybersecurity practices provide additional contextual data.

- **Secondary Data:** Data from college websites, reports, and related sources were integrated to support the primary data.

Document Analysis

Institutional documents, including cybersecurity policies, procedures, training manuals, and incident reports, were analyzed to understand colleges' approaches to managing cybersecurity risks. This document analysis added a layer of depth to the findings, enabling a more comprehensive evaluation of the strategies implemented by U.S. colleges.

Data Storage

All the collected data were securely stored using encrypted storage solutions, including password-protected folders, secure cloud services, and encrypted external drives. Only authorized personnel (the researcher) had access to the data, ensuring confidentiality and adherence to ethical research practices.

Combining primary data from interviews, observations, and document analysis with secondary data from institutional websites and cybersecurity reports, this study offers a comprehensive understanding of cybersecurity risk management practices at U.S. colleges. This data triangulation ensures a well-rounded perspective on the topic, enhancing the reliability and depth of the study.

Data Analysis

The data analysis in this study follows a holistic and integrated approach, which is consistent with the case study methodology. The primary focus was on qualitative data from observations, semi-structured interviews, and document analysis. A comparative analysis was conducted across the selected U.S. colleges to identify patterns, similarities, and differences in cybersecurity measures. This

comprehensive approach ensured that each data-collection method contributed to an in-depth understanding of the research problem. The initial guiding structures for thematic analysis were NIST CSF 2.0, and the HEISC Cybersecurity Framework for Higher Education.

Qualitative Data Analysis

NIST CSF 2.0 and the HEISC Cybersecurity Framework for Higher Education were central to structuring the data analysis process, particularly for thematic analysis and the case study methodology. These frameworks provide key domains and principles that are used as initial categories for coding and organizing raw data. For instance, themes may emerge under the NIST CSF 2.0's domains:

1. Govern
2. Identify
3. Protect
4. Detect
5. Respond
6. Recover

--or they may align with specific principles outlined in the HEISC framework, such as governance, risk management, compliance, and cybersecurity awareness, all of which are tailored to the higher education sector."

As the analysis progressed, these initial categories guided the refinement of specific themes and sub-themes. These refined themes were compared across U.S. colleges to understand the commonalities and differences in their cybersecurity measures. Questionnaire responses were uploaded to Taguette to facilitate coding and theme identification.

Inductive Coding Process

An inductive approach was employed to develop codes, tags, and themes from data. This method ensured that the analysis remained rooted in participants' perspectives and experiences. The data underwent continuous comparison and refinement as the research progressed, ensuring consistency and rigor throughout the analysis.

Historical Studies: Incorporating historical analysis allowed the study to examine the evolution of cybersecurity practices, policies, and incidents over time. These practices were contextualized using the NIST CSF 2.0 and the HEISC Cybersecurity Framework.

Addressing Bias and Preconceptions: The researcher adopted a meticulous and systematic approach to data analysis to mitigate potential biases and preconceptions. Care was taken to ensure that the analysis remained objective and produced reliable insights into the challenges and opportunities related to cybersecurity risk management in U.S. colleges. This approach also ensured the validity of this study's findings.

Data Management and Security: Data storage and management were critical for preserving the integrity of the research and ensuring the privacy of the participants. The following strategies were used to maintain the data security.

- **Secure Storage**: All data are stored on password-protected devices and encrypted cloud storage services to prevent unauthorized access, loss, or tampering. Regular backups were performed to safeguard against technical issues and data loss.

- **Access Control**: Access to data was strictly limited to the researcher, with unique login credentials ensuring security and exclusive access.

- **Data Anonymization**: PII was replaced with pseudonyms or identifiers during data analysis and reporting. This protected the identities of the participants and ensured that they could not be identified in their final publication.

- **Data Retention**: Following Institutional Review Board (IRB) requirements, all data were securely stored for five years after the study's completion. This retention period ensured that the data were available for the reanalysis or verification of the findings.

- **Data Disposal**: After the retention period, the data was securely disposed of by permanently deleting electronic files and shredding physical documents. This process protected the participants' privacy and prevented unauthorized access.

- **Regulatory Compliance**: The study adhered to local, national, and international data protection regulations, including the General Data Protection Regulation (GDPR), to preserve the privacy and rights of all participants.

Triangulation of Data

Triangulation was employed using multiple data collection methods to strengthen the credibility and validity of the study's findings. Observations, interviews, and document analysis were cross-referenced, allowing for a well-rounded understanding of cybersecurity risk management practices in the selected U.S. colleges. The triangulation process ensured the findings were robust and supported by evidence from diverse sources.

Alignment Table

An alignment table is a vital component of this study. It provided a comprehensive overview of the research design and methodology used to explore how much U.S. colleges relied on cybersecurity measures and their impact on the overall security posture. The table visually represents the alignment

between the research questions, theoretical frameworks, data sources, and data-collection instruments. In addition, the table was organized to enable readers to trace the relationship between the research questions and data collection instruments, providing a clear and concise representation of the research design. As such, the alignment table served as a crucial tool for ensuring the validity and reliability of the study, allowing assessment of the consistency and coherence of the data collection process.

Table 3.1 Presents Linking Research Questions to Data Analysis Strategies.

Research Question	Theoretical Frameworks	Conceptual Framework	Data Sources	Data Collection Instruments
RQ1: What are the best practices in the U.S. college environment for the use of security firms, third-party software, endpoints, and cybersecurity insurance?	TAM, Resource Dependency Theory	NIST CSF 2.0	Interviews with IT managers, cybersecurity officers; Documents; Observations	Semi-structured Interviews, Document Analysis, Observations
What is their influence on the overall security posture of U.S. colleges?	Coopetition Theory,	NIST CSF 2.0	Interviews with Stakeholders; Training records; Policy documents; Observations	Semi-structured Interviews, Document Analysis, Observations
RQ2: What proven and effective cybersecurity practices or strategies should U.S. colleges adopt to enhance their security posture and protection?	Coopetition Theory, Social Cognitive Theory	NIST CSF 2.0	Interviews with Stakeholders; Training records; Policy documents; Observations	Semi-structured Interviews, Document Analysis, Observations

This study employs multiple theoretical and conceptual frameworks to comprehensively understand the cybersecurity landscape within U.S. colleges.

- **NIST CSF 2.0**: This serves as an overarching conceptual framework for both the research questions. It offers a structured approach to identifying, analyzing, and mitigating risks. It provides a common language and a set of standards for evaluating the efficacy of cybersecurity practices.

- **TAM and RDT**: These theories are used in alignment with Research Question 1 to understand how and why U.S. colleges adopt certain cybersecurity practices and the resources they rely on for such adoption.

- **Coopetition Theory and Social Cognitive Theory**: These aligned with Research Question 2 to explore the strategies that U.S. colleges might adopt for a better cybersecurity posture. Coopetition Theory helps us understand how colleges collaborate and compete in shared cybersecurity. Social Cognitive Theory provides a lens for exploring how behavioral changes, possibly triggered by training and awareness programs, can influence cybersecurity.

This research aimed to produce a multifaceted understanding of the challenges and best practices associated with cybersecurity in U.S. colleges by employing these theories and frameworks. This integrative approach will also help to offer actionable recommendations based on individual and collective insights from these perspectives.

Ethical Considerations

Protecting Participants in Interviews

Several essential steps were taken to safeguard participants in this study. First, the researcher secured approval from the Kansas State University IRB before beginning any data-collection activities. Additionally, approval was obtained from any participating college that required approval in accordance with their guidelines. This study adhered to IRB guidelines for protecting human subjects and conducting research, ensuring that ethical guidelines and proper protocols were maintained throughout the exploratory process.

Second, participants were provided a thorough **Informed Consent** form, as shown in Appendix A.4. The form details the study's purpose, procedures, potential risks, and benefits. It also informed the

participants of their right to withdraw from the study without penalty. Transparency was ensured so that participants could understand their rights and make informed decisions regarding their involvement.

Third, measures were taken to ensure the confidentiality and anonymity of both the participants and colleges involved. Each participant and college were assigned a unique pseudonym to protect their identities. Pseudonyms were used when referring to the participants, and the collected data were securely stored. Aggregated results have been reported to prevent identification of individual participants. Sensitive information or personal identifiers were removed from the research documents and strict data access protocols were implemented, granting access only to the researcher.

Additionally, the researcher underwent training in ethical research practices to ensure that the responsibilities and obligations were met to protect the participants. Any unforeseen ethical concerns that arose during the research process were promptly addressed with appropriate adjustments made to maintain the highest level of ethical conduct throughout the study.

To maintain the participants' privacy and ensure the integrity of the research data, several strategies were employed for data storage and management. Data were stored on password-protected devices and encrypted cloud storage services with regular backups performed to minimize data loss risks. Data access was limited to researchers through unique login credentials. During data analysis and reporting, PII were removed or replaced with pseudonyms to ensure that participant identities were protected.

In compliance with the Kansas State University IRB requirements, the data will be securely stored for five years, allowing for potential reanalysis or verification of findings. After the retention period, the data will be securely disposed of, including permanently deleted electronic files or shredding

physical documents. This ensured the participants' privacy and prevented unauthorized access to the data.

Throughout the study, the researcher adhered to local, national, and international data protection regulations, including the GDPR (Franzke et al., 2021), to preserve the privacy and rights of all participants involved.

Limitations

Several limitations of this study have affected the transferability and applicability of the results. First, the small sample size and the specific selection of U.S. colleges limited the extent to which the findings could be generalized to broader higher education contexts, including other types of institutions, such as four-year universities, private colleges, and vocational schools.

Second, there was a potential for researcher bias in interpreting qualitative data. As the researcher was responsible for collecting, analyzing, and interpreting the data, personal beliefs, values, or expectations may have influenced the findings. To mitigate this risk, the researcher engaged in reflexivity and maintained transparency regarding their assumptions throughout the research process.

Another limitation is the reliance on self-reported participant data, which may have been subject to recall or social desirability bias. Participants might have inaccurately remembered past experiences or provided responses they believed were more socially acceptable. To address this concern, the researcher used multiple data sources and triangulation methods to corroborate the findings and to reduce the impact of these biases.

Additionally, this study's limited scope, which focused on specific research questions and variables, restricted the exploration of other potentially relevant factors that influenced the

phenomenon under study. Future research could address this limitation by expanding the range of variables or by exploring alternative research questions.

Time constraints also posed a limitation, as the study did not capture long-term trends, changes in the higher education context, or participants' experiences over time. Long-term studies or follow-up research could help to explore the persistence or evolution of the observed phenomena.

Lastly, non-response bias could have been a concern if participants who chose to participate in the study had distinct characteristics or experiences from those who did not. This bias may have affected the study findings and limited their generalizability. The researcher employed strategies to encourage participation and ensure a diverse sample to mitigate non-response bias.

By acknowledging these limitations, the study provides a more accurate representation of its scope and applicability and helps future researchers identify areas for further examination or improvement.

Study Quality

This study employs a qualitative research approach, focusing on trustworthiness by adhering to the quality criteria outlined by Lincoln and Guba (1985). These criteria include credibility, transferability, dependability, and confirmability. By carefully considering and addressing these facets of research quality, this study aims to produce robust and reliable findings.

Credibility:

This study used triangulation of data sources to gather multiple perspectives and various data types. Techniques such as member checking, where participants reviewed the findings for accuracy, and peer debriefing, involving an external examination of the research process, were conducted to verify the accuracy of the results.

Dependability:

To enhance dependability, the research design, methodology, and data collection process are described in detail. An audit trial was conducted to document all decisions and changes throughout the research process. This audit path allowed other researchers to replicate the study and verify its findings, enhancing the dependability of the study.

Transferability:

Detailed descriptions of the research context, participants, and findings were provided to allow readers to evaluate the applicability of the study to other settings. This information will provide future researchers with valuable insights to assess the relevance of these findings in their research contexts.

Confirmability:

Transparency and reflexivity were maintained throughout the data analysis and interpretation processes. This involved acknowledging the researcher's biases and assumptions, and providing clear rationales for decisions made during the analysis. These practices ensured that the study's findings reflected the participants' experiences and ideas, rather than the researcher's preferences and views.

Incorporating Methodological Recommendations.

The study incorporated best practices and criteria recommended by renowned methodology authors, such as Creswell (2014) and Yin (2018), to ensure a rigorous research design and execution. By adhering to these guidelines, the study strengthened its overall quality and impact, contributed valuable insights into cybersecurity, and supported future research.

Summary

This dissertation's third chapter outlined the methodology adopted for the exploration, emphasizing the research design, theoretical frameworks, conceptual frameworks, study context, participants, instrumentation, data gathering, data analysis and interpretation, ethical guidelines, limitations, and study quality. The research design selected for this study was rooted in qualitative methods, providing an enriched understanding of cybersecurity practices at U.S. colleges and their subsequent influence on the overall security posture.

The research was conducted across various colleges in the United States. The participants were chosen using purposive sampling techniques to ensure diverse representations. Data collection employed tools and strategies such as questionnaire-based responses, observations, and document analysis to gather in-depth information.

The collected data were analyzed using thematic analysis, which is particularly suited to qualitative data. This involved a comprehensive review of the data, coding for significant phrases or concepts, and developing themes that encapsulated participants' experiences and perspectives.

Historical studies were incorporated to provide a longitudinal perspective on cybersecurity practices and trends in U.S. colleges. This helped us to understand the evolution of these practices and their impact on security posture over time. The case study methodology guided the development of insights directly from the collected data, generating a new understanding of cybersecurity practices.

The study was deeply conscious of ethical considerations, ensuring that the rights and well-being of the participants were protected. Informed consent was obtained from all the participants, and their confidentiality and anonymity were maintained. Additionally, the study aimed to maintain

transparency regarding its objectives and methodology, and any potential conflicts of interest were carefully managed to preserve the integrity of the research.

Chapter 4 - Findings

In this chapter, the researcher analyzed the qualitative data collected from three educational institutions—two community colleges (Institution A and Institution B) and one University College (Institution C)—regarding their cybersecurity practices. Data were gathered through interview questionnaires completed by key personnel at each institution. Specifically, three interviews were completed at Institution A, two at Institution B, and two at Institution C, totaling eight interview responses. The participants held roles as IT Directors, Cybersecurity Officers, Database Directors, and Network Managers, each offering valuable insights into their institution's cybersecurity landscape.

Following the interviews, the data were systematically coded using thematic tags that represented the essential aspects of cybersecurity measures, challenges, and areas of improvement. This methodology involves qualitative content analysis and categorizing responses to these tags to identify prevalent themes and patterns. This approach highlights the strengths and vulnerabilities of higher education cybersecurity practices and sheds light on the effectiveness of current measures and the urgency of policy adaptations. Analysis is crucial for understanding how U.S. colleges can enhance their defenses against increasingly sophisticated cyber threats.

Theoretical Frameworks

This study is grounded in NIST CSF 2.0, which provides a structured approach to managing cybersecurity risks. NIST CSF 2.0, which offers a systematic lens through which the best practices, challenges, and effectiveness of various cybersecurity measures are evaluated across the institutions studied. It emphasizes Six Core Functions—Govern, Identify, Protect, Detect, Respond, and Recover—that guide the thematic analysis of the data, ensuring a comprehensive understanding of how cybersecurity risks are managed in educational settings.

Participant Demographics

The study included participants from three educational institutions: A, B, and C. Participants were selected because of their involvement in cybersecurity management and decision-making at their institutions, ensuring that their insights were relevant to the research questions.

The participants were all male, primarily identifying as white, except for Participant 3 (Institution A), the Manager of Networks (Hispanic), and Participant 4 (Institution A), the Director of Systems Management (Asian). Participant 3 was the youngest and Participant 5 was the oldest. All participants held at least a bachelor's degree, with two participants —Participant 1 (Institution C) and Participant 4 (Institution A)—holding master's degrees.

In terms of professional roles, participants included chief information security officers, IT security officers, and other cybersecurity staff, providing diverse insights into their institutions' cybersecurity practices. These participants represented both strategic and operational levels, enriching the data with detailed accounts of the cybersecurity management challenges faced by their institutions. Considering their roles and backgrounds, this study provides a comprehensive understanding of the cybersecurity landscape across different institutions.

Gathering and Analyzing Data

Data were systematically gathered via semi-structured interviews conducted in two rounds: initial interviews and follow-up questionnaires distributed to key personnel at the three educational institutions. These participants provided eclectic insights into the cybersecurity practices of their institutions.

Data Collection Process

- **Initial Questionnaire Design:** The initial questionnaire included a mix of open-ended and structured questions, allowing participants to provide detailed feedback on various aspects of cybersecurity such as best practices, challenges, and strategic improvements. This format facilitated the collection of comprehensive data tailored to the research questions.

- **Participant Selection:** Participants were selected based on their roles in cybersecurity management and decision-making. This selection process ensured that the gathered data were relevant and insightful to the study's focus on cybersecurity practices within institutions.

- **Interviews:** Data were collected through a multi-stage process that began with an initial questionnaire. The questionnaire was distributed to key personnel at three educational institutions to gather preliminary insights into their cybersecurity practices. Based on their responses, participants were selected for follow-up interviews to explore the key themes in more detail. After the interviews, a final questionnaire was administered to clarify the findings. This approach ensures comprehensive understanding of the challenges and strategies employed by institutions.

While the researcher gathered the data through questionnaires and interviews, the findings will be discussed in detail in subsequent sections, including visual representations of key insights (see Section 4.10c for detailed visual presentations).

Follow-Up Questionnaire:

- **Purpose:** A follow-up questionnaire was conducted to elaborate on the initial responses and explore whether participants would answer analogous questions differently. This follow-up helped to verify the consistency of the responses and provided an additional context where needed.

- The follow-up was distributed electronically, allowing participants flexibility to clarify or expand on their initial answers.

Data Analysis Process:

- **Questionnaire Process**: The questionnaire allowed the participants to provide detailed responses on their cybersecurity practices, challenges, and strategies. This approach enabled a deep dive into specific topics, while allowing participants to express their insights in their own words. The initial and follow-up rounds of the questionnaire were designed to explore the core areas of cybersecurity management in educational institutions.

- **Initial Coding**: Responses from the initial and follow-up questionnaires were uploaded to qualitative analysis software (e.g., Taguette) for systematic coding. Each answer was meticulously examined to identify recurring themes, concepts, and patterns relevant to the research question.

- **Thematic Development**: Codes from both rounds of data collection were grouped into broader themes that reflected critical aspects of cybersecurity within educational settings. This process ensured that the themes were firmly grounded in the participants' responses and were not influenced by researcher bias.

- **Ensuring Consistency**: An iterative approach was used to refine the themes, ensuring consistent application across all responses from both questionnaires. Code cross-referencing was used to validate the findings and provide a robust analysis.

Ensuring Consistency: The research used an iterative approach to refine the themes, ensuring their consistent application across responses from both questionnaires. Cross-referencing of the codes helped validate the findings and provided a more robust analysis.

Using NIST CSF 2.0 Framework

This section combines the data analysis process and key findings from participant interviews. Through qualitative content analysis using predefined thematic tags in Taguette (Rampin & Rampin, n.d.), the study identified several recurring themes related to cybersecurity practices, challenges, and strategies in U.S. colleges.

Data Analysis Process

The data were processed using qualitative analysis software, which helped categorize answers based on recurring themes, reflecting participants' insights into cybersecurity management in educational settings. Thematic tags were consistently applied across all answers to ensure reliability, and these patterns were explored for commonalities and variances among institutions. The analysis helped to identify key challenges, successes, and future directions for cybersecurity in higher education.

- To organize the data analysis and key findings from participant interviews, the researcher used the Six Core Functions of the NIST CSF 2.0: Govern, Identify, Protect, Detect, Respond, and Recover. By aligning these findings with this structure, this study clarifies how institutions manage their cybersecurity practices within this framework.

Govern

The Govern function emphasizes strategic oversight, policy development, and compliance, which are all crucial for building a structured cybersecurity approach. Several interviewees discussed the importance of strong leadership and clear cybersecurity policies for maintaining institutional security.

For example, Interviewee 8 noted, “Our strategy has improved under new leadership, with a clear focus on prevention and regular security assessments. However, we are still working to address the deficiencies left by past leadership” (Interviewee 8, personal communication, 2024). This reflects the role of governance in shaping cybersecurity practices and ensuring continuous improvement.

Interviewee 5 highlighted the significance of aligning cybersecurity measures with institutional goals: “I oversee the strategic direction of cybersecurity measures, ensuring alignment with institutional goals” (Interviewee 5, personal communication, 2024). This illustrates the governance process in which aligning cybersecurity efforts with institutional priorities fosters a proactive security culture.

Additionally, Interviewee 6 emphasized the value of well-defined policies and compliance: “My role involves overseeing cybersecurity policies, managing the IT team, and ensuring compliance with security standards” (Interviewee 6, personal communication, 2024). This approach ensures that an institution’s security practices are consistently applied and monitored, embodying the core aspects of governance.

Identify

The Identify function focuses on understanding the risks to systems, assets, data, and capabilities. This ensures that institutions can prioritize their efforts based on the identification of vulnerabilities and potential threats. A notable example of this can be seen in the 2020 ransomware attack on Institution A, where outdated technology was a key vulnerability. The institution ran obsolete servers, including systems based on Windows 2008, which had been flagged for replacement years before but were still in use at the time of the attack. This failure to identify and address outdated technology directly led to a ransomware incident that cost the college over $1.1 million (Stahl, 2023). This case illustrates the critical need for institutions to prioritize vulnerability assessments as part of the identify function, ensuring that outdated systems are regularly audited and updated. Participant 5 noted, “Overcoming the legacy of poor decisions and outdated practices from previous leadership has been challenging, compounded by budget limitations.”

Training and Awareness Programs

- Participants stressed the importance of cybersecurity training as a key method for identifying risks. Training enhances awareness and empowers staff to recognize potential vulnerabilities before incidents occur. Participant 1 (Institution A) stated, "We're focusing a lot on training everyone better so that all staff understand how important security is" (Participant 1, personal communication, 2024). This proactive approach aligns with the Identify function, as it equips institutions to pinpoint weaknesses early on.

Compliance and Regulatory Challenges

- Regulatory compliance has emerged as a challenge in identifying vulnerabilities in the legal and privacy requirements. Institutions must stay updated on evolving regulations such as FERPA, HIPAA, and state-specific mandates such as the CCPA. Participant 4 (Institution C) noted, "We're constantly behind because new standards come up faster than we can adjust. Without proper support from administration, it's impossible to keep up" (Participant 4, personal communication, 2024). Participant 3 (Institution A) echoed this concern, stating, “It feels like we're playing catch-up all the time, especially with the new state-specific regulations coming out of nowhere" (Participant 3, personal communication, 2024). These consistent concerns demonstrate how compliance issues can hinder an institution’s ability to effectively identify and address risks.

- Cybersecurity training should not only focus on immediate threats, but also consider long-term education strategies, such as incorporating CTE programs that prepare students for careers in cybersecurity. By integrating cybersecurity into CTE programs, institutions can help build a skilled workforce to address growing cyber risks.

Challenges with Static Cybersecurity Models

- Several participants emphasized that relying on static security measures, such as firewalls and antivirus software, is insufficient in today’s rapidly evolving cyber threat landscape. Participant 3 (Institution B) remarked, “Our firewalls and antivirus tools are effective to a point, but they cannot keep up with the sophisticated attacks we are seeing now. We need more adaptive solutions that learn and evolve with the threats” (Participant 3, personal communication, 2024).

- This sentiment was echoed by Participant 4 (Institution C), who explained that "Cybersecurity is no longer a 'set it and forget it' field. You can't install a firewall and think you have recovered for the next year. Threats change daily, and we need systems that can evolve just as fast" (Participant 4, personal communication, 2024).

- The participants discussed the need to move beyond traditional static security models in favor of more adaptive solutions. For example, Participant 3 (Institution A) highlighted the evolving nature of cyber threats, stating, "Our cybersecurity landscape is constantly changing. We cannot just rely on the tools we put in place last year; they need to evolve as the threats evolve" (Participant 3, personal communication, 2024).

- Similarly, Participant 6 (Institution B) emphasized the importance of continuous improvement: "We need more than just firewalls and antivirus software; we need systems that can learn and adjust. Our approach has to be dynamic because what worked last year will not work this year" (Participant 6, personal communication, 2024).

- These insights align with the need for institutions to adopt continuous improvement models such as the NIST Cybersecurity Framework, which encourages ongoing updates and proactive security measures.

Protect

The Protect function refers to the implementation of safeguards to ensure the continued delivery of critical infrastructure services. The participants highlighted several protective measures in place at their institutions. After a significant data breach in 2010, Institution B strengthened its cybersecurity measures, implementing robust encryption protocols and increasing the frequency of security updates. This breach affected many individuals and forced the institution to adopt more

stringent protective measures to safeguard sensitive information. This aligns with the NIST Protect function by highlighting how proactive strategies can prevent future cyberthreats.

Several participants noted that their institutions have integrated or outsourced Security Operations Center (SOC) services to enhance their cybersecurity posture. Participant 2 (Institution A) mentioned, "We rely heavily on an outsourced SOC to provide 24/7 monitoring because we simply don't have the internal resources to handle that level of vigilance" (Participant 2, personal communication, 2024). Similarly, Participant 5 (Institution C) emphasized, "Our SOC is managed externally, and it's been crucial in responding to incidents in real-time" (Participant 5, personal communication, 2024).

For instance, Institution C relies on an external SOC provider to manage security incidents.

"We have a third-party MSSP that handles our SOC services, and they are engaged in actively protecting our data while the attack is happening" (Participant 7, personal communication, 2024).

Additionally, Institution B adopted a similar approach to enhance its round-the-clock protection:

"Our institution's MSSP manages SOC operations, providing 24/7 monitoring and threat intelligence, which is something our internal team could not match alone”’ (Participant 5, personal communication, 2024).

Effectiveness of Cybersecurity Measures

Participants frequently emphasized the critical role of continuous improvement and updates in protecting their systems. Participant 2 (Institution A) stated, “Our investment in training and upgrading our security systems has been crucial in enhancing our defenses” (Participant 2, personal communication, 2024). Similarly, Participant 5 (Institution B) mentioned, "Without regular updates and continuous investment in new technologies, our systems would quickly become obsolete" (Participant 5,

personal communication, 2024). This shows how proactive protection measures can help prevent security breaches.

The participants stressed the importance of using proactive systems to identify vulnerabilities before escalating. Standard practices included Intrusion Detection and Prevention Systems (IDPS), as emphasized by Participant 4 (Institution C), who stated, "Our IDPS has caught several attempted breaches before they could cause harm. This real-time monitoring has been essential for us' (Participant 4, personal communication, 2024). The IDPS highlights the importance of real-time monitoring and continuous surveillance as best practices in the identification stage, ensuring that institutions can detect threats before they escalate.

Layered security refers to the use of multiple independent layers of defense to protect an organization's digital assets from various cyber threats. Rather than relying on a single security measure, a layered approach ensures that, if one layer is compromised, additional layers continue to protect the institution. This multilayered strategy aligns with the NIST Cybersecurity Framework, which outlines five key steps for improving security posture: Govern, Identify, Protect, Detect, Respond, and Recover. Participant 3 (Institution A) emphasized the importance of a layered security approach, stating, "we have had to adopt multiple layers of security, including firewalls, multi-factor authentication, and constant monitoring because relying on just one defense is not enough anymore" (Participant 3, personal communication, 2024). Similarly, Participant 5 (Institution B) noted, "Our layered security model gives us more flexibility and protection, allowing us to respond faster to different types of threats" (Participant 5, personal communication, 2024). This highlights how institutions utilize a layered approach to mitigate risks at various levels, ensuring that, if one control fails, others are in place to protect the system. Protect: Firewalls, encryption, endpoint protection, and multi-factor authentication (MFA) are implemented to secure the perimeter and internal systems. This layer also includes comprehensive employee training on security protocols, ensuring that staff understand how to

recognize and respond to potential threats. Detect: Utilizing SOC services or advanced detection systems such as SIEM platforms to continuously monitor suspicious activities. These systems can identify abnormal behavior in real time, allowing swift threat identification. Respond: Create a clear incident response plan so that, in the event of a breach, the institution can quickly isolate affected systems, mitigate damage, and notify key stakeholders. The SOC team (whether in-house or outsourced) plays a critical role by providing real-time threat intelligence and coordinating responses. Recover: Ensuring that the institution can quickly restore any services impacted by a cyberattack, including robust backup systems that allow for rapid recovery of compromised data.

Additionally, the institution must analyze the incident to learn from the breach and improve future defenses. In this layered approach, each security measure reinforces the other measures. For example, although employee training helps reduce the chances of a phishing attack succeeding, endpoint protection and SOC monitoring provide additional safeguards if an employee accidentally clicks on a malicious link. By implementing these interconnected layers, the institution ensures a more resilient cybersecurity posture that can withstand various threats better. Furthermore, Institutions are becoming increasingly aware of the need to protect against DDoS attacks, which can overwhelm college networks and render essential services inaccessible. Effective mitigation strategies such as traffic filtering and load balancing can minimize the impact of DDoS attacks on institutional operations.

Security Concerns That Affect Protection

Participants with dependents expressed heightened concerns about data privacy and the safety of personal information, mainly because they manage both home and work responsibilities. These concerns have driven a stronger focus on implementing robust protective measures in their institutions. Participant 3 (Institution A) stated, “With kids at home using devices for schoolwork, I am even more

aware of the risks and the need for robust cybersecurity measures at home and work" (Participant 3, personal communication, 2024).

These personal responsibilities emphasize the need for more robust data-protection strategies, reinforcing the importance of cybersecurity policies and safeguards that protect both institutional and personal data. For instance, *immutable backups* have emerged as a critical safeguard, ensuring that sensitive information remains protected from unauthorized alterations or deletions, even in the event of ransomware attacks. By implementing such measures, institutions can enhance data integrity and compliance with regulations like FERPA and HIPAA, which require stringent student and health data protection. Dependent participants are likely to advocate for stronger cybersecurity measures, recognizing that data protection vulnerabilities can affect their professional and personal environments.

Compliance and Regulatory Challenges

Institutions face ongoing challenges in complying with evolving cybersecurity regulations, which are essential for safeguarding sensitive data. Participant 4 (Institution C) stated, "We're constantly behind because new standards come up faster than we can adjust. Without proper support from administration, it's impossible to keep up" (Participant 4, personal communication, 2024).

- Compliance with data protection regulations, such as FERPA and HIPAA, and state-specific mandates, such as the CCPA, require institutions to implement robust protective measures. These regulations mandate the safeguarding of sensitive students and health data, thereby adding significant complexity to cybersecurity strategies. For example, maintaining compliance while managing resource limitations can make it difficult to fully protect the data.

- Data Protection Regulations: Ensuring compliance with laws such as FERPA and HIPAA while maintaining strong cybersecurity practices remains a challenging balancing act, especially given resource demands. Participant 3 (Institution B) mentioned, "Ensuring compliance with FERPA while also

maintaining robust cybersecurity practices is difficult because both demand significant resources" (Participant 3, personal communication, 2024).

- **State-Specific Mandates**: Institutions in California, for example, must comply with the CCPA, which adds additional layers of regulatory obligation to their cybersecurity operations. Participant 2 (Institution A) stated, "The CCPA has added a whole new layer of complexity to our compliance efforts, and we are constantly trying to ensure we meet both federal and state requirements" (Participant 2, personal communication, 2024).

Implementation of Third-Party Security Solutions

- Several institutions rely heavily on Managed Security Service Providers (MSSPs) to enhance their security capabilities and provide continuous protection through proactive monitoring. Participant 5 (Institution C) stated, "Our partnerships provide us with expertise and round-the-clock monitoring that our in-house team cannot match" (Participant 5, personal communication, 2024). While these third-party partnerships strengthen defenses, participants acknowledged the need to balance external services with internal security capacity to avoid overreliance on third parties.

Influence of Personal Responsibilities on Cybersecurity Practices

- Participants with dependents expressed concerns about the potential risks posed by their responsibilities, particularly regarding the possibility of dependents inadvertently accessing institutional systems or opening malicious email or websites. Participant 3 (Institution A) mentioned, "With kids at home using devices for schoolwork, I'm even more aware of the risks and the need for robust cybersecurity measures at home and work" (Participant 3, personal communication, 2024). This highlights the need for increased cybersecurity vigilance to protect both individual and institutional data.

- Allowing family members to use devices connected to institutional networks introduces additional risks, underscoring the need for clear policies to address these potential vulnerabilities. The risks posed by dependents using these systems can lead to the introduction of malware or unauthorized access to sensitive information. Institutions should consider developing policies that account for this reality and implement best practices to minimize these risks, such as restricting access to certain systems or enhancing employee awareness of secure home network practices.

- **Policy Implications**: Interviewees agreed that best practices in cybersecurity include developing policies that recognize the blurred lines between personal and institutional device usage, particularly for employees with dependence. These best practices involve training employees in securing remote access, setting up firewalls, and using separate devices to mitigate the risks associated with both personal and professional use.

Resource Limitations and Funding Challenges

- A common theme across participants was the impact of budget constraints on their ability to identify potential threats and implement adequate cybersecurity measures. Smaller institutions such as Institution B face challenges in maintaining updated protection tools and employing sufficient staff. Participant 2 (Institution B) shared, "We struggle with balancing our budget constraints while trying to implement robust security measures" (Participant 2, personal communication, 2024).

- These financial challenges limit the capacity of institutions to invest in advanced cybersecurity solutions, such as IDPS, firewalls, and continuous security monitoring. Participant 5 (Institution A) mentioned, "Our budget is stretched thin, and without adequate funding, it's impossible to invest in the latest technologies or hire more personnel" (Participant 5, personal communication, 2024).

- Consequently, many institutions rely heavily on cost-effective third-party solutions or open-source tools to mitigate the risks they cannot afford to address directly. However, this reliance also introduces risks, as noted by Participant 7 (Institution B), who emphasized, "The budget limitations mean we're often forced to choose between upgrading software or training staff, both of which are essential for protecting our systems" (Participant 7, personal communication, 2024).

Detect

The Detect function focuses on identifying cybersecurity events in a timely manner. Participants frequently mentioned AI-driven detection tools as critical components of their cybersecurity infrastructure.

AI Tools for Detection

- The use of AI to detect threats was a recurring theme in these interviews. Participant 1 (Institution C) emphasized the shift from a reactive to a proactive stance: "AI has shifted our security posture from reactive to proactive, allowing us to anticipate threats before they fully develop' (Participant 1, personal communication, 2024). However, the dual-edge nature of AI has also been mentioned. As Participant 7 (Institution B) noted, "AI is a powerful tool, but it is a double-edged sword. Just as it helps us protect our systems, attackers can use it to create more sophisticated threats" (Participant 7, personal communication, 2024).

Technological Integration and AI Influence

- The integration of AI-driven technologies has been transformative in protecting institutions from cyber-attack. Participant 1 (Institution C) explained, "AI has shifted our security posture from reactive to proactive, allowing us to anticipate threats before they fully develop"

(Participant 1, personal communication, 2024). AI tools, CrowdStrike Falcon Complete (EDR) and Wazuh (XDR and SIEM) can play a critical role in enhancing the ability of institutions to detect and mitigate threats.

- Advanced Persistent Threats (APTs) pose a significant risk to institutions by utilizing sophisticated tactics to gain unauthorized, long-term network access. Participant 2 (Institution A) shared, “We've faced threats that don't just go away after a firewall block. These attackers find ways to stay in our network, and if we're not constantly monitoring, they can do real damage over time” (Participant 2, personal communication, 2024). Identifying APTs requires constant monitoring and advanced detection systems that can track and neutralize persistent cyber-adversaries before considerable damage occurs.

Respond

The Respond function theme deals with taking appropriate action once a cybersecurity event is detected to contain its impact. The participants discussed their reliance on incident and third-party services to respond to cyber incidents. In 2020, Institution C faced a ransomware attack that took critical systems offline for an extended period (Dissent, 2020). The delayed response was a direct result of insufficient incident response planning, which prolonged the institution’s downtime and complicated the recovery efforts. This highlights the need for institutions to have a well-prepared and tested incident response plan that is capable of quickly and effectively mitigating the impact of cyber incidents.

In the aftermath of the 2010 breach, Institution B responded by notifying affected individuals and offering them 12 months of free credit protection services. This response highlighted the importance of having a well-structured incident response plan that includes clear communication with those affected and steps to mitigate further risks such as identity theft (Twingate, n.d.). However,

Participant 2 (Institution B) noted, "The delay in notifying the public was a major lesson for us. We realized that quicker, more transparent communication is essential in maintaining trust" (Participant 2, personal communication, 2024). The two-month delay in public notification highlights the need for quicker and more transparent response procedures to prevent further reputational damage and ensure timely action.

Implementation of Third-Party Security Solutions

- Institutions with well-defined incident response strategies could reduce fallout from incidents, downtime, and the risk of further compromise. These plans include detailed protocols for communication, containment, and recovery. For example, Participant 6 (Institution A) mentioned, "We hold periodic drills to ensure everyone is aware of their roles during an incident, which helps us maintain an organized response" (Participant 6, personal communication, 2024).

- Several institutions have partnered with Managed Security Service Providers (MSSPs) to bolster their incident response capabilities. Participant 5 (Institution C) shared, "We have partnered with an MSSP to help monitor our network round-the-clock, providing us with threat intelligence and automated response capabilities, including real-time alerts, vulnerability assessments, and rapid containment of threats" (Participant 5, personal communication, 2024). These enhancements have enabled institutions to respond to threats more efficiently, reduce response times, and improve overall threat detection. While third-party services enhance an institution's security posture, they also require continuous oversight to ensure alignment with institutional policies and update as threats evolve.

Incident Response Plans

- A clear, structured incident response plan was reported to be vital for minimizing the damage from cybersecurity events. Participant 3 (Institution C) noted, “Our incident response plan allows us to respond quickly to minimize the damage from any breach” (Participant 3, personal communication, 2024). Incident response plans commonly include several key components, such as clear communication protocols, predefined roles and responsibilities for the response team, procedures for containing and mitigating threats, and steps for recovery and post-incident analysis. For example, Participant 3 also mentioned that their plan included an “immediate lockdown procedure for compromised systems, notifications to all critical departments, and a predefined escalation path to ensure timely involvement of senior management.”

- These plans should also emphasize regular testing and updates to ensure that they remain effective as the threats evolve. Institutions with mature incident-response strategies often conduct tabletop exercises or simulated attacks to refine their processes. Appendix A provides a sample response plan (based on the COD plan) that outlines the key steps and protocols for effective incident management while redacting sensitive institutional identifiers.

Recover

The Recover function ensures resilience and restores any capabilities or services impaired during a cybersecurity incident. Resource limitations are frequently highlighted as a challenge in this area. During the 2020 ransomware attack, Institution A relied heavily on cybersecurity insurance to cover the financial costs of the breach. However, delays in receiving support from the insurance provider hinder

the speed of the recovery process, extending the downtime of the institution (Stahl, 2023). As Participant 5 (Institution A) stated, “We waited weeks for the insurance claim to go through, which really set us back in terms of recovery time” (Participant 5, personal communication, 2024).

Similarly, Institution B's dependency on external services delayed recovery efforts following a phishing attack. Participant 3 (Institution B) noted, ‘”We were stuck waiting on third-party providers to assist with the system restoration, which left us unable to operate fully for days” (Participant 3, personal communication, 2024).

The Federal Terrorism Risk Insurance Program (TRIP) serves as an additional layer of financial protection for institutions facing cybersecurity risks that may fall within the broader scope of terrorism. While primarily aimed at traditional terrorism-related incidents, TRIP highlights the potential of insurance solutions to mitigate the fiscal impact of large-scale cyberattacks. "Our cybersecurity insurance has helped cover the costs of breaches, but it is important to consider additional protection for more extreme scenarios such as large-scale attacks or incidents that could fall under terrorism” (Participant 7, personal communication, 2024). The quote from Participant 7 highlights the importance of programs such as TRIP, which serves as an extra layer of financial protection for institutions facing cybersecurity risks that could fall under the broader scope of terrorism.

Following their breach, Institution B implemented an Information Security Incident Response Management Policy to streamline future incident reporting, investigation, and notification processes. The policy also includes a review of existing security protocols, leading to improvements in the university's overall cybersecurity posture (Twingate, n.d.). This breach demonstrates the importance of a strong recovery strategy, including both technical recovery (e.g., restoring compromised systems) and policy-driven recovery, ensuring that institutions are better prepared for future incidents.

Resource Limitations and Funding Challenges

- Smaller institutions, particularly Institution B, faced significant challenges in recovering from cybersecurity incidents due to limited resources. Participant 2 (Institution B) stated, “We struggle with balancing our budget constraints while trying to implement robust security measures” (Participant 2, personal communication, 2024). These resource limitations slowed recovery efforts, making it difficult for institutions to quickly return to normal operations after an attack.

Cybersecurity Insurance

- Cybersecurity insurance was another factor in the recovery process, although participants noted delays in receiving support during the incidents. Participant 6 (Institution B) mentioned, “While insurance helps, the delays in getting support during an incident can be a major hindrance” (Participant 6, personal communication, 2024). This finding highlights the need for more efficient recovery strategies to complement insurance coverage.

- The findings reveal the benefits and limitations of relying on Cybersecurity Insurance: The recovery phase of a cyber incident. While insurance can provide critical financial support, it often fails to ensure a prompt and adequate recovery. Participant 3 (Institution B) commented, "I firmly oppose relying on cyber insurance as it often encourages the payment of ransoms, which only perpetuates the problem. Instead, colleges should develop their own comprehensive response plans and establish partnerships with vendors supplying security and networking equipment” (Participant 3, personal communication, 2024).

Participant 2 (Institution A) expressed similar concerns: "Insurance can only get you so far. You need to have your own systems in place that can act quickly; otherwise, you're just

waiting for funds while the attack keeps costing you" (Participant 2, personal communication, 2024).

These comments underscore the importance of not relying overly on insurance as a primary risk-management tool. Policy recommendations should include reassessing the role of cybersecurity insurance in U.S. colleges and promoting policies that encourage robust internal defenses alongside insurance as part of a broader cybersecurity strategy.

4.4b Overview of Key Themes

Based on the data collected from interviews and questionnaires, four key themes emerged, representing the core challenges and strategies within U.S. college cybersecurity practices.

1. **Cybersecurity Readiness Disparity**: The uneven application of cybersecurity best practices, such as ongoing staff training, technology updates, and policy enforcement, creates a significant readiness gap across institutions. This disparity leaves many U.S. colleges vulnerable to advanced threats, especially those driven by artificial intelligence (AI). Larger institutions often have more resources to apply best practices consistently, while smaller colleges struggle to keep up because of budget constraints and limited cybersecurity expertise. Consequently, institutions are unevenly prepared to defend against evolving threats, highlighting the need for standardized readiness protocols across the sector.

2. **Role of External Support**: Many institutions, especially those with fewer internal resources, rely heavily on external cybersecurity services such as Managed Security Service Providers (MSSPs). While outsourcing certain security functions can offer immediate access to expertise and advanced tools, over-reliance without proper integration into an institution’s internal security framework can introduce additional risks. These partnerships need continuous oversight to

ensure that third-party vendors align with institutional policies and effectively address the unique security challenges faced by U.S. colleges. Evaluating the strengths and limitations of these partnerships is critical for institutions to maintain control over their cybersecurity posture.

3. **Adoption of Cybersecurity Technologies**: The integration of AI-driven security technologies offers substantial opportunities to improve threat detection and response times. However, institutions face significant barriers in the adoption of these technologies. Policy inadequacies, a lack of institutional readiness, and limited technical expertise often prevent colleges from fully leveraging AI and other advanced technologies. Smaller colleges, in particular, struggle with the high cost and complexity of implementing these tools. This gap underscores the importance of creating accessible and scalable solutions that can be adapted to meet the needs of diverse institutions, regardless of their size or financial resources.

4. **Impact on Institutional Trust**: Trust is a critical component in maintaining stakeholder confidence in an institution's cybersecurity capabilities. Effective management of cybersecurity risks, through transparent strategies, comprehensive insurance coverage, and clear communication, reinforces this trust. Failures in these areas not only compromise institutional security, but also erode confidence among students, staff, and external partners. The study revealed that institutions without robust cybersecurity policies often face reputational damage after a security breach, highlighting the need for proactive strategies to reinforce trust through transparent and well-communicated cybersecurity practices.

Summary of Theme Analysis

The data analysis process was intricately linked with the theoretical frameworks to ensure that each piece of data was categorized and evaluated in terms of its relevance to proven cybersecurity frameworks. This involved a detailed comparison of how different cybersecurity strategies were

perceived in terms of effectiveness and efficiency, thereby providing insights into the practical application of theoretical models in real-world settings.

Summary of the Findings

The key findings of this study indicate that, while there is a robust theoretical framework for handling cybersecurity issues, practical gaps in training, compliance, and resource allocation significantly affect the overall effectiveness of cybersecurity measures. These conclusions were drawn from an in-depth analysis of qualitative data collected through interviews with key personnel at U.S. colleges and a university.

What Led to the Conclusions:

1. **Interview Data:** The interview data revealed specific institution-level challenges that significantly shaped their cybersecurity strategies. For example, Participant 2 (Institution A) emphasized the difficulty of balancing budget limitations with the need for updated security tools: "We know what we need, but it's hard to justify the expense when we have competing priorities" (Participant 2, personal communication, 2024). Similarly, Participant 4 (Institution C) pointed out the challenge of securing buy-in from upper management for more comprehensive cybersecurity initiatives: "Without clear leadership support, it's nearly impossible to implement any meaningful changes" (Participant 4, personal communication, 2024).

2. **Recurring Themes:** During the institution data-gathering process, several themes emerged consistently across the interviews, such as the inadequacy of training programs and the challenges in fully complying with cybersecurity protocols. These themes were particularly clear in institutions with limited resources, where staff often needed help to keep up

with the latest cybersecurity threats due to insufficient training and lack of ongoing professional development.

3. **Analysis of Institutional Variances:** The study also examined how differences in institutional priorities and resource allocation contributed to the effectiveness of cybersecurity measures. For example, colleges with more substantial budgets could afford advanced cybersecurity tools and dedicated staff, whereas those with fewer resources had to rely more on basic measures and external support, leading to gaps in security.

4. **Practical Observations:** Beyond theoretical frameworks, the practical experiences shared by participants revealed a gap between theory and practice. Even when robust policies were in place, the lack of practical training and resource allocation often led to the insufficient implementation of these policies. This finding underscores the need for institutions to develop solid theoretical frameworks and ensure that they have a practical means of enforcing and sustaining them.

These insights, drawn from the direct experiences of those responsible for cybersecurity in educational settings, highlight critical areas where improvements are necessary. Addressing these gaps requires a focus on enhancing training, ensuring compliance, and optimizing resource allocation to build more resilient cybersecurity strategies.

Presentation of Data and Findings

1. **Resource Allocation**: Participants from all institutions highlighted disparities in available resources, which affected their ability to implement comprehensive cybersecurity strategies. Previous research aligns with this observation, suggesting that institutions with fewer resources face significant challenges in maintaining effective and updated security measures.

2. **Third-Party Solutions**: The reliance on third-party audits and security solutions has emerged as a recurring theme. For example, Participant 6 (Institution B) mentioned, "Our reliance on third-party security audits has significantly enhanced our threat detection capabilities," indicating the importance of external partnerships in mitigating institutional vulnerabilities.

3. **Compliance Challenges**: Another prominent theme was keeping up with the evolving regulatory requirements. Participants highlighted that, while compliance is necessary, maintaining pace with changing standards often requires additional administrative support. Participant 4 (Institution C) noted, "Without proper support from administration, it's impossible to keep up," emphasizing the critical role of institutional support.

By reinforcing these themes through direct participant insights, this study adds to the ongoing conversation on the challenges and opportunities in cybersecurity management for higher education institutions.

Participants with Dependents

From the interviews, it became clear that many participants expressed concerns about the potential security risks posed by dependents using institutional technological equipment at home. While these risks certainly relate to protection measures, the focus here is on how participants' personal responsibilities, such as caring for dependents, influence their overall perceptions and practices regarding cybersecurity. The participants frequently mentioned how these responsibilities could complicate or shape their approaches to securing their work environments, especially when the personal and professional use of devices overlapped.

Impact on Behavior:

This heightened concern translates into more cautious online behaviors, both at home and in the workplace, influencing the perception and adherence of cybersecurity policies. Participant 7 (Institution B) noted, 'I find myself being much more vigilant not only in enforcing cybersecurity protocols at work but also at home, where my kids are constantly online for school and social activities' (Participant 7, personal communication, 2024). Blending personal and professional vigilance underscores the broader impact of dependence on cybersecurity practices.

Since the attack, staff have shown heightened vigilance in their daily activities, particularly in cybersecurity. One participant explained, "Our staff are now hyper-aware of phishing and suspicious activities. There is a heightened sense of caution after the attack, and it changes how we approach everyday tasks, not just in IT, but across the board. It feels like cybersecurity is everyone's responsibility now" (Participant 1, personal communication, 2024)

The 2020 ransomware event drastically shifted the institution's approach to cybersecurity. As one participant described, "Before the breach, most people didn't take cybersecurity training seriously. Now, it is mandatory, and everyone is on alert. We are constantly thinking about what could go wrong" (Participant 6, personal communication, 2024).

Policy Advocacy:

Dependent participants are often more vocal in advocating comprehensive cybersecurity policies, reflecting their broader concerns about family and community safety. Participant 1 (Institution C) shared, "Having dependents changes your perspective on what is essential in cybersecurity. I push harder for policies protecting institutional and personal data because I know the risks extend beyond the workplace" (Participant 1, personal communication, 2024).

Summary:

These insights suggest that personal responsibilities significantly influence how professionals perceive and practice cybersecurity. The heightened awareness and proactive behavior driven by dependents highlights the importance of considering personal contexts when developing and implementing cybersecurity policies).

Participants Without Dependents

Conversely, participants without dependents often have different perspectives and concerns about cybersecurity, which is characterized by distinct focus areas and engagement patterns.

Focus Areas:

- Participants without dependents tended to focus more on personal data security and the immediate impact of cybersecurity breaches on their professional responsibilities rather than on broader family oriented concerns. This focus on personal and professional spheres shapes how they prioritize cybersecurity issues.

Engagement in Cybersecurity Practices

- These participants may engage differently in cybersecurity training and protocols, often showing less personal concern but maintaining professional diligence. Their approach is often characterized by adherence to required practices without the added layer of personal vigilance seen in participants with dependents.

Advocacy and Policy Engagement

- Participants without dependents might prioritize efficiency and usability in cybersecurity measures over stringent controls, which they may perceive as impeding the workflow or personal convenience. This perspective highlights the potential preference for a balance between security and operational ease.

These analyses used comprehensive collected data and thematic tags applied during the study to draw contrasts and parallels between different demographic groups within the participant pool. For example, Participant 3 (Institution A) shared, "Having dependents makes me more cautious with cybersecurity, especially when my kids are using our devices for schoolwork" (Participant 3, personal communication, 2024). Similarly, Participant 5 (Institution B) stated, “I'm constantly aware of what my family is doing online, which makes me more vigilant about security policies at work” (Participant 5, personal communication, 2024). These insights illustrate how personal responsibility influences security behavior and beliefs.

Advocating stronger cybersecurity policies became the central focus after the breach. One participant shared, "Since the attack, we’ve advocated heavily for more funding and state-level policy changes. Cybersecurity needs to be a larger part of the budget discussion for all colleges. We’ve pushed this at our administrative meetings” (Participant 2, personal communication, 2024).

This approach enriches the understanding of how personal circumstances influence cybersecurity and aids in tailoring cybersecurity education and policies to meet diverse needs. For instance, Participant 7 (Institution C) emphasized the importance of flexible security training programs to, “accommodate different personal responsibilities, and we need to account for these differences in our training and ensure everyone is equipped to handle security risks at home and work" (Participant 7, personal communication, 2024).

Insights and Analysis

The analysis of cybersecurity practices based on interviewees’ responses highlights several critical trends and disparities.

1. Training and Awareness have emerged as fundamental components of a robust cybersecurity defense strategy. With access to more resources, larger institutions were better positioned to implement continuous and comprehensive training initiatives, ensuring that all staff members, from IT personnel to administrative staff, were well versed in cybersecurity protocols. By contrast, smaller institutions face significant challenges due to constrained budgets, limiting their ability to provide regular or specialized training. This lack of consistent education could leave smaller institutions more vulnerable to human error, one of the most significant contributors to security breaches, highlighting the importance of securing additional funding or government grants to expand cybersecurity education across all levels of institutions.

2. Technological Integration, particularly with AI-driven solutions, has been recognized as essential for proactive threat detection. Larger institutions were able to invest in cutting-edge technologies, such as artificial intelligence, to identify and mitigate threats in real time, thereby reducing the risk of breaches. However, smaller institutions need help with the initial cost and complexity of integrating these advanced systems into their cybersecurity infrastructure. The need for more accessible and scalable solutions is evident, as smaller institutions face a growing gap in their ability to combat increasingly sophisticated cyber threats. Open-source AI tools, partnerships with larger institutions, and government-funded solutions can help bridge this gap.

3. Resource and Budget Limitations have emerged as one of the most consistent challenges across institutions, particularly affecting smaller colleges. These limitations hinder their ability to adopt advanced technologies, such as AI, implement high-level security protocols, and hire specialized personnel with the expertise needed to manage modern cybersecurity infrastructure. As a result, many smaller institutions were forced to rely on third-party Managed Security Service Providers (MSSPs) to manage their security needs, which introduced risks, such as over-dependence and potential delays in response times. Institutions must find a balance between leveraging third-

party services and developing internal capabilities to ensure long-term sustainability of their cybersecurity efforts.

4. Compliance with Evolving Regulations posed a significant challenge for institutions of all sizes, particularly for smaller ones, which often lacked the resources to keep pace with shifting legal requirements, such as FERPA, HIPAA, and state-specific mandates, such as the CCPA. Larger institutions have dedicated compliance teams that could stay on top of these evolving regulations, but smaller colleges often face increased vulnerability due to insufficient resource allocation. Additionally, as institutions increasingly integrate AI into their cybersecurity strategies, the legal and regulatory landscapes become even more complex. Guidelines for the ethical use of AI in security are still under development, making it imperative for institutions to adopt more dynamic compliance strategies that can evolve with regulatory changes. Engaging proactively with regulatory bodies could help institutions shape future policies and ensure that compliance strategies are forward thinking.

5. Incident Response and Recovery Practices varied dramatically depending on institutional size. Larger institutions have more established, well-defined incident response plans, enabling them to react swiftly and effectively to cybersecurity breaches. They also benefited from internal teams dedicated to recovery efforts, reducing downtime, and potential damage. By contrast, smaller institutions, which are more reliant on external services such as MSSPs and cybersecurity insurance, often face delays in incident response and recovery. This reliance on external support underscores the importance of building an internal capacity to handle cyber-attacks immediately after math while maintaining relationships with external vendors to supplement in-house capabilities.

6. AI Technologies is becoming increasingly vital for improving the detection and response capabilities of educational institutions. AI offers a real-time threat analysis, which is crucial for

identifying and neutralizing threats before they can cause significant damage. However, institutions must update their AI-driven security systems regularly to ensure that they remain effective against evolving threats. AI's capacity to analyze large datasets and detect anomalies could make it an invaluable tool in preventing cyber-attacks. Still, institutions must remain vigilant in maintaining and upgrading these systems to adapt to new threats.

7. Continuous Evaluation and Updating of AI-Enhanced Security Measures are critical for staying ahead of sophisticated cyber-attacks. AI systems are not set-it-and-forget-it solutions; they require frequent reconfigurations and updates to maintain effectiveness. In addition, security personnel must be adequately trained to operate these systems and address the complexities of AI configuration and management. Leveraging AI tools responsibly means ensuring that institutions have both the technological infrastructure and the human expertise necessary to effectively integrate these systems into their broader security framework.

8. Training and Awareness Programs have evolved to include specialized AI-focused content, reflecting AI's dual role as both a defense tool and a potential attack vector. These programs teach the technical skills required to manage AI-driven security systems and emphasize critical thinking in anticipating AI-based attacks. With AI being used by malicious actors to automate and enhance cyberattacks, such as generating deepfakes or launching sophisticated phishing campaigns, institutions must prepare their staff to recognize and respond to these evolving threats.

9. High-Security Awareness Programs among all institutional stakeholders are becoming more important than ever as AI tools become integrated into daily cybersecurity operations. The content of these programs must be continuously updated to reflect the latest developments in AI, covering not only technical aspects but also ethical considerations, potential vulnerabilities, and ways to detect AI-driven threats. For example, identifying the rise of AI-generated phishing attempts

and fake online identities (deepfakes) requires training to become more sophisticated and adaptive to the changing cyber landscape. These programs serve as frontline defenses, ensuring that all personnel actively contribute to the institution's cybersecurity posture.

Several participants expressed concerns about the increasing use of AI-driven cybersecurity tools, particularly regarding handling student data and compliance with regulations, such as FERPA. Interviewee 3 noted, 'While AI helps us detect threats faster, we're always concerned about how these tools manage sensitive information' (Interviewee 3, personal communication, 2024). This finding aligns with recent literature indicating that organizations adopt AI technologies without fully addressing privacy concerns (BBC 2024; Perna 2024).

These insights emphasize the need for educational institutions to leverage AI for cybersecurity and to ensure that their use of these technologies complies with privacy regulations. Concern over data protection highlights a critical area in which institutions must balance technological advancements with ethical and legal responsibilities.

Conclusion

This chapter summarizes the research questions and key findings from the interviews, highlighting the significant challenges that institutions face in building robust cybersecurity defenses. These challenges include limitations in recovery strategies, the need for continuous audits, and the complexities of integrating advanced technologies such as AI-driven detection. Participants also emphasized a critical shortage of skilled cybersecurity personnel, which exacerbates existing vulnerabilities. The analysis further underscores the importance of aligning cybersecurity measures with institutional priorities to ensure long-term resilience. Chapter 5 provides an overview of the recommendations developed from these insights, focusing on strategies to address the identified challenges and improve cybersecurity defenses in educational institutions.

Chapter 5 - Conclusions and Recommendations

This chapter explores the main aspects of the study, starting with the problem statement, purpose, research questions, and the theoretical and conceptual frameworks that shaped the research. It outlines the methodology and data collection process and presents the findings. The analysis connects these findings to prior research and the guiding frameworks, considering their implications for educational institutions. Finally, this chapter offers recommendations for strengthening cybersecurity practices and proposes areas for further research.

Study Overview

U.S. colleges currently face unprecedented cyber-attacks due to their public identity, substantial volumes of sensitive student and staff data, and limited cybersecurity resources. These challenges are exacerbated by increasing reliance on third-party services, which introduce additional vulnerabilities. In response to these threats, this study sought to critically evaluate how resource-constrained colleges and universities manage cybersecurity risks, particularly through external resources and strategic partnerships.

By applying the NIST Cybersecurity Framework (CSF 2.0) alongside theoretical models, such as Resource Dependency Theory, Social Cognitive Theory, and the Technology Acceptance Model, the research identified effective strategies for enhancing institutional cybersecurity. A qualitative approach was used, employing semi-structured interviews and questionnaires to gather insights from cybersecurity professionals from multiple institutions. A thematic analysis of the data revealed that governance, continuous training, and strategic technology adoption play crucial roles in mitigating risks and ensuring compliance with data protection regulations.

The findings provide actionable recommendations for strengthening cybersecurity measures in educational settings, emphasizing the need for proactive governance, robust training programs, and technology integration tailored to the unique contexts of U.S. colleges and universities.

Discussion of the Findings

This section addresses the three research questions outlined at the beginning of the study, synthesizes the data gathered from interviews, and discusses the practical implications of the findings. The findings align with the Six Core Functions of the NIST CSF 2.0: Govern, Identify, Protect, Detect, Respond, and Recover. The study's best practices reflect how U.S. colleges operationalize these functions within their cybersecurity strategies.

Research Question 1 (RQ1): What are the best practices in the U.S. college environment for the use of security firms, third-party software, endpoints, and cybersecurity insurance?

The study identified several best practices, including the strategic use of managed security services, comprehensive training programs, and leveraging of advanced security software.

Advanced Security Software and AI Integration

As discussed in Section 4, the implementation of AI in security systems is rapidly evolving. Several participants highlighted the role of AI in real-time threat detection, with Participant 3 from Institution A noting, "Our AI systems allow us to catch threats that would have otherwise been missed". (Participant 3, personal communication, 2024). One best practice institution should consider investing in in-house built AI-driven solutions to enhance its security posture.

This trend indicates that the most effective institutions rely heavily on advanced security tools to strengthen their cybersecurity defenses. For example, Participant 7 (Institution B) noted, "AI is featured in many tools we utilize. Machine learning is a part of solutions such as EDR and SIEM. It

adjusts alerting based on the behaviors in your environment, shifting the tool from being reactive to a more proactive response" (Participant 7, personal communication, 2024). This reflects the best practice for utilizing AI and machine learning to detect and respond to cyber threats more effectively. As noted in Chapter 4, each institution studied has adopted SOC services to manage security more effectively. For example, Participant 7 from Institution C emphasized, "Our SOC is essential in monitoring threats around the clock, providing protection that our internal team alone couldn't manage" (Participant 7, personal communication, 2024). (SOC, as introduced under 4.4 Data Analysis Process—Using NIST Framework, refers to the Security Operations Center.) This shift towards centralized security management aligns with contemporary trends in cybersecurity strategies, as discussed in Chapter 2.

To enhance the effectiveness of advanced security software, institutions should integrate SOCs that provide a centralized approach to monitoring and responding to threats. One participant explained, "The SOC plays a critical role in how we manage our AI-driven security tools, ensuring that all alerts are properly assessed and acted upon swiftly." (Participant 8, personal communication, 2024) This integration allows for real-time adjustments and more dynamic threat mitigation strategies.

Comprehensive Training Programs

Ongoing training is crucial. Participant 2 (Institution A) emphasized, "We've stepped up since then. We have invested more in our cybersecurity, upgrading our antivirus software, adding advanced intrusion detection firewalls, and focusing a lot on training everyone better so that all our staff understand how important security is and what they can do to help keep our networks safe' (Participant 2, personal communication, 2024). Continuous cybersecurity education for all institutional members is essential for maintaining secure defense. Effective training programs typically include awareness of phishing attempts, suspicious links, and handling potential malware emails. In addition, educating staff on secure password practices, reporting suspicious activities promptly, and understanding their role in

the institution's broader cybersecurity strategy are critical components of a comprehensive training regimen. Targeted training efforts are crucial for creating a culture of security awareness across institutions, empowering staff to act as the first line of defense against cyber threats.

Third-party Security Firms

Unfortunately, institutions continue to increase their dependence on third-party firms for threat detection, driven primarily by resource limitations and the need for advanced capabilities. This dependency raises serious concerns about potential vulnerabilities because relying too heavily on external providers can weaken institutional control over critical security functions. The July 2024 CrowdStrike incident is a prime example of why it remains a significant risk (Hale, 2024). A prime example is reflected in the Participant 6 (Institution C) statement, "We have engaged with external experts who provide us with 24/7 monitoring, advanced threat intelligence, and tailored security solutions that have significantly strengthened our cybersecurity framework" (Participant 6, personal communication, 2024). This highlights why institutions often consider external partnerships valuable for accessing specialized expertise and round-the-clock monitoring. However, this underscores the ongoing tension between enhanced security capabilities and potential dependency risk.

The institution has outsourced critical security functions to compensate for limited internal resources. A participant shared, "Outsourcing to third-party firms has definitely relieved some pressure off our internal team. But there's always a risk. We try to strike a balance between leveraging their expertise and not becoming too dependent on them" (Participant 4, personal communication, 2024).

However, institutions must be cautious of overreliance on third-party vendors. The CrowdStrike incident occurred because of a security software update deployed to one of its products, resulting in a worldwide IT outage that had a substantial impact on numerous sectors, including airlines and hospitals. This demonstrates the risks associated with the third-party solutions. This incident underscores the

importance of institutions developing in-house AI systems to reduce their dependency on external vendors. The adoption of open-source tools can provide greater control and security oversight. Implementing the NIST framework internally is also a best practice, ensuring that institutions maintain robust security standards through a structured, step-by-step process managed directly by the college IT function.

Research Question 2 (RQ2): What is their influence on the overall security posture of U.S. colleges?

The adoption of these best practices significantly enhances the overall security stance of U.S. colleges by minimizing vulnerabilities, strengthening response capabilities, and promoting a culture of cybersecurity awareness.

Enhanced Security Posture.

Institutions that have implemented robust security measures and comprehensive training programs have reported fewer security breaches and faster response times to cyber threats. Participant 2 (Institution A) noted, "After adopting these practices, we saw a noticeable decrease in successful phishing attempts and other cyber threats. Our staff is now more vigilant, and our response times have improved significantly" (Participant 2, personal communication, 2024).

Institution B's security posture has evolved significantly over the past few years, becoming more proactive. As one participant mentioned, "…our security posture was vastly different from that of five years ago. Now, it's much more proactive thanks to the layered systems we've put in place, like continuous monitoring and MFA" (Participant 5, personal communication, 2024).

Establishing an SOC is crucial for maintaining an institution's security. One participant remarked, "The SOC has become the nerve center of our security operations. It's where we monitor, detect, and

respond to all potential threats, strengthening our overall defensive strategies" (Participant 6, personal communication, 2024). If a Chief Technology Officer at a college prioritizes cybersecurity, they should focus on creating and continuously enhancing in-house SOC to ensure robust cybersecurity measures.

Implementing an advanced SIEM system is essential for maximizing its effectiveness. SIEM integration with AI and machine learning would enable real-time analysis and predictive threat detection, allowing the SOC team to identify potential attacks before they fully materialize.

In addition, the development of a layered defense strategy is crucial. Integrating firewalls, intrusion detection/prevention systems, and endpoint security tools to work with the SOC creates a cohesive defense infrastructure, triggering automated alerts for rapid incident response.

Regular training and simulations of SOC team members remain a priority. Simulating cyber-attacks, such as phishing or ransomware scenarios, ensures that the team remains proactive in identifying and neutralizing threats rather than simply reacting to them. Continuous learning and adaptation are key to the ever-evolving cybersecurity landscape.

While maintaining a strong internal SOC, selective outsourcing to Managed Security Service Providers (MSSPs) offers additional support during resource-constrained periods. However, emphasis remains on building and maintaining internal expertise to ensure complete control over the institution's security operations.

Through these strategies, the institution remains well-prepared to handle emerging cybersecurity threats and maintain operational resilience in an increasingly complex digital environment.

Proactive Approaches and Real-Time Detection.

AI-driven tools have enabled institutions to shift their security posture from reactive to proactive, thereby allowing them to detect and respond to threats more quickly than ever before. Participant 6 (Institution B) highlighted, "Our security posture has improved, and we are more resilient because we can identify and respond to threats faster than ever before" (Participant 6, personal communication, 2024). Adopting a proactive approach is crucial for keeping up with evolving cyber threats and enabling quicker detection and response to potential security breaches. By anticipating and preparing for threats before they occur, institutions can minimize the impact of attacks, reduce downtime, and prevent data loss. Rapid response times are critical when dealing with advanced threats, such as ransomware, where every minute of delay can increase the risk of widespread system compromise. Moreover, a proactive stance helps institutions stay ahead of emerging attack vectors, ensuring that security measures evolve alongside new threats, rather than reacting only after an incident occurs.

Layered Security and Training Impacts

A layered security approach combined with regular training resulted in a marked improvement in incident response times. Participant 4 (Institution C) shared, "With our layered security approach and comprehensive training, we've seen a significant reduction in the number of successful attacks and a marked improvement in our incident response times" (Participant 4, personal communication, 2024). This emphasizes the importance of both technological tools and human readiness.

The impact of layered security and comprehensive training has transformed institutions. One participant explained, "We've seen how critical training is as part of our overall security strategy. It's not just about having firewalls or endpoint detection—it's about making sure everyone knows how to react when something suspicious happens" (Participant 1, personal communication, 2024).

One critical component for enhancing security posture is implementing an SOC. SOCs play a vital role in proactively detecting and responding to cyber threats in real-time. As cybersecurity threats become more sophisticated, institutions are turning to SOC services—whether managed in-house or through third-party MSSPs—to maintain continuous defense.

At Institution B, the importance of SOC services has been recognized as crucial in achieving a proactive stance:

"Our institution's MSSP manages SOC operations, providing 24/7 monitoring and threat intelligence" (Participant 5, personal communication, 2024).

Similarly, Institution C noted the benefits of outsourcing SOC functions:

"We have a third-party MSSP that handles our SOC services, and they are engaged in actively protecting our data while the attack is happening" (Participant 7, personal communication, 2024).

Research Question 3 (RQ3): How can U.S. colleges evolve their cybersecurity strategies to anticipate and counter emerging cyber threats based on historical trends and expert insights?

This study reveals that institutions must continuously evolve their cybersecurity strategies to anticipate and counter future threats, focusing on predictive analytics, flexible security policies, and proactive incident management.

Integrating Comprehensive Risk Management

Institutions are evolving by integrating comprehensive risk-management strategies that utilize predictive analytics tools to mitigate potential threats. Comprehensive risk management involves a holistic approach to identifying, assessing, and responding to cybersecurity risk. This strategy requires constant monitoring, employee training, system updates, and the adoption of advanced technologies such as AI-driven analytics. In a college setting, this might include regularly assessing vulnerabilities

across all systems, ensuring compliance with regulatory frameworks, such as FERPA and HIPAA, and developing detailed incident response plans to handle potential breaches.

Participant 7 (Institution B) said, "Our institution is preparing by strengthening our cybersecurity posture, adding layers to our 'Defense in Depth's strategy. Predictive analytics tools are part of this, allowing us to foresee and mitigate potential threats before they fully materialize" (Participant 7, personal communication, 2024).

For a college looking to implement comprehensive risk management, it should include steps such as conducting regular risk assessments, incorporating threat intelligence to predict potential attacks, and continuously improving staff training and system updates. Predictive analytics tools, as mentioned by Participant 7, would serve as an integral component by analyzing historical data and identifying patterns that could signal emerging threats. This approach enables institutions to respond to risks and proactively mitigate them before they incur considerable damage.

The integration of comprehensive risk management strategies has become more critical. As one participant described, "We're working towards a more integrated risk management system, one that encompasses both technical and human risks. It's not easy, especially with budget constraints, but it's necessary if we're going to stay secure" (Participant 6, personal communication, 2024).

Adaptive and Future-Focused Security Strategies

Institutions must continuously adapt their security strategies. As Participant 2 (Institution A) suggested, "We're continuously working on improving our security measures. It's all about not just getting back to where we were but going beyond and being prepared for whatever comes next" (Participant 2, personal communication, 2024). This indicates that institutions must prioritize the evolution of their cybersecurity strategies rather than merely maintaining the status quo.

For a college CEO to understand the necessity of this evolution, several steps must be considered (Cybersecurity and Infrastructure Security Agency [CISA], 2024).

- **Proactive Security Audits**: Regularly conduct internal and external security audits to identify weaknesses in the system. This approach goes beyond meeting compliance requirements and helps to uncover potential vulnerabilities before they become real threats.

- **Investing in Emerging Technologies**: Continuously upgrading the latest cybersecurity technologies, such as AI-driven threat detection or behavioral analytics, to stay ahead of increasingly sophisticated cyber threats.

- **Employee and Staff Training**: Both cybersecurity threats and the knowledge required to counter them constantly evolve. Continuous training and benchmarking with similar institutions ensure that employees are aware of the latest phishing schemes, social engineering tactics, and security protocols.

- **Enhancement of incident response plans**: An evolving incident response plan is essential. Institutions should have a plan in place, and regularly test and update it based on new threat landscapes and past incidents.

- **Partnerships with Cybersecurity Vendors**: Building long-term partnerships with cybersecurity vendors ensures timely access to advanced tools and expertise, allowing institutions to address new threats as they arise.

- **Budgeting for Security Innovations**: Allocating a portion of the annual budget to invest in new cybersecurity tools, staff training, and response mechanisms is vital for staying adaptive. The CEO should understand that cybersecurity is not a one-time investment, but an ongoing priority.

The implementation of these steps clearly makes it necessary to develop security strategies. This approach underscores the critical importance of ensuring the institution's resilience in an ever-changing threat landscape, helping the CEO recognize cybersecurity as a dynamic process that demands consistent attention and investment.

Institutional B's approach has become more adaptive, with a focus on future threats. One participant stated, "Our strategy has always been to stay ahead of threats. It's not enough to react. We need to anticipate what's coming next, especially as AI-driven attacks become more common" (Participant 4, personal communication, 2024).

Flexible Security Policies

The ability to adapt security policies to address changing cyber threats is essential. Participant 5 (Institution C) mentioned, "We need policies that are not just set in stone but can evolve with the changing threat landscape. Flexibility and adaptability in our security protocols are key to staying ahead of cyber threats" (Participant 5, personal communication, 2024). This underscores the need for policies that evolve in tandem with emerging cyberthreats.

Institution C adopted more flexible security policies that can adapt to emerging threats. One participant shared, "Our security policies have become much more flexible. We update them regularly, incorporating feedback from recent incidents to ensure they remain relevant" (Participant 7, personal communication, 2024).

Learning from Past Incidents.

- Finally, institutions must learn from past incidents to refine their strategies continuously. Participant 3 (Institution A) added, "The future of cybersecurity in education will depend on our ability to continuously learn from past incidents and adjust our strategies to

meet new challenges head-on" (Participant 3, personal communication, 2024). This iterative approach ensures that institutions remain resilient and prepare for threats in the future.

The findings of this study reveal that U.S. colleges employ a range of cybersecurity practices that align with the Six Core Functions of the NIST CSF 2.0: Govern, Identify, Protect, Detect, Respond, and Recover. By organizing the discussion around these functions, the best practices identified in this study can be clearly linked to a structured cybersecurity approach. The best practices discussed in relation to the research questions align with the core NIST functions, as shown below.

NIST Function 1: Govern

Best Practices:

- **Establishing Cybersecurity Governance Policies**: Governance is essential for aligning cybersecurity strategies with institutional goals. Interviewee 7 noted, "It's more than just having the right tech or tools. It's about creating a culture where everyone understands they play a part in keeping us safe". Establishing clear governance frameworks ensures the effective and consistent implementation of policies.

- **Board-Level Cybersecurity Oversight**: Involving senior leadership in cybersecurity decision making can drive more substantial institutional support. Interviewee 2 emphasized, "Ensuring that everyone understands and adheres to our cybersecurity policies is crucial. Cybersecurity isn't just about having strong policies; it's also about ensuring people follow them".

- **Continuous Policy Review and Updates**: Regularly updating cybersecurity policies to reflect emerging threats is crucial. According to Interviewee 4, "Continuous

improvement is necessary; we regularly review our policies to stay ahead of threats". This approach helps institutions to remain agile in the face of new risks.

- **Data Privacy and Compliance Management**: Compliance with regulations such as FERPA, HIPAA, and GDPR is integral to governance. Interviewee 1 shared that their institution had "implemented changes such as multi-factor authentication and restricted access to sensitive data to meet compliance standards." Aligning data protection measures with compliance requirements helps mitigate legal risk.

- **Cybersecurity Culture and Leadership Training**: Promoting a cybersecurity-aware culture across all levels, including leadership, ensures that cybersecurity becomes an institutional priority. Interviewee 7 stated, "Our leadership has become more receptive to recommendations around cybersecurity, which has helped integrate better practices into our overall strategy."

NIST Function 2: Identify

Best Practices:

- **Risk Assessments and Vulnerability Identification**: Effective vulnerability identification is a core part of the NIST Framework. In line with this, Participant 3 from Institution A noted the importance of regular risk assessments, stating, "We regularly perform risk assessments now, something we didn't always do before." (Participant 3, personal communication, 2024) This practice helps to catch vulnerabilities before they escalate into serious issues. Institutions commonly use risk assessments to pinpoint vulnerabilities and prioritize resources. This helps ensure that critical infrastructure is protected. Participant 2 (Institution A) mentioned, "We use risk assessments to identify where our vulnerabilities are before anything can happen" (Participant 2, personal communication, 2024). Risk assessments

and vulnerability identification have become integral to Institution A's cybersecurity approach. One participant explained, "We regularly perform risk assessments now, something we did not always do before. It helps us catch vulnerabilities before they turn into bigger problems" (Participant 1, personal communication, 2024).

- **Cybersecurity Training Programs**: To identify risks, training programs are implemented to raise awareness of cybersecurity threats among the staff and students. This allows institutions to identify potential weaknesses proactively before they can result in incidents. Training is an integral part of maintaining vigilance across all institutional levels.

NIST Function 3: Protect

Best Practices:

- **IDPS**: Many institutions use IDPS tools to prevent unauthorized access. Participant 4 (Institution C) noted, 'Our IDPS has caught several attempted breaches before they could cause harm' (Participant 4, personal communication, 2024).

- **Implementation of Role-Based Access Control (RBAC)**: Some institutions have integrated RBAC to ensure that only authorized users can access critical systems. Participant 1 (Institution A) mentioned, "RBAC has greatly reduced the risk of internal data leaks" (Participant 1, personal communication, 2024). For Institution C, implementing RBAC was a key protective measure. One participant noted, "With RBAC, we've minimized the number of people who have access to sensitive data. It's a simple but effective way to reduce risks" (Participant 6, personal communication, 2024).

- **Regular Security Updates**: Ongoing maintenance and updates are crucial for maintaining relevant protective measures. Participant 5 (Institution B) said, 'Without regular

updates and continuous investment in new technologies, our systems would quickly become obsolete" (Participant 5, personal communication, 2024).

NIST Function 4: Detect

Best Practices:

- **AI-Driven Detection Tools**: Colleges increasingly use AI-powered tools to proactively detect and respond to threats. Participant 1 (Institution C) shared, "AI has shifted our security posture from reactive to proactive, allowing us to anticipate threats before they fully develop" (Participant 1, personal communication, 2024).

- **SIEM**: Institutions have integrated SIEM systems to monitor unusual activities and alert administrators when suspicious events occur. This contributes to a quicker threat detection and incident prevention. Intuition B implemented advanced detection tools to stay ahead of threats. One participant remarked, "Our SIEM systems have drastically reduced our response times. We're able to detect anomalies in real-time and act before anything escalates" (Participant 5, personal communication, 2024).

NIST Function 5: Respond

Best Practices:

- **Incident Response Plans (IRP)**: Institutions have formalized incident response strategies to mitigate the effects of cybersecurity events. Participant 3 (Institution C) emphasized the importance of IRP: "Our incident response plan allows us to respond quickly and minimize the damage from any breach" (Participant 3, personal communication, 2024). The incident response plan at Institution A been tested and proven to be effective during recent attacks. One participant shared, "Our incident response plan has been tested twice in the last

year, and it's clear that early planning made all the difference. The team knew exactly what to do, and we minimized the impact of both incidents" (Participant 3, personal communication, 2024).

- **MSSPs**: Many institutions have partnered with MSSPs to provide continuous monitoring and response. Participant 5 (Institution C) said, "Our partnerships provide us with expertise and round-the-clock monitoring that our in-house team cannot match" (Participant 5, personal communication, 2024). While effective, there is also a recognized need for internal response capacity to avoid over-reliance on external services.

NIST Function 6: Recover

Best Practices:

- **Cybersecurity Insurance**: Some institutions utilize cybersecurity insurance to help recover from the financial damage caused by attacks. However, delays in receiving support remain a challenge, as noted by Participant 6 (Institution B): "While insurance helps, the delays in getting support during an incident can be a major hindrance" (Participant 6, personal communication, 2024). Cybersecurity insurance has played a role in recovery efforts at Institution B. One participant noted that, "Cybersecurity insurance has helped, but we learned the hard way that it's no substitute for having robust recovery systems in place. You can't wait for the insurance company to help you bounce back" (Participant 5, personal communication, 2024).

- **Resource Allocation for Recovery**: Resource limitations, especially in smaller institutions, hinder the ability to quickly recover from cyber incidents. Participant 2 (Institution B) highlighted the financial strain: "We struggle with balancing our budget constraints while trying to implement robust security measures" (Participant 2, personal communication, 2024).

Comparative Analysis of Cybersecurity Practices

Based on the data collected from interviews and questionnaires, several important challenges and strategies have emerged within U.S. college cybersecurity practices. One of the main issues highlighted was the inconsistent application of best cybersecurity practices across institutions. Many smaller institutions need more resources to maintain regular training sessions or to enforce policies effectively, leaving them vulnerable to advanced cyber threats. Continuous improvements in cybersecurity awareness, training, and resource allocation are crucial for helping institutions of all sizes defend themselves against evolving threats. One participant from Institution A noted that their investment in upgraded systems and improved training ensured that staff remained vigilant and actively engaged in maintaining security.

Another critical aspect discussed was reliance on third-party cybersecurity providers. Many institutions, particularly those with limited IT staff, have turned to externally Managed Security Service Providers (MSSPs) for support. These third-party services offer essential tools, such as round-the-clock monitoring and advanced threat detection. However, overreliance on these external providers without proper oversight introduced new vulnerabilities. Participants emphasized that while external partnerships were necessary, continuous evaluation and integration with internal security policies were vital for reducing risks. In particular, the CrowdStrike incident served as a reminder of the potential risks inherent in relying heavily on third-party services.

The adoption of AI-driven security technologies presents opportunities and challenges for educational institutions. Although AI-enhanced tools, from an external perspective, have improved the ability of institutions to detect and respond to cyber threats, many participants reported difficulties in integrating these tools due to financial constraints and a lack of institutional readiness. Smaller institutions in particular struggle with outdated policy frameworks and limited expertise, making it

challenging to fully leverage these emerging technologies. Regular updates to security measures are essential to ensure that these technologies keep pace with the rapidly evolving cyber threats.

However, despite the advantages of AI-driven tools in enhancing the efficiency of cybersecurity practices, several challenges remain, particularly the ethical implications of their use. The participants expressed concerns about the potential risks associated with using AI, especially in the context of protecting student data. As Interviewee 3 emphasized, “While AI helps us detect threats faster, we’re always concerned about how these tools manage sensitive information” (Interviewee 3, personal communication, 2024).

These findings align with recent discussions in the literature, which highlight the tension between leveraging AI to enhance cybersecurity and ensure compliance with privacy regulations, such as FERPA and GDPR (BBC, 2024; Perna, 2024). While traditional, less-automated approaches may offer greater control over sensitive data, AI-driven solutions, although efficient, can inadvertently introduce privacy vulnerabilities if not properly governed. Thus, when adopting AI tools, institutions must carefully weigh the trade-offs between automation and data protection to ensure that the efficiency benefits do not come at the expense of data privacy.

Finally, maintaining institutional trust emerged as a key concern for the participants. Effective management of cybersecurity incidents, transparent communication, and comprehensive insurance coverage have been identified as crucial components for preserving trust among stakeholders. Failures in these areas have led to a loss of confidence from students, staff, and external partners, impacting the institution's credibility. Participants discussed the need for robust incident response plans and proactive security measures to minimize damage to institutional trust in the event of a breach.

Discussion of Findings in Relation to Literature

A comparison of this study's findings with the existing literature reveals corroborations and unique insights. The literature extensively discusses the importance of technological measures such as firewalls, intrusion detection systems, and antivirus software in mitigating cyber threats. However, this study emphasizes the equally critical role of human factors and organizational culture in shaping cybersecurity efficacy. While many studies have focused on technical defenses, this research suggests that without a strong cybersecurity culture and continuous training, even the most advanced technological measures may fall short. Overreliance on third-party vendors or quick, easy-to-implement solutions often dilutes critical skills within IT teams. This tendency means that internal teams may not be fully equipped to respond effectively when incidents occur, such as issues experienced by vendors such as CrowdStrike.

U.S. colleges should adhere to federal and state recommendations while exploring no-to-low-cost open-source applications to strengthen their cybersecurity infrastructure without compromising their internal expertise. By focusing on IT teams' skills and capabilities, colleges can mitigate the risks associated with external dependencies and foster a more sustainable and resilient security posture. These findings extend the academic conversation around cybersecurity practices, suggesting that a more integrated approach that combines technology, human behavior, and organizational culture is essential to effectively address cyber threats. This aligns with recent literature discussions that advocate for comprehensive strategies that go beyond technical solutions to include behavioral and cultural elements within organizations.

Implications for the Field

Critical recommendations for educational institutions regarding cybersecurity are categorized according to the Six Core Functions of the NIST Cybersecurity Framework: Govern, Identify, Protect, Detect, Respond, and Recover. These recommendations build on the findings of this study and offer practical insights into improving cybersecurity resilience across community colleges and universities.

Strengthening Governance and Policy Oversight: Institutions must prioritize developing a robust cybersecurity governance structure that involves senior leadership in the decision-making processes. This ensures that cybersecurity policies are effectively created and implemented across departments. Establishing a dedicated cybersecurity governance committee can help align institutional goals with risk management strategies, fostering a culture in which cybersecurity is integral to institutional planning and decision making. Continuous policy updates are crucial, especially in light of emerging threats and evolving regulatory requirements such as FERPA and GDPR.

Board of Trustees' Cybersecurity Accountability: While traditionally focused on high-level governance, Boards of Trustees can enhance institutional resilience by prioritizing cybersecurity at the strategic level. This includes supporting the allocation of the necessary resources, endorsing comprehensive policies, and holding executive leadership accountable for cybersecurity readiness. By doing so, boards can help foster a proactive risk-management culture, aligning institutional priorities with evolving cybersecurity challenges. However, it is crucial that their role remains focused on oversight rather than operational decision making to maintain a clear distinction in governance responsibilities.

Enhancing the Capacity to Identify Risks: Regular risk assessments should be expanded to include evaluations of automated deployment systems and cloud-based applications, which educational institutions are increasingly using. This proactive approach allows institutions to identify vulnerabilities

in their digital infrastructure before exploitation. Furthermore, institutions should invest in cybersecurity awareness training for staff, faculty, and students to increase vigilance against phishing attempts, social engineering, and other cyber threats that target human vulnerability.

Balancing Automation with Technical Expertise: The reliance on automated systems, such as one-touch or no-touch deployments, poses a significant risk to educational institutions if these systems fail during cybersecurity incidents. While automation can streamline operations, it can also create dependency on external vendors and automated processes, which internal teams may not fully understand. If these systems fail, institutions can face significant downtime or data breach. To mitigate this risk, colleges and universities must invest in continuous training programs focusing on developing in-house technical expertise.

Investing in Open-Source Solutions: Encouraging the use of open-source software solutions is an effective strategy for educational institutions. Unlike proprietary software, open-source platforms require active maintenance and customization, which helps internal IT teams to develop critical skills. Institutions can foster a hands-on approach to cybersecurity management by relying on open-source tools and reducing their dependency on external vendors. Open-source tools offer greater transparency, enabling institutions to identify and address vulnerabilities more effectively.

Continuous Technical Training: Educational institutions should establish regular mandatory training sessions for IT staff to support the effective use of both proprietary and open-source solutions. Ensuring that IT staff skills are up-to-date fosters a proactive mindset in identifying and mitigating potential cybersecurity threats, and encourages institutions to invest in growing their internal IT knowledge.

Advanced Detection Capabilities: The use of AI-driven detection tools and Security Information and Event Management (SIEM) systems is critical for identifying unusual activities in institutional networks. However, institutions should not rely solely on automated detection systems. Instead, they

should train internal teams to effectively interpret SIEM alerts and AI output. This dual approach ensures that automated systems are complemented by human expertise, thereby enabling a more adaptive and responsive cybersecurity posture.

This study's findings on adopting AI in cybersecurity have significant implications for educational institutions. Although AI tools offer substantial benefits in automating threat detection and response, they also present new challenges in terms of compliance with data privacy regulations. The fact that participants voiced concerns over the ethical use of AI underscores the need for institutions to prioritize privacy safeguards.

These implications extend beyond the educational sector, suggesting that institutions must establish robust governance frameworks to monitor the ethical deployment of AI technology. Policymakers should consider revising the existing regulations to account for the unique privacy risks associated with AI. As AI continues to be integrated into cybersecurity strategies, institutions must ensure that these technologies align with the ethical standards and regulatory requirements. The findings from this study highlight the urgent need for educational institutions to adopt a balanced approach to integrate AI technologies. Although AI-driven cybersecurity tools provide significant benefits, such as improved efficiency and real-time threat detection, they pose substantial challenges in protecting personally identifiable information (PII). Participants in the study voiced concerns about whether AI tools are being implemented with proper privacy safeguards, particularly concerning compliance with regulations such as the FERPA.

Institutions must prioritize the ethical use of AI technologies by conducting privacy impact assessments prior to deployment. This process should include technical evaluations and ensure that AI applications align with institutional data-protection policies. The push to adopt AI should maintain students' privacy and compliance with legal standards. Ignoring these concerns can lead to severe legal and reputational consequences.

Building a Resilient Response Framework: Developing robust incident response plans is essential for minimizing damage during a cybersecurity breach. Institutions should regularly test these plans using simulated exercises to ensure their readiness. Additionally, leveraging partnerships with Managed Security Service Providers (MSSPs) can provide around-the-clock monitoring, but institutions should avoid overreliance on external vendors. Instead, they should focus on building internal response capabilities to reduce the time required to detect and mitigate breaches.

Fostering a Culture of Cybersecurity Resilience: Beyond technical measures, institutions should cultivate a cybersecurity-aware culture among staff and students. Regular training sessions, phishing simulations, and awareness campaigns can help to embed cybersecurity practices into institutional culture. Leadership is key to driving this cultural shift by prioritizing cybersecurity in budgeting, strategic planning, and resource allocation.

Ensuring Effective Recovery Plans: The final function, Recover, emphasizes the importance of planning for business continuity after a cybersecurity incident. Institutions should establish a comprehensive recovery plan that includes technical recovery and communication strategies to address stakeholders and minimize reputational damage. Cybersecurity insurance can offer financial protection; however, it should be complemented with robust internal recovery systems to ensure a quick return to normal operations.

NIST Function 1: Govern

- **Cybersecurity Governance Policies**: Institutions must establish clear governance structures to align cybersecurity practices with institutional goals. This involves the integration of cybersecurity considerations into strategic planning. “Cybersecurity needs to be treated with the same seriousness as physical security. Most of our data is now online, and yet IT often has to fight to get funding for cybersecurity tools and staff” (Interviewee 1, personal communication, 2024).

- *Example*: As Interviewee 7 from Institution A emphasized, “Leadership has become more receptive to recommendations around cybersecurity, which has helped integrate better practices into our overall strategy” (Interviewee 7, personal communication, 2024).
- *Recommendation 1*: Regularly involves senior leadership in cybersecurity updates to ensure alignment with institutional priorities and foster a proactive cybersecurity culture.
- **Continuous Policy Review and Updates**: Governance includes ongoing reviews of cybersecurity policies to adapt to emerging threats. “We continuously review our security protocols to keep up with new regulations and threats. It’s a constant cycle of assessment and improvement” (Interviewee 3, personal communication, 2024).
- **Example**: Interviewee 2 highlighted, “Our compliance efforts focus on securing data and aligning with regulatory requirements” (Interviewee 2, personal communication, 2024)
.
- *Recommendation 2*: Implement quarterly reviews of cybersecurity policies to ensure that they remain aligned with the latest regulations and industry best practices.
- **Data Privacy and Compliance**: Ensuring compliance with data protection laws, such as FERPA, HIPAA, and GDPR, is essential. “We have taken significant steps to tighten our data security policies to meet compliance requirements” (Interviewee 4, personal communication, 2024).
- *Example:* According to Interviewee 7, “Our training ensures that staff are aware of compliance issues, which helps us stay ahead of potential penalties” (Interviewee 7, personal communication, 2024).
- *Recommendation 3*: Focus on integrating robust data privacy training to maintain compliance and minimize risks.

NIST Function 2: Identify

- **Risk assessment and vulnerability identification**: Institutions should regularly conduct risk assessments to proactively identify vulnerabilities in their systems. Training programs should help staff to recognize potential risks, allowing for quicker identification of threats.
- **Example:** As Participant 2 (Institution A) mentioned, "We use risk assessments to identify where our vulnerabilities are before anything can happen" (Participant 2, personal communication, 2024).
- *Recommendation 1*: Implement annual risk assessments and create specialized training modules that focus on threat recognition and vulnerability management for staff and students.
- **Tailored Training for Non-traditional Students**: Non-traditional Career and Technical Education (CTE) students present unique risks owing to irregular access to secure networks. Educational programs should focus on equipping students with cybersecurity knowledge, mainly through phishing simulations and secure password practices.
- *Recommendation 2*: Develop cybersecurity education specifically for non-traditional student populations, ensuring that they have tools to mitigate risks even when using insecure networks.

NIST Function 3: Protect

- **IDPS**: One of the best practices identified is the use of IDPS tools to prevent unauthorized access and monitor network activities.

- **Example:** Participant 4 (Institution C) noted, “Our IDPS has caught several attempted breaches before they could cause harm” (Participant 4, personal communication, 2024).
- *Recommendation 3*: Regularly update and audit IDPS systems to ensure that they effectively mitigate risks and adapt to new cyber threats.
- **RBAC**: To prevent unauthorized access, institutions should implement RBAC and ensure continuous security updates to protect the sensitive data.
- **Example:** Participant 1 (Institution A) mentioned, "RBAC has greatly reduced the risk of internal data leaks" (Participant 1, personal communication, 2024).
- *Recommendation 4*: Apply RBAC across the institution and regularly review access control systems for its effectiveness.
- **Budget Constraints on Protection**: Resource limitations can constrain institutions' ability to effectively protect their systems, notably smaller institutions.
- *Recommendation 5*: Develop targeted funding initiatives that prioritize upgrading outdated cybersecurity infrastructure and investing in advanced threat detection systems.
- *Recommendation 6*: Implement immutable backups to strengthen cybersecurity resilience. By integrating these unalterable data copies into their security framework, institutions can ensure that critical data remain protected from ransomware attacks and accidental deletions, providing a reliable restoration path. This approach enhances data protection and supports compliance with data privacy regulations, thereby offering a safeguard that complements other internal and external cybersecurity strategies.

NIST Function 4: Detect

- **AI-driven Detection Tools**: The use of AI for detecting cybersecurity threats has become critical for identifying potential breaches in real time.
- **Example:** Participant 1 (Institution C) shared, "AI has shifted our security posture from reactive to proactive, allowing us to anticipate threats before they fully develop" (Participant 1, personal communication, 2024).
- *Recommendation 6*: Invest AI-powered detection tools that utilize machine learning to predict and mitigate threats before escalating.
- **SIEM**: Implement SIEM systems to monitor unusual activity and alert administrators to suspicious events. This helps institutions to respond faster to potential threats.
- *Recommendation 7*: Regularly audit SIEM systems to ensure that they are adaptable and continually aligned with evolving threat landscapes.

NIST Function 5: Respond

- **IRP**: Institutions must have a formalized incident response plan to contain the damage caused by cybersecurity breaches.
- **Example:** Participant 3 (Institution C) emphasized, "Our incident response plan allows us to respond quickly and minimize the damage from any breach' (Participant 3, personal communication, 2024).
- *Recommendation 8*: Ensure that all institutions have well-documented and regularly updated incident response plans. This plan should be rehearsed using regular cybersecurity drills.

- **MSSPs**: While third-party security providers can enhance threat detection, institutions must avoid overreliance on them and maintain their internal response capabilities.
- **Example:** Participant 5 (Institution C) shared, "We've partnered with an MSSP to help monitor our network round-the-clock, providing us with threat intelligence and automated response capabilities" (Participant 5, personal communication, 2024).
- *Recommendation 9*: Institutions should maintain a balance between external partnerships with MSSPs and internal cybersecurity teams capable of handling breaches independently.

NIST Function 6: Recover

- Cybersecurity Insurance: While helpful in mitigating the fiscal impact of cyber incidents, relying heavily on insurance can delay recovery efforts.
- **Example:** Participant 6 (Institution B) noted, “While insurance helps, the delays in getting support during an incident can be a major hindrance” (Participant 6, personal communication, 2024). Similarly, at Institution C, another interviewee pointed out the limitations of relying on cyber insurance, noting: “Insurance offers financial protection in the event of a cyber incident, but it cannot substitute for the internal resilience required to detect and respond to threats quickly” (Participant 3, personal communication, 2024).

At Institution A, another participant was critical of the effectiveness of cybersecurity insurance, stating: “Only utilizing it once, I see it more as a hindrance personally. You waste several critical hours getting the relevant information to your insurance, and then there’s a lot of waiting while critical systems remain down.” (Participant 1, personal communication, 2024).

- *Recommendation 10*: As highlighted in Chapter 4, cybersecurity insurance has limitations in terms of the speed of incident response. Participant 5 from Institution B explained, “While insurance helps, the delays in getting support during an incident can be a major

hindrance" (Participant 5, personal communication, 2024). This finding aligns with the literature in Chapter 2, where Eling and Schnell (2016) emphasize that, while cyber insurance can mitigate risks, it should not replace robust internal recovery systems and a comprehensive cybersecurity risk management strategy. Therefore, institutions should use cybersecurity insurance as a supplementary tool while focusing on strengthening their internal recovery systems. Institutions should recognize the limitations of cybersecurity insurance and focus on building robust internal recovery systems. Relying on insurance alone can delay critical response efforts; therefore, it should be used only as a supplementary tool to ensure that internal strategies are in place for rapid service restoration post-incident.

Mandatory Cybersecurity Audits: Regular audits ensure that institutions are compliant with best practices and capable of adapting to the evolving cybersecurity threat landscape. At Institution B, a participant shared their views on the need for these audits, saying, "Cybersecurity audits are no longer optional. We treat them as a mandatory part of our operations to ensure that all security measures work as expected. Without these audits, we would be at serious risk of falling behind' (Participant 4, personal communication, 2024). Institution C recognized the value of external audits. One participant explained, "Having an external firm come in for mandatory audits gives us an unbiased view of where we stand. It helps us identify issues we might not see internally and keep us aligned with best practices" (Participant 6, personal communication, 2024).

- *Recommendation 11*: As discussed in Chapter 4, cybersecurity audits help institutions to proactively identify gaps in their recovery strategies. Participant 4 from Institution C emphasized the role of regular audits, noting, "These audits help us find vulnerabilities we might otherwise missed" (Participant 4, personal communication, 2024). This aligns with the research in Chapter 2, where Jones (2020) recommended mandatory audits as a critical part of

an institution's recovery planning. Therefore, institutions should conduct mandatory cybersecurity audits to ensure a swift and comprehensive post-incident recovery. Conduct mandatory and regular cybersecurity audits to proactively identify gaps in recovery strategies and overall security measures These audits should be treated as an essential component of cybersecurity management, ensuring that weaknesses are addressed before they can be exploited, and that recovery efforts are efficient and effective, enabling a swift return to normal operations after an incident.

Recommendations for Further Research

Based on this study's findings, several areas of further research are worth exploring. Future research should explore AI's evolving role in defending against and perpetrating cyberattacks in educational settings. Understanding AI's dual role as both a tool and threat will be crucial for developing effective cybersecurity strategies, as these technologies become more advanced. Given the growing reliance on AI technologies, future research should explore the impact of these tools on data privacy in an educational context. Longitudinal studies could provide valuable insights into how AI adoption affects compliance with regulations, such as the GDPR and FERPA. Additionally, more research is needed to identify the best practices for integrating AI in a way that upholds ethical standards, particularly when handling PII.

Institutions should also investigate the development of governance frameworks that address the risks associated with AI use. This could include examining the effectiveness of privacy impact assessments, audits, and staff training programs designed to mitigate risks associated with AI adoption.

Additionally, further studies could reassess the effectiveness of cybersecurity insurance as part of a comprehensive risk-management strategy, particularly considering the delays and challenges

highlighted in this study. Examining alternative risk-mitigation approaches that complement insurance could offer valuable insights for educational institutions seeking to enhance their cybersecurity posture.

While this study highlights two critical areas for further research, these could offer deeper insights and potentially enhance cybersecurity practices in educational settings. Future research could be structured into the following key areas:

- **Long-term Effectiveness of Cybersecurity Training Program**

Future studies could assess the durability of the knowledge and skills imparted by cybersecurity training programs. Longitudinal studies measure the retention of cybersecurity practices among faculty and students over time, and determine the frequency and content updates required for sustained efficacy.

- **Integration of AI and Machine Learning in Cybersecurity**.

As AI technologies evolve, further research is needed to explore their role in defending against and perpetrating cyberattacks within educational institutions. Research could focus on predictive models, real-time threat detection, and ethical considerations of using AI in cybersecurity.

- **Long-term Effectiveness of Cybersecurity Training Program**

Future studies could assess the durability of the knowledge and skills imparted through current cybersecurity training programs. Longitudinal studies could precisely measure the retention of cybersecurity practices among faculty and students over time, and determine the frequency and content updates required for sustained efficacy.

Additionally, research could evaluate the impact of different training modalities (e.g., in-person vs. online and interactive simulations vs. traditional lectures) on long-term cybersecurity behavior and incident response capabilities. Future research should explore and investigate the long-term impact of automated deployments and third-party solutions on the retention of technical skills within IT teams in

educational institutions. Exploring how continuous training and open-source software usage can mitigate these risks could provide valuable insights for developing sustainable cybersecurity practices.

1. **Integration of AI and Machine Learning in Cybersecurity.**

With the rapid advancement of artificial intelligence, further research is needed to explore how AI and machine learning technologies can be effectively integrated into cybersecurity frameworks in educational institutions. This includes developing and evaluating predictive models to detect and respond to cyber threats in real-time.

Studies could also explore or investigate the ethical implications and potential risks associated with AI-driven cybersecurity solutions, such as privacy concerns and manageability of AI systems.

2. **Psychological and Behavioral Factors in Cybersecurity Policy Adherence**

General psychological and behavioral factors that affect adherence to cybersecurity policies should be explored. Understanding the motivations, cognitive biases, and social influences that drive compliance or non-compliance could offer valuable insights into improving institutional cybersecurity culture.

3. **The impact of Cybersecurity Measures on Academic Freedom and Privacy**

Further research is required to explore the balance between robust cybersecurity measures and protection of academic freedom and privacy. This includes studying the impact of surveillance and monitoring tools on the educational environment and the perceptions of staff and students regarding their privacy.

This area of research can provide guidelines for developing cybersecurity policies that protect sensitive information and infrastructure without infringing on the rights and freedoms of the academic community.

4. **Comparative Studies Across Different Educational Contexts**

Comparative research across various educational institutions (e.g., community colleges vs. large universities and public vs. private) could provide insights into how contextual factors influence the effectiveness of cybersecurity measures.

Such studies could help tailor cybersecurity strategies to the specific needs and resources of diverse types of institutions, thereby enhancing overall security postures in a practical and contextually relevant manner.

5. **Role of Leadership in Shaping Cybersecurity Culture**

Exploring the role of educational leaders in shaping the cybersecurity culture can offer critical insights into how top-down influences affect the implementation and success of cybersecurity strategies. Future research could examine how leadership commitment to cybersecurity influences budget allocation, policy development, and institutional priorities, providing a blueprint for effective leadership in cybersecurity.

6. Rethinking Risk Management

To mitigate the limitations of cybersecurity insurance, institutions should shift their focus to building and maintaining strong internal defenses. This includes regularly updating the IRP and ensuring that these defenses are culturally ingrained across all levels of the institution.

US Colleges must consider adopting in-house AI-driven cybersecurity systems owing to recent third-party software vulnerabilities such as the CrowdStrike outage. These systems offer a range of benefits, including real-time threat detection, predictive analytics, and autonomous threat mitigation, and are all tailored to an institution's specific security needs. By leveraging machine learning models trained on institutional data, AI systems can evolve, providing a robust defense against emerging

threats. Furthermore, collaboration with universities or AI research institutions can reduce implementation costs and complexity. By investing in AI, institutions can significantly enhance their cybersecurity posture while reducing reliance on external vendors who are prone to unpredictable disruptions.

Future research should explore the long-term effects of AI-driven cybersecurity tools on data privacy and compliance at educational institutions. Given the concerns raised by participants regarding the handling of PII, longitudinal studies could provide deeper insights into how AI adoption impacts institutional compliance with regulations, such as FERPA and GDPR.

In addition, research should investigate the effectiveness of privacy impact assessments in mitigating the risks associated with AI deployment. Exploring the best practices for integrating AI that balance efficiency with privacy protection could provide valuable guidelines for educational institutions. A mixed-method approach that combines quantitative data on AI adoption with qualitative interviews on privacy concerns would be particularly beneficial for understanding this complex issue.

By addressing these recommended areas for further research, scholars and practitioners can contribute to a more comprehensive understanding of cybersecurity in the educational environment. This will ultimately lead to more sophisticated and adaptive cybersecurity strategies. This proactive approach not only enhances the immediate security of educational institutions but also effectively prepares them to meet future challenges. Institutions should avoid relying on single or multiple points of failure, especially when they are deeply embedded into the IT infrastructure or run and maintain critical functions. Instead, adopting a diversified approach enhances resilience and ensures robust cybersecurity defenses.

Conclusion

The findings of this study contribute significantly to the body of knowledge by providing empirical evidence on how educational institutions manage cybersecurity risks and implement security practices, with a focus on the practical application of frameworks such as NIST CSF 2.0. This study extends the current understanding of several critical areas.

1. **Operationalizing the NIST Framework in Education**: The study highlights how U.S. colleges and universities are integrating the NIST CSF 2.0 into their cybersecurity strategies. While the framework is widely known, this study provides tangible examples of how institutions apply their Six Core Functions—Govern, Identify, Protect, Detect, Respond, and Recover—in real-world educational settings. By illustrating these practical applications, this study contributes insights into how the framework can be adapted and operationalized within educational environments, which have unique challenges such as resource constraints and a diverse user base.

2. **Gaps in Compliance and Resource Allocation**: The research finds significant gaps in both compliance with evolving cybersecurity regulations and the allocation of resources. Smaller institutions, in particular, face challenges in keeping up with regulations such as the FERPA, HIPAA, and the CCPA due to budgetary limitations. This contribution helps policymakers and administrators to recognize the need for increased support and resources for institutions struggling to meet compliance requirements, suggesting a critical area for future investment and regulatory focus.

3. **Role of AI in Cybersecurity**: By exploring the integration of AI technologies such as machine learning in detection and response systems, this study advances the academic discussion on the dual role of AI as both a defensive tool and a potential source of risk. The

empirical findings emphasize the need for continuous evaluation of AI technologies, and this research adds to the understanding of how AI can be effectively incorporated into institutional cybersecurity strategies, offering institutions predictive analytics, and autonomous threat mitigation capabilities.

4. **Impact of Third-Party Security Solutions**: The study contributes to the ongoing debate regarding reliance on third-party security vendors. While managed security services (MSSPs) provide valuable expertise and monitoring, the July 2024 CrowdStrike incident underscores the risks of over-reliance on external solutions. This research highlights the importance of balancing external partnerships with internal expertise development, which is essential for institutional resilience in the face of cybersecurity incidents.

5. **Cybersecurity Culture and Training**: Another key contribution of this research is its focus on the human elements of cybersecurity. The findings suggest that fostering a cybersecurity-aware culture, supported by comprehensive training and awareness programs, is as crucial as implementing advanced technical solutions. This emphasis on the intersection between human behavior and technical measures contributes to a broader understanding of how educational institutions can build sustainable, proactive defenses against cyber threats.

Furthermore, this study has highlighted the increasing complexity of cybersecurity threats faced by U.S. educational institutions, particularly U.S. colleges. As shown through the interviews and data analysis, reliance on reactive security measures is no longer sufficient to protect sensitive institutional data. Instead, the findings underscore the growing need for a more integrated approach that includes both technological solutions and comprehensive cybersecurity culture.

The analysis of practices across institutions revealed the importance of collaboration, continuous training, and the integration of advanced security tools such as AI to improve both detection

and response. Furthermore, this study emphasizes that a strong cybersecurity posture must be supported at all organizational levels, from administrative staff to IT personnel, to ensure effective mitigation of risks.

The research contributes to the existing body of knowledge by validating the necessity of dynamic cybersecurity frameworks like the NIST CSF 2.0 and the importance of continuous adaptation in educational settings. The findings suggest that institutions must remain vigilant and adaptable as they face ever-evolving cyber threats.

One of the most significant outcomes of this research is highlighting the risks associated with over-reliance on external solutions, while emphasizing the importance of building a cybersecurity culture embedded into every aspect of an institution's operations. This study underscores that external solutions such as automated systems, third-party deployments, and cyber insurance offer convenience, a sense of security, and efficiency. However, they also introduce significant risks when institutions become overly dependent on them. Such reliance can result in a critical gap in the technical skills of internal teams. Institutions are left vulnerable when incidents occur without necessary expertise, as evidenced by the CrowdStrike outage. In these scenarios, a major cybersecurity incident could expose institutional vulnerabilities and prolong recovery efforts owing to the lack of internal capabilities and technical expertise required to troubleshoot and resolve these issues independently.

To counter these risks, educational institutions must adopt a proactive strategy that prioritizes continuous training of IT staff, ensuring that technical skills are developed, maintained, and enhanced over time. This strategy involves integrating no-to-low-cost open-source software solutions that require regular involvement from IT teams. Such solutions provide practical, hands-on experience, and encourage the ongoing use and refinement of skills that might otherwise become obsolete. By maintaining a level of internal engagement and expertise, institutions can minimize the risks associated

with external dependencies and ensure that they are prepared and knowledgeable in reducing and mitigating risks using external assistance only as a supplement rather than a crutch. This investment in training and skill development cultivates a more robust and self-reliant IT department, which serves as the first line of defense against cyber threats.

In addition to addressing external dependencies, this study emphasizes the importance of growing a solid cybersecurity culture that permeates all institutional levels. Institutions with a proactive cybersecurity posture invest in advanced technologies and comprehensive training and awareness programs for all members, including the staff, faculty, and students. Such programs should include phishing simulations, secure Internet practice workshops, and frequent updates on evolving threats. These initiatives are designed to raise awareness and create a shared sense of responsibility for security, ensuring that every individual, regardless of technical expertise, contributes to maintaining the institution's cybersecurity defenses.

Furthermore, educational institutions can create a sustainable and adaptive cybersecurity framework by integrating advanced technological solutions with a focus on developing internal capabilities and a continuous learning culture. This framework reduces the likelihood of breaches caused by human error, a leading cause of cyber incidents, and empowers institutions to respond swiftly and effectively to incidents. The combination of proactive training, skill development, and a cohesive cybersecurity culture enables institutions to build resilience from within, ensuring that they are equipped to face a complex and ever-evolving threat landscape. Ultimately, this study recommends that institutions balance their technological investments with efforts to cultivate internal expertise and a culture of vigilance, providing a comprehensive and adaptable defense system that extends beyond reliance on external vendors.

While external solutions such as cybersecurity insurance and third-party vendors provide essential support, this research highlights the dangers of over-reliance on these measures.

Insurance offers financial protection if a cyber incident occurs, but it cannot substitute for the internal resilience needed to detect and respond to threats quickly. Owing to budget constraints, many institutions and significantly smaller community colleges face challenges in developing robust internal defenses. In addition, owing to limited resources, universities encounter difficulties in sustaining comprehensive cybersecurity measures. This study suggests that, while insurance is a valuable risk management tool, institutions must prioritize building their ability to manage cyber threats effectively. This involves investing in an advanced cybersecurity infrastructure and developing IRP and internal teams capable of handling breaches without relying solely on external actors.

AI technologies have appeared to be both a critical asset and potential liability in cybersecurity. On the one hand, AI-driven tools such as machine learning-based threat detection systems can analyze large datasets in real-time, identify anomalies, and predict potential attacks before they fully materialize. These technologies offer institutions an initiative-taking defense mechanism that can keep pace with the rapidly evolving nature of cyber threats. However, this study also found that AI presented new risks. Attackers are increasingly leveraging AI to automate and scale their attacks, making it more challenging to detect and counter attacks. Institutions must be cautious in adopting AI, ensuring that they have the necessary safeguards to protect themselves against AI-enabled attacks. Furthermore, institutions should consider developing ethical guidelines for using AI in cybersecurity to avoid privacy and security violations.

In addition to the technical aspects of cybersecurity, this study emphasizes the importance of internal resilience. Institutions must implement the latest technologies and develop a robust and adaptable cybersecurity framework that can evolve alongside the threat landscape. This implies regular

policy updates, continuous staff training, and investment in human resources to ensure that the institution can independently manage its cybersecurity posture. Smaller institutions must find ways to balance their limited resources with the need for comprehensive security measures. This study advocates collaboration between institutions, such as sharing best practices and pooling resources, to enhance the overall security posture of the educational sector.

Moving forward, institutions must adapt to the current threat landscape and anticipate future challenges. As technologies such as quantum computing and sophisticated AI systems have become more prevalent, the nature of cyber threats will continue to evolve. Educational institutions should invest in research and development to explore the implications of emerging technologies on cybersecurity. By staying ahead of these advancements, institutions can ensure that they respond to threats and actively shape their cybersecurity future.

In conclusion, the findings of this study highlight the need for a holistic approach to cybersecurity that integrates advanced technological solutions with a proactive, institution-wide culture of security. Educational institutions must prioritize internal resilience, continuous training, and responsible adoption of AI to ensure that they are well-equipped to face the challenges of an increasingly complex cyber environment.

References

Adane, K. (2020). Current Status of Cyber Security in Ethiopia. Social Science Research Network. https://doi.org/10.2139/ssrn.3545189

Alawida, M., Omolara, A. E., Jantan, A., Al-Rajab, M. M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. Journal of King Saud University - Computer and Information Sciences, 34(10), 8176–8206. https://doi.org/10.1016/j.jksuci.2022.08.003

Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harm. (2023, June 27). Brookings. https://www.brookings.edu/articles/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/

Ashraf, S., Shawon, M. H., Khalid, H., M., & Muyeen, S. M. (2021). Denial-of-Service Attack on IEC 61850-Based Substation Automation System: A Crucial Cyber Threat towards Smart Substation Pathways. Sensors, 21(19), 6415. https://doi.org/10.3390/s21196415

Bandura A. B. (1986). Social Cognitive Theory. https://psycnet.apa.org/record/1985-98423-000

Baxter, P., & Jack, S. M. (2015). Qualitative case study methodology: Study design and implementation for novice researchers. The Qualitative Report. https://doi.org/10.46743/2160-3715/2008.1573

BBC News. (2024, October 15). **AI and privacy: Balancing innovation with compliance**. Retrieved from https://www.bbc.com/news/articles/c93pz1dz2kxo

Burt, T. (2021, May 5). Microsoft report shows increasing sophistication of cyber threats. Microsoft on the Issues. https://blogs.microsoft.com/on-the-issues/2020/09/29/microsoft-digital-defense-report-cyber-threats/

Brandenburger, A. M., Nalebuff, B. J. (1998). Coopetition. Currency.

Brinkmann, S., & Kvale, S. (2014). InterViews: Learning the Craft of Qualitative Research Interviews. SAGE Publications, Incorporated.

Caron, F. (2019). Obtaining reasonable assurance of cyber resilience. Managerial Auditing Journal, 36(2), 193–217. https://doi.org/10.1108/maj-11-2017-1690

Cerra A (2019). The Cybersecurity Playbook: How Every Leader and Employee Can Contribute to a Culture of Security. John Wiley & Sons.

Chapter 4-Security Management, from Safeguarding Your Technology, NCES Publication 98-297 (National Center for Education Statistics). (n.d.). https://nces.ed.gov/pubs98/safetech/chapter4.asp

Chapter 5-Protecting Your System: Physical Security, from Safeguarding Your Technology, NCES Publication 98-297 (National Center for Education Statistics). (n.d.). https://nces.ed.gov/pubs98/safetech/chapter5.asp

Cisomag. (2021, April 7). Cybersecurity post-COVID: A new era of sophistication. *CISO MAG | Cyber Security Magazine*. https://cisomag.com/cybersecurity-post-covid/

Creswell, J. W., & Poth, C. N. (2017). Qualitative inquiry and research design: Choosing Among Five Approaches. Sage Publications, Incorporated.

Computer Security Resource Center (CSRC). (n.d.). Cybersecurity: Glossary. Retrieved from https://csrc.nist.gov/glossary/term/cybersecurity

Computer Security Resource Center (CSRC). (n.d.-a). Best Practice: Glossary. Retrieved from https://csrc.nist.gov/glossary/term/best_practice

Computer Security Resource Center (CSRC). (n.d.-b). Risk management: Glossary. Retrieved from https://csrc.nist.gov/glossary/term/risk_management

Computer Security Resource Center (CSRC). (n.d.-c). Risk Management Framework (RMF) Step: Glossary. Retrieved from https://csrc.nist.gov/glossary/term/risk_management_framework_step

Computer Security Resource Center (CSRC). (n.d.-d). Risk assessment: Glossary. Retrieved from https://csrc.nist.gov/glossary/term/risk_assessment

Computer Security Resource Center (CSRC). (n.d.-f). Sensitive information: Glossary. Retrieved from https://csrc.nist.gov/glossary/term/sensitive_information

Computer Security Resource Center (CSRC). (n.d.-g). Risk mitigation: Glossary. Retrieved from https://csrc.nist.gov/glossary/term/risk_mitigation

Computer Security Resource Center (CSRC). (n.d.-h). PII - Glossary. Retrieved from https://csrc.nist.gov/glossary/term/PII

CSRC Content Editor. (n.d.). *security posture - Glossary | CSRC*. https://csrc.nist.gov/glossary/term/security_posture

Cybersecurity Best Practices | Cybersecurity and Infrastructure Security Agency CISA. (n.d.). https://www.cisa.gov/topics/cybersecurity-best-practices

Cybersecurity | Homeland Security. (n.d.). https://www.dhs.gov/topics/cybersecurity

Cybersecurity Master's Degree | Online | NYU Tandon School of Engineering. (n.d.). https://engineering.nyu.edu/academics/programs/cybersecurity-ms-online

Cybersecurity and Infrastructure Security Agency. (2024). *Questions every CEO should ask about cyber risks*. U.S. Department of Homeland Security. https://www.cisa.gov/news-events/news/questions-every-ceo-should-ask-about-cyber-risks

Cyber insurance. (2021, November 9). Federal Trade Commission. https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/cyber-insurance

The Cyber Resilient Organization: Learning to Thrive against Threats: Ponemon Institute. (n.d.). Ponemon Institute. https://www.ponemon.org/research/ponemon-library/security/the-cyber-resilient-organization-learning-to-thrive-against-threats.html

Cyber Risk Monitoring | BitSight. (n.d.). Bitsight. https://www.bitsight.com/glossary/cyber-risk-monitoring

Cyber Skills for All: Community Colleges Lead the Way. (n.d.). https://www.aacc.nche.edu/programs/workforce-economic-development/cyber-skills-for-all/

Davis, F. D., Granic, A., & Marangunic, N. (2020). The Technology Acceptance Model: 30 Years of Tam. Springer.

Definition & Meaning Educational institution. (n.d.). https://www.dictionary.university/Educational%20institution

Dissent. (2020, August 12). *Imperial Valley College hit with ransomware attack; multiple systems impacted – DataBreaches.Net*. https://databreaches.net/2020/08/12/imperial-valley-college-hit-with-ransomware-attack-multiple-systems-impacted/

EDUCAUSE. (n.d.). https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/toolkits

Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? The Journal of Risk Finance, 17(5), 474–491. https://doi.org/10.1108/jrf-09-2016-0122

Griffith, M. K. (2022). Cyber security and emerging technologies. *Survival*, *64*(5), 174–180. https://doi.org/10.1080/00396338.2022.2126189

Force, J. T. (2018). *Risk management framework for information systems and organizations:* https://doi.org/10.6028/nist.sp.800-37r2

Franzke, A. S., Muis, I., Schäfer, M. (2021). Data Ethics Decision Aid (DEDA): a dialogical framework for ethical inquiry of AI and data projects in the Netherlands. Ethics and Information Technology, 23(3), 551–567. https://doi.org/10.1007/s10676-020-09577-5

What is FERPA? | Protecting Student Privacy. (n.d.). https://studentprivacy.ed.gov/faq/what-ferpa

Fujs, D., Mihelič, A., & Vrhovec, S. (2019). The power of interpretation. The Power of Interpretation: Qualitative Methods in Cybersecurity Research. https://doi.org/10.1145/3339252.3341479

Hale, C. (2024, September 20). CrowdStrike outage is causing businesses to switch security vendors. *TechRadar*. https://www.techradar.com/pro/security/crowdstrike-outage-is-causing-businesses-to-switch-security-vendors

Holistic IT governance, risk management, security and privacy: needed for effective implementation and continuous improvement. (n.d.). ISACA. https://www.isaca.org/resources/isaca-journal/issues/2016/volume-5/holistic-it-governance-risk-management-security-and-privacy-needed-for-effective-implementation-and

Hornetsecurity. (2024, September 6). *Immutable Backups Explained – Why are immutable backups critical - HornetSecurity – Next-Gen Microsoft 365 Security*. Hornetsecurity – Next-Gen Microsoft 365 Security. https://www.hornetsecurity.com/en/blog/immutable-backups-explained/

Information technology security risk management - ProQuest. (n.d.). https://www.proquest.com/dissertations-theses/information-technology-security-risk-management/docview/304954702/se-2

Insurance Circular Letter No. 2 (2021): Cyber Insurance Risk Framework. (n.d.). Department of Financial Services. https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2021_02

ISO/IEC JTC 1/SC 27 - Information security, cybersecurity and privacy protection. (2023, February 2). ISO. https://www.iso.org/committee/45306.html

Keskin, O. F., Caramancion, K. M., Tatar, I., Raza, O., & Tatar, U. (2021). Cyber Third-Party Risk Management: A Comparison of Non-Intrusive Risk Scoring Reports. Electronics, 10(10), 1168. https://doi.org/10.3390/electronics10101168

Krippendorff, K. (2013). Content analysis: An Introduction to Its Methodology. SAGE.

Krueger, R. A., & Casey, M. A. (2014). Focus groups: A Practical Guide for Applied Research. SAGE Publications, Incorporated.

Kruk, M. E., Gage, A. D., Arsenault, C., Jordan, K., Leslie, H. H., Roder-DeWan, S., Adeyi, O., Barker, P. M., Daelmans, B., Doubova, S. V., English, M., Garcia-Elorrio, E., Guanais, F. C., Gureje, O., Hirschhorn, L. R., Jiang, L., Kelley, E. F., Lemango, E. T., Liljestrand, J.,... Pate, M. (2018). High-quality health systems in the Sustainable Development Goals era: time for a revolution. The Lancet Global Health, 6(11), e1196–e1252. https://doi.org/10.1016/s2214-109x(18)30386-3

Landoll, D. J. (2020). Information Security Policies, Procedures, and Standards: A Practitioner's Reference. Auerbach Publications.

RWJF - Qualitative Research Guidelines Project | Lincoln & Guba | Lincoln and Guba's Evaluative Criteria. (n.d.). http://www.qualres.org/HomeLinc-3684.html

MarkSimos. (2021, December 13). Microsoft Cybersecurity Reference Architectures - Security documentation. Microsoft Learn. https://learn.microsoft.com/en-us/security/cybersecurity-reference-architecture/mcra

MAYOUNGA, A. T. (2017). Mitigating Supply Chain Disruptions, Risks, and Vulnerabilities. https://digitalcommons.liberty.edu/cgi/viewcontent.cgi?article=4729&context=doctoral

Mohajeryami, S., PhD. (2023, January 9). SecOps Engineering Interview Questions: The Top 25 - Saeed Mohajeryami, PhD. Medium. https://techleadcuriosity.com/secops-engineering-interview-questions-the-top-25-ea2a818f89f2

Musser, M., & Garriott, A. (2021). Machine learning and **cybersecurity: Hype and reality**. Center for Security and Emerging Technology. Retrieved from https://cset.georgetown.edu/wp-content/uploads/Machine-Learning-and-Cybersecurity.pdf

New Cybersecurity Resources for Institutes of Higher Education Available | Knowledge Center. (2023, February 16). https://fsapartners.ed.gov/knowledge-center/library/electronic-announcements/2023-02-16/new-cybersecurity-resources-institutes-higher-education-available

NIST. (n.d.). NIST Risk Management Framework | CSRC | CSRC National Institute of Standards and Technology at the U.S. Department of Commerce. https://csrc.nist.gov/projects/risk-management/about-rmf

National Institute of Standards and Technology. (2024). *Cybersecurity Framework update fact sheet*. U.S. Department of Commerce. https://www.nist.gov/system/files/documents/2022/10/03/NIST_CSF_update_Fact_Sheet.pdf

National Institute of Standards and Technology (NIST)**. (n.d.).** NIST Risk Management Framework**.** Computer Security Resource Center (CSRC). Retrieved from https://csrc.nist.gov/projects/risk-management/about-rmf

NIST Risk Management Framework | CSRC. (n.d.). https://csrc.nist.gov/projects/risk-management/about-rmf

Office of Inspector General (OIG)**.** (2022, October). **Report OIG-23-01**. Department of Homeland Security. Retrieved from https://www.oig.dhs.gov/sites/default/files/assets/2022-11/OIG-23-01-October22.pdf

Orlando, A. (2021**).** Cyber risk quantification: Investigating the role of cyber value at risk**.**

Perna, M. (2024, October 1). Is AI making work better or worse? Forbes. Retrieved from https://www.forbes.com/sites/markcperna/2024/10/01/aiis-ai-making-work-better-or-worse/

Pfeffer, J., & Salancik, G. R. (2003). The External Control of Organizations: A Resource Dependence Perspective. Stanford University Press.

Rampin, R., & Rampin, V. (n.d.). **Taguette: The free and open-source qualitative data analysis tool**. Retrieved from https://www.taguette.org/

Risks. (2021). Cybersecurity threats and risk management**.** *Risks*, 9(10), 184. https://doi.org/10.3390/risks9100184

Selman, H. (2022, June 3). What is data redundancy? - Dataconomy. Dataconomy. https://dataconomy.com/2022/03/09/what-is-data-redundancy/

Senthilkumar, K., & Easwaramoorthy, S. (2017). A Survey on Cyber Security awareness among college students in Tamil Nadu. IOP Conference Series, 263, 042043. https://doi.org/10.1088/1757-899x/263/4/042043

Shackelford, S., Proia, A. A., Martell, B., & Craig, A. J. (2014). Towards a Global Cybersecurity Standard of Care? Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices. Social Science Research Network. https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2465926_Institution Ae410303.pdf?abstractid=2446631&mirid=1

Snavely, D. (2023). Rapid estimation for cyber insurance premium pricing for company decision-makers (Order No. 30001169). Available from ProQuest Central. (2753318350). Retrieved from https://er.lib.k-state.edu/login?url=https://www.proquest.com/dissertations-theses/rapid-estimation-cyber-insurance-premium-pricing/docview/2753318350/se-2

Spitzner, L. (2022, February 25). 2023 SANS Report: The State of MDR | SANS Institute. https://www.sans.org/white-papers/2023-sans-report-state-mdr/

Stahl, J. (2023, March 24). *College of the Desert paid $1.1M to hackers in 2020 ransomware attack, doing more now to cyber safeguard its IT systems - KESQ*. KESQ. https://kesq.com/news/i-team/2023/03/18/college-of-the-desert-paid-1-1m-to-hackers-in-2020-ransomware-attack-doing-more-now-to-cyber-safeguard-its-it-systems/

Stouffer, K. A., Falco, J. A., & Scarfone, K. A. (2015). NIST Special Publication 800-82 Revision 2. Guide to Industrial Control Systems (ICS) Security. https://doi.org/10.6028/nist.sp.800-82r2

Tabassi, E. (2023). A Taxonomy and Terminology of Adversarial Machine Learning. Adversarial Machine Learning a Taxonomy and Terminology of Attacks and Mitigations. https://doi.org/10.6028/nist.ai.100-2e2023.ipd

Table of Contents - NSCAI Final report. (n.d.). https://reports.nscai.gov/final-report/

Rampin, R., & Rampin, V. (n.d.). *Taguette, the free and open-source qualitative data analysis tool*. https://www.taguette.org/

What happened in the Ohio State University data breach? | Twingate. (n.d.). https://www.twingate.com/blog/tips/ohio-state-university-data-breach

What is Higher Education Institution | IGI Global. (n.d.). https://www.igi-global.com/dictionary/higher-education-institution/13096

Wazuh. (n.d.). Getting started with Wazuh · Wazuh documentation. https://documentation.wazuh.com/current/getting-started/index.html

Woods, D., Agrafiotis, I., Nurse, J. R. C., & Creese, S. (2017). Mapping the coverage of security controls in cyber insurance proposal forms. Journal of Internet Services and Applications, 8(1). https://doi.org/10.1186/s13174-017-0059-y

What is XDR? | Microsoft Security. (n.d.). https://www.microsoft.com/en-us/security/business/security-101/what-is-xdr

Xie, X., Lee, C., & Eling, M. (2020). Cyber insurance offering and performance: an analysis of the U.S. cyber insurance market. Geneva Papers on Risk and Insurance-Issues and Practice, 45(4), 690–736. https://doi.org/10.1057/s41288-020-00176-5

Yazan, B. (2015). Three Approaches to Case Study Methods in Education: Yin, Merriam, and Stake. The Qualitative Report. https://doi.org/10.46743/2160-3715/2015.2102

Yeo & Yeo. (2023, January 6). Are Federal Government Backstops the Answer to Rising Cyber Insurance Costs? Yeo And Yeo. https://www.yeoandyeo.com/resource/are-federal-government-backstops-the-answer-to-rising-cyber-insurance-costs

Yin, R. K. (2017). Case study research and applications: Design and Methods. SAGE Publications, Incorporated.

Zhang, D. (2022, October 7). As Cyber Insurance Dries Up, Treasury Department Eyes a Backstop. https://news.bloomberglaw.com/insurance/as-cyber-insurance-dries-up-treasury-department-eyes-a-backstop

Appendix A - Charts and Data

Table 1 Research Design and Methodology

Aspect	Qualitative Case Study Research Design	NIST CSF 2.0 Risk Management Methodology	HEISC Cybersecurity Framework
Nature and Purpose	Explores complex phenomena in real-life contexts, focusing on in-depth understanding through interviews and document analysis.	A structured approach to identifying, assessing, responding to, financing, and monitoring cyber risks.	Tailored cybersecurity guidance for higher education, setting standards and best practices.
Application in Research	Examines risk management processes in U.S. colleges, exploring their reliance on cybersecurity insurance and external resources.	Guides the systematic analysis of cybersecurity risks and informs the development of risk management strategies in the case study.	Assesses the effectiveness' and appropriateness of cybersecurity measures in educational contexts, informing policy and practice.
Contribution to Study	Provides a comprehensive, context-rich understanding of cybersecurity challenges and practices in U.S. colleges.	Offers a step-by-step framework for managing cyber risks, enhancing the rigor of risk analysis in the study.	Serves as a benchmark for evaluating cybersecurity efforts, aligning them with the unique needs of educational institutions.
Outcome	Aids in identifying themes and patterns related to cybersecurity risk management, informing best practices and policy recommendations.	Facilitates effective management of cyber risks, potentially preventing and mitigating cyber incidents.	Guides decision-making and policy formulation in educational institutions, ensuring tailored and effective cybersecurity strategies.

Appendix A Figure A.1

Table 2 Conceptual framework alignment and explanations.

NIST CSF 2.0	Conceptual Framework	Alignment	Explanation	HEISC Cybersecurity Framework Alignment
Risk Identification	Protection against potential cyber threats	High	US Colleges use cybersecurity insurance to identify and protect against potential cyber threats, thereby reducing their risk exposure.	Identifying and defining cybersecurity policies and procedures
Risk Analysis	Reduction of financial and reputational risks	High	By purchasing cybersecurity insurance, U.S. colleges aim to reduce the financial and reputational consequences that a successful cyber-attack could bring.	Assessing the current cybersecurity posture and vulnerabilities
Risk Control	Minimization of the likelihood and impact of cyber risks	High	Cybersecurity insurance provides resources and support to help U.S. colleges control and minimize the likelihood and impact of cyber risks.	Implementing safeguards and measures to control risks
Risk Financing	Provision of financial protection when a cyber risk occurs	High	Cybersecurity insurance provides financial protection if a cyber-attack helping to mitigate the financial consequences of such an event.	Funding and budgeting for cybersecurity measures
Risk Monitoring	Continual evaluation and adjustment of cyber risk management strategies	Medium	The continual monitoring of the U.S. college's cyber risk environment allows for the adjustment of policies and strategies as necessary to ensure that the college is well-protected against new and evolving cyber threats.	Continuous monitoring and updating of cybersecurity policies and procedures

Appendix A Table A.2

Table 3.1 Presents Linking Research Questions to Data Analysis Strategies.

Research Question	Theoretical Frameworks	Conceptual Framework	Data Sources	Data Collection Instruments
RQ1: What are the best practices in the U.S. college environment in the	TAM, Resource Dependency Theory	NIST CSF 2.0	Interviews with IT managers, cybersecurity officers;	Semi-structured Interviews, Document

use of security firms, third-party software, endpoints, and cybersecurity insurance, and what is their influence on the overall security posture of U.S. colleges?			Documents; Observations	Analysis, Observations
RQ2: What proven and effective cybersecurity practices or strategies should U.S. colleges adopt to enhance their security posture and protection?	Coopetition Theory, Social Cognitive Theory	NIST CSF 2.0	Interviews with Stakeholders; Training records; Policy documents; Observations	Semi-structured Interviews, Document Analysis, Observations

Appendix A Table A.3

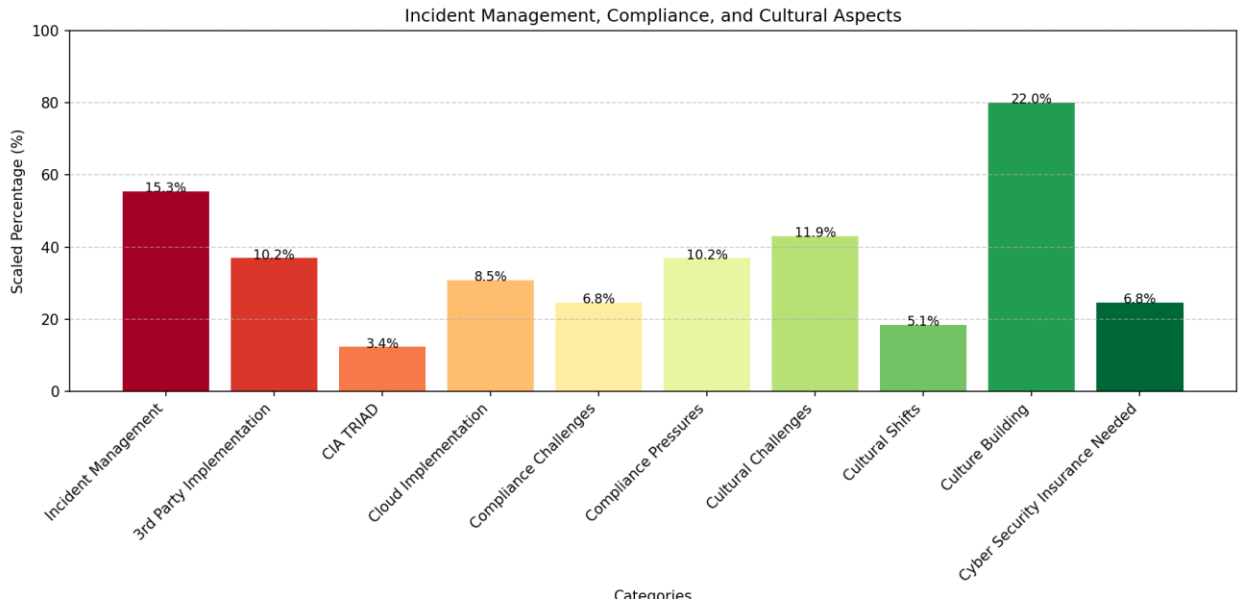

Figure 2 Incident Management, Compliance and Cultural Aspects

Appendix A Table A.4

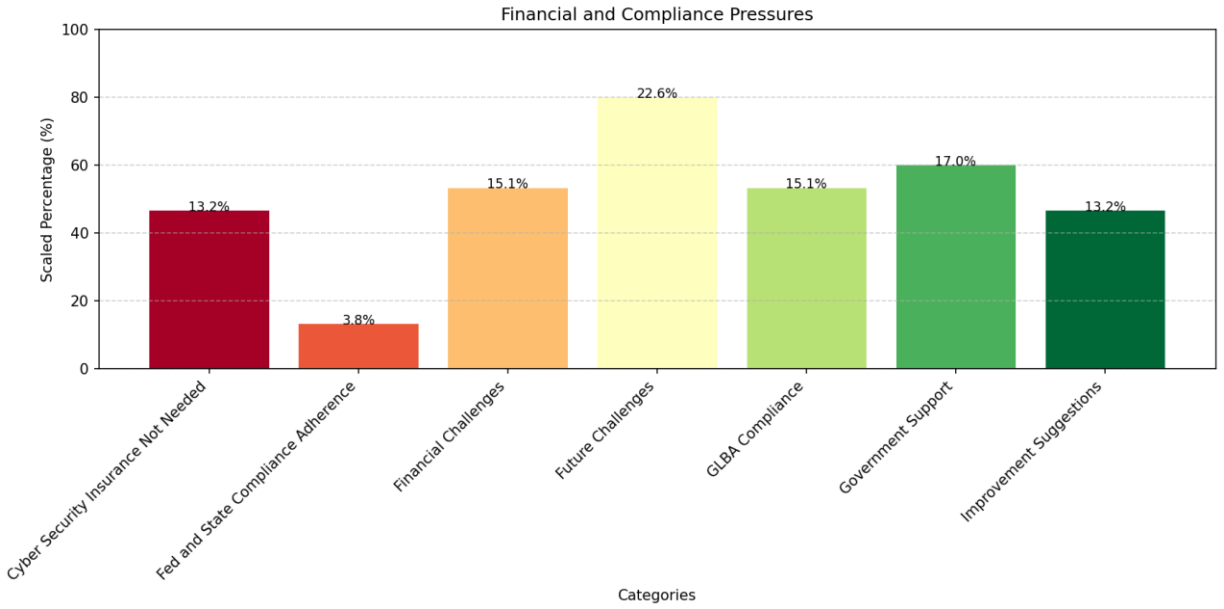

Figure 3 Financial and Compliance Pressures

Appendix A Table A.5

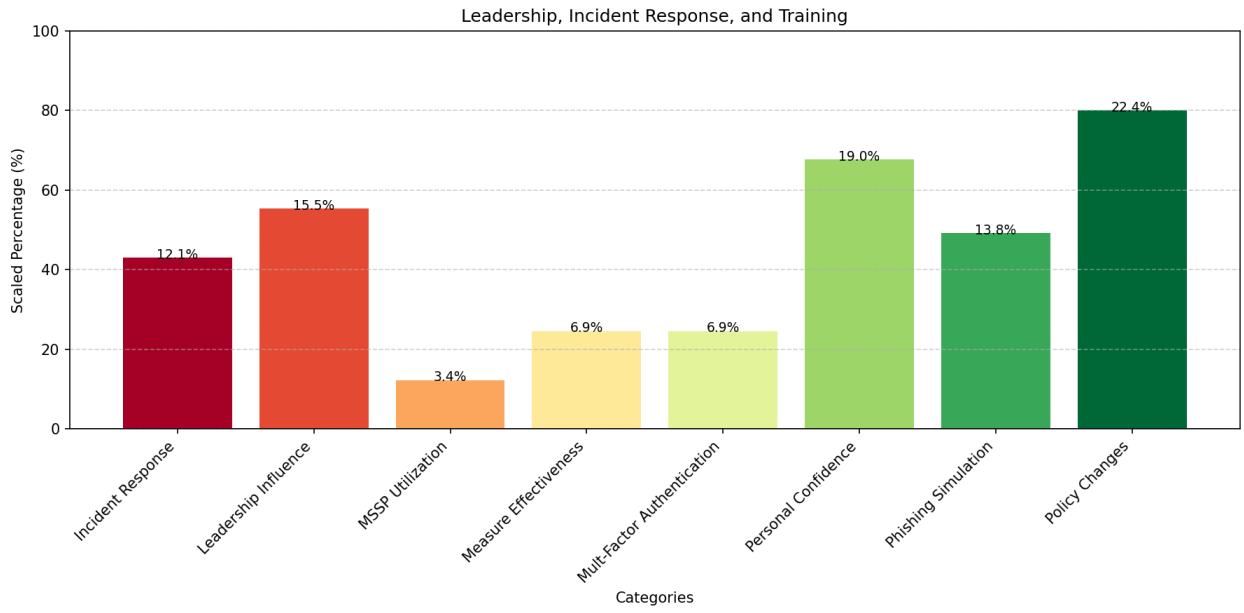

Figure 4 Leadership, Incident Response and Training

Appendix A Table A.6

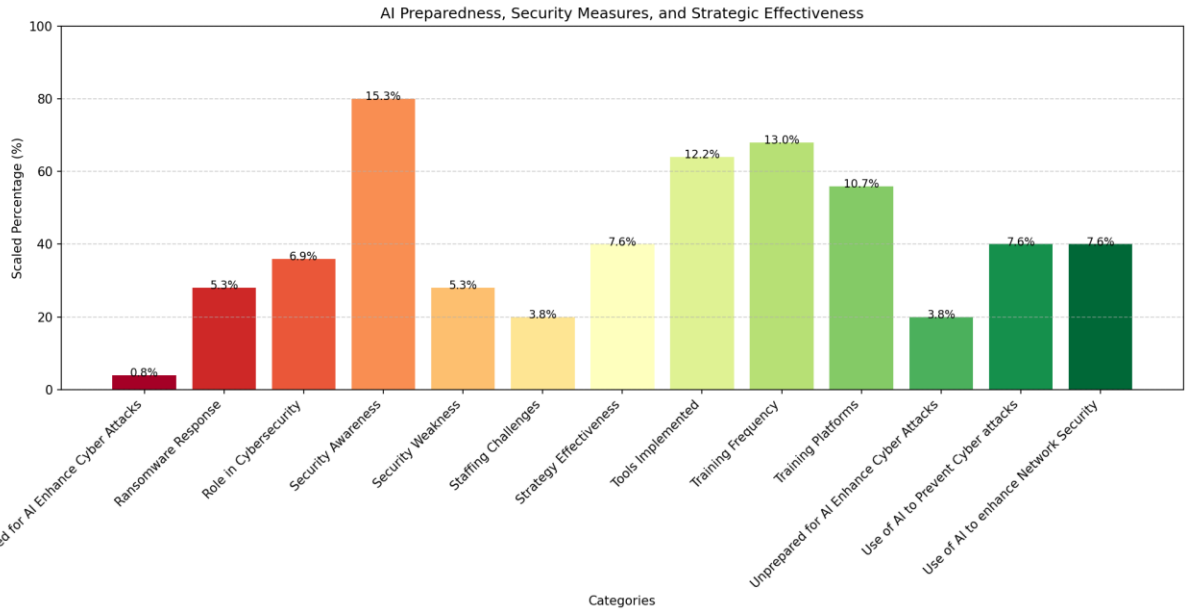

Figure 5 AI Preparedness, Security Measures and Strategic Effectiveness

Appendix A Table A.7

Appendix B - KSU IRB Approval

KANSAS STATE UNIVERSITY | University Research Compliance Office

TO: Terry Calaway
Educational Leadership

Proposal Number: IRB-11969

FROM: Lisa Rubin, Chair
Committee on Research Involving Human Subjects

DATE: 12/18/2023

RE: Proposal Entitled, "Paradigm-shifting back to the future: A revolutionary exploration in cybersecurity best practices for U.S. colleges."

The Committee on Research Involving Human Subjects / Institutional Review Board (IRB) for Kansas State University has reviewed the proposal identified above and has determined that it is EXEMPT from further IRB review. This exemption applies only to the proposal - as written – and currently on file with the IRB. Any change potentially affecting human subjects must be approved by the IRB prior to implementation and may disqualify the proposal from exemption.

Based upon information provided to the IRB, this activity is exempt under the criteria set forth in the Federal Policy for the Protection of Human Subjects, **45 CFR §104(d), category:Exempt Category 2 Subsection ii.**

Certain research is exempt from the requirements of HHS/OHRP regulations. A determination that research is exempt does not imply that investigators have no ethical responsibilities to subjects in such research; it means only that the regulatory requirements related to IRB review, informed consent, and assurance of compliance do not apply to the research.

Any unanticipated problems involving risk to subjects or to others must be reported immediately to the Chair of the Committee on Research Involving Human Subjects, the University Research Compliance Office, and if the subjects are KSU students, to the Director of the Student Health Center.

Electronically signed by Lisa Rubin on 01/03/2024 12:07 AM ET

203 Fairchild Hall, Manhattan, KS 66502 | (785) 532-3224 | fax: (785) 532-3278

Appendix C - Letter of Consent

Email

Greetings,

Thank you for the interest in participating in my study. Please review the info below:

--Informed Consent--

Researcher and Study is conducted by Jim M. Lilly of Kansas State University Doctoral student under the guidance of Dr. Terry Calaway.

Title of Research:

Paradigm-shifting back to the future: A revolutionary investigation in cybersecurity best practices for U.S. colleges.

What is the study about?

This study investigates best practices in cybersecurity standards adopted by community colleges, focusing on security firms, third-party software, endpoints, and cybersecurity insurance. It aims to evaluate the effectiveness of various cybersecurity measures in mitigating risks and vulnerabilities, including the role of security firms and the efficacy of endpoint solutions.

What will be asked of me?

Initially, you will receive an email containing a set of qualitative questions regarding your institution's cybersecurity practices. These questions are designed to gather detailed insights into your experiences and perspectives. After you have responded to these initial questions, a second set of follow-up questions will be sent to further explore specific areas based on your initial responses. Following this, you will be invited to participate in a follow-up interview via Zoom, which will last approximately 30 minutes. This interview will involve both video and audio recordings and will delve deeper into certain topics based on your responses to the initial and follow-up questions. The purpose of this interview is to clarify, expand upon, and discuss in more depth the topics covered in your written responses. Please be assured that no sensitive or highly personal questions will be asked. After the interview, you will receive a summary of the findings for your comments and corrections.

Who is involved?

The research is conducted by Jim Lilly, a doctoral candidate at Kansas State University.

Are there any risks?

Minimal risk is involved. You will discuss topics related to cybersecurity practices. Sensitive or proprietary information will not be requested. You have the right to skip any uncomfortable questions or withdraw at any time. All information will be handled confidentially to protect personal and institutional reputations.

What are some benefits?

No direct benefits for participants. Your insights will enhance the understanding of cybersecurity practices in community colleges and may benefit your institution by providing access to study findings, offering insights into best practices and approaches in cybersecurity.

Is the study anonymous/confidential?

Your participation is confidential. Interviews will be conducted with cameras off, and no personally identifying information linking you to your answers will be used.

How will the data collected in the study be protected?

Data will be stored on a multi-factor authentication password-protected laptop and an offline USB drive accessible only via biometrics.

Can I stop participating in the study?

You can withdraw from the study at any time without penalty.

Disclosure Statement:

The researcher is an Information Security Officer and a classified professional staff member at a College of the Desert.

What if I have questions about my rights as a research participant or complaints?

Contact Lisa Rubin, Chair, Committee on Research Involving Human Subjects, 203 Fairchild Hall, Kansas State University, Manhattan, KS 66506, Phone: (785) 532-3224.

Consent Form: To access, click IVC

I will send the password for the form separately via email once you have confirmed the receipt of this email. Once filled out, please upload your signed consent form with your first initial and last name. I will then send out your first round of questions.

IRB CONSENT FORM

PURPOSE OF THE RESEARCH:
This study aims to explore and evaluate cybersecurity practices in U.S. colleges, focusing on the effectiveness of various measures such as third-party applications, internal policies, AI, and cybersecurity insurance. Using a qualitative multi-case study approach, the research will involve interviews with IT managers, cybersecurity officers, and faculty from selected colleges. The study seeks to understand how these institutions manage cybersecurity risks and their reliance on external resources. The findings are expected to improve cybersecurity strategies in the higher education sector.

PROCEDURES OR METHODS TO BE USED:
The study will employ a qualitative multi-case study design involving semi-structured interviews with key stakeholders in U.S. colleges. Participants will be selected based on their role in managing cybersecurity.

Data will be analyzed using thematic analysis to identify patterns and themes related to cybersecurity practices.

AUDIO RECORDING OF INTERVIEWS:
As part of this research study, audio-recorded interviews will ensure data collection and analysis accuracy. These recordings will be used solely for this research. All audio recordings will be handled with strict confidentiality. Only the research team will have access to these recordings, which will be securely stored in encrypted digital formats.

Participants have the right to request that the recording be stopped during the interview. They also have the option not to be recorded, though their participation in the interview is still highly valued. All recordings will be destroyed at the end of the study, following the data analysis phase, to maintain the privacy and confidentiality of the participants.

RISKS OR DISCOMFORTS ANTICIPATED:
In this study, there are minimal risks associated with participation. These may include the potential for a breach of confidentiality and the discomfort of discussing sensitive topics related to cybersecurity practices. However, all necessary precautions will be taken to minimize these risks, including secure data handling and anonymization of participant information.

STATEMENT OF FUTURE USE OF DATA:
Data collected in this study may be used for future research purposes. However, any future use will be devoid of personal identifiers to ensure ongoing confidentiality. Participants' consent for such use is implied by their participation in the current study, and they have the right to withdraw consent at any time.

EXTENT OF CONFIDENTIALITY:
Confidentiality of participant information will be strictly maintained. Data will be stored securely in encrypted digital formats, accessible only to the research team. Identifiable information will be removed from the dataset, and all data will be retained for a period of three years post-study, after which it will be securely destroyed. Participants' identities will not be disclosed in any reports or publications resulting from this study.

IS COMPENSATION OR MEDICAL TREATMENT AVAILABLE IF INJURY OCCURS?
☐ Yes ☒ No

TERMS OF PARTICIPATION:
I understand this project is research, and that my participation is voluntary. I also understand that if I

decide to participate in this study, I may withdraw my consent at any time, and stop participating at any time without explanation, penalty, or loss of benefits, or academic standing to which I may otherwise be entitled.

I verify that my signature below indicates that I have read and understand this consent form, and willingly agree to participate in this study under the terms described. My signature also acknowledges that I have received a signed and dated copy of this consent form.

Appendix D - Informed Consent

PARTICIPANT NAME: _____

PARTICIPANT SIGNATURE: _____

DATE: _____

WITNESS TO SIGNATURE (PROJECT STAFF): _____

DATE: _____

PROJECT TITLE:
Paradigm-shifting back to the future: Evolutionary vs. Revolutionary Shifts in Cybersecurity Best Practices for U.S. Colleges

---

PROJECT APPROVAL DATE:
6/4/2023

PROJECT EXPIRATION DATE:
TBD

LENGTH OF STUDY:

PRINCIPAL INVESTIGATOR:
Terry Calaway

CO-INVESTIGATOR(S):
Jim Lilly

CONTACT DETAILS FOR PROBLEMS/QUESTIONS:
Phone: 442-241-5500

IRB CHAIR CONTACT INFORMATION:
Lisa Rubin, Chair, Committee on Research Involving Human Subjects
203 Fairchild Hall, Kansas State University
Manhattan, KS 66506
Phone: (785) 532-3224

Appendix E - Interview Questions

Appendix B.2:

Participant Questionnaire:

1. Please describe your role and responsibilities concerning cybersecurity risk management at your college.
2. How would you describe your college's current cybersecurity risk management strategy?
3. Could you discuss any significant changes in your college's cybersecurity practices over the past 5-10 years?
4. What challenges has your institution faced in implementing effective cybersecurity measures?
5. Can you share any specific incidents where cybersecurity breaches occurred and how the college handled them?
6. What are some of the strengths and weaknesses of your institution's current cybersecurity risk management practices?
7. How does your institution ensure continuous learning and improvement in its cybersecurity measures?
8. Can you share your thoughts on the future of cybersecurity in U.S. colleges?
9. In your opinion, what steps could U.S. colleges take to improve their cybersecurity practices?
10. Are there any other insights or experiences you would like to share regarding cybersecurity risk management in your institution?

Supplemental:

1. **General Information:**
    - What is your current position at your institution?
    - How long have you been in your current position?
    - How long have you been involved in cybersecurity risk management?
2. **Institutional Cybersecurity Practices:**
    - Discuss your perspective on the effectiveness of your institution's current cybersecurity measures?
    - What forms of cybersecurity training does your institution provide? (multiple options can be provided for the participant to select)
    - What changes, if any, have you observed in your institution's cybersecurity practices over time?
    - What challenges does your institution face in maintaining and improving cybersecurity?

3. **Personal Involvement and Perspectives:**
    - What role do you play in shaping or implementing cybersecurity measures at your institution?
    - How comfortable do you feel in your understanding of cybersecurity best practices?
    - Do you have any suggestions for improving the cybersecurity posture of U.S. colleges?

Second Round of Participant Questionnaire:

1. **Collaboration and Partnerships:**
    - Does your institution collaborate with other colleges, government agencies, or private entities in cybersecurity efforts? If so, how have these partnerships benefited your cybersecurity posture?
2. **Cybersecurity Culture and Awareness:**
    - How does your institution promote a culture of cybersecurity awareness among students and staff? Can you share an effective strategy or program you've implemented?
3. **Cyber Insurance:**
    - Could you elaborate on your institution's reliance on cybersecurity insurance? Do you find it beneficial, or are there aspects that you see as a hindrance? Please share specific experiences or examples that have shaped your views.
4. **Scenario-Based Question:**
    - Imagine a scenario where your college faces a sophisticated cyber-attack. What immediate steps would be taken by your team?
5. Comparative Analysis:
    - How do you perceive your cybersecurity practices compared to industry standards or practices at similar institutions?
6. **Future Trends and Adaptation:**
    - What emerging cybersecurity threats are you most concerned about for the future? How is your institution preparing to tackle these?
    - Considering the rise of AI-enhanced cyber threats, how prepared is your institution to tackle such sophisticated challenges and have you adopted specific measures or technologies to defend against AI-driven attacks?
7. **Suggestions for Improvement:**
    - Based on your experience, what key suggestions would you offer to other U.S. colleges looking to strengthen their cybersecurity frameworks?
    - Can you describe how AI is integrated into your cybersecurity operations? What specific roles does AI play in enhancing your institution's cybersecurity measures?