Quantitative Exploration of AI's Impact on Financial Cybersecurity: Trends, Data Privacy, and Human Expertise

Dissertation Manuscript

Submitted to National University

School of Technology and Engineering

In Partial Fulfillment of the

Requirements for the Degree of

DOCTOR OF PHILOSOPHY

by

TANYA R. STEWART

San Diego, California

March 2026

Acknowledgement

I would like to acknowledge my doctoral committee, Dr. Milton Kabia, Dr. Chris Schweigert, and Dr. William Souza. Your guidance, patience, and detailed feedback shaped every revision and pushed me to do better each time. I am truly grateful for the time and care you invested in my growth. To my husband, thank you for your unwavering support, encouragement, and constant belief in me, especially during the moments when this journey felt overwhelming and the finish line seemed out of reach. To my parents, thank you for listening to every update along the way and for always reminding me that I was capable and strong enough to succeed. Your words gave me confidence when I needed it most. To my siblings, thank you for cheering me on through every hurdle. Your encouragement never went unnoticed, and I carried it with me each time I sat down to work. To my friends, who are truly my chosen family, thank you for bringing me peace, laughter, and balance when I needed to step away and reset. Your support meant more than you know. To Dr. Galvao, thank you for creating a space where current and future students at National University could ask questions, find support, and feel less alone while balancing work and school. To the Tea family, thank you for sharing your experiences and wisdom. Your openness helped guide me through this journey. To Phillip Oels, thank you for believing in me and encouraging me to share my story with the university community on Facebook and LinkedIn. Your support gave me the confidence to use my voice.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction

Adopting artificial intelligence (AI) in cybersecurity practices has profoundly transformed the financial sector. As financial institutions become prime targets for cyber threats, they increasingly rely on AI-driven technologies to enhance security, mitigate risks, and ensure adherence to continuously evolving regulatory and compliance standards (Mishra, 2023). Among these challenges, data privacy has emerged as a crucial concern, as the integration of AI into cybersecurity requires the collection, processing, and analysis of large volumes of sensitive financial information. While AI has enhanced fraud detection, real-time threat intelligence, and automated incident response, it has raised significant concerns regarding regulatory compliance, data security, and the balance between automation and human oversight (Vial et al., 2024).

With the rapid digitization of financial services, AI has played a crucial role in protecting sensitive financial data, securing digital identities, and addressing sophisticated cyber threats (Binhammad et al., 2024). However, AI-driven cybersecurity models introduce privacy risks, including data breaches, unauthorized access, and potential misuse of personal financial information (Vial et al., 2024). Furthermore, the growing complexity of AI-based security mechanisms has posed challenges for ensuring transparency, accountability, and compliance with privacy regulations such as the General Data Protection Regulation (GDPR). In the U.S., commercial banks were subject to oversight by the Office of the Comptroller of the Currency (OCC) and the Federal Reserve, credit unions by the National Credit Union Administration (NCUA), investment banks by the Securities and Exchange Commission (SEC), and insurance companies by state insurance commissioners in coordination with the Federal Insurance Office (FIO). These regulators enforce unified cybersecurity and privacy standards through frameworks such as the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule and SEC Regulation S-P

(Baruwal Chhetri et al., 2024; Vial et al., 2024). These concerns underscore the need to comprehensively assess AI's impact on financial data privacy, particularly in balancing AI-driven automation and human decision-making and ensuring regulatory safeguards.

The increasing sophistication and scale of cyber threats further complicate data privacy management within financial institutions. AI-powered hacking techniques, deepfake fraud, and adversarial machine learning (ML) have been leveraged to bypass traditional security defenses (Todupunuri, 2023). Despite AI's advantages in cybersecurity, its application in financial data privacy has raised critical risks, including privacy breaches, biases in threat detection, regulatory noncompliance, and ethical concerns surrounding automated decision-making (Mishra, 2023).

The relevance of this study lies in its quantitative assessment of AI's impact on financial data privacy, focusing on emerging trends, regulatory challenges, and the role of human expertise in managing AI-driven cybersecurity. Although AI has demonstrated effectiveness in fraud detection and risk mitigation, its broader implications for governance, privacy, and workforce integration remain insufficiently quantified in empirical research (Udeh et al., 2024). Regulatory scrutiny has compelled financial institutions to ensure their AI-driven cybersecurity measures complied with data protection standards and ethical AI governance (R et al., 2023). Misalignment with obligations such as the GLBA Safeguards Rule, SEC S-P, or GDPR has led to penalties, reputational harm, and heightened exposure to breaches (Rana et al., 2023). This study explored these challenges through a quantitative approach, leveraging empirical data and statistical analysis to evaluate AI's role in financial data privacy, regulatory compliance, and the human-AI collaboration necessary for effective cybersecurity governance.

Prior research has extensively documented AI's role in cybersecurity threat intelligence, anomaly detection, and fraud prevention (Faraji et al., 2024). Artificial Intelligence-driven

security models have significantly enhanced financial institutions' ability to detect and mitigate threats in real-time by leveraging machine learning algorithms to analyze vast volumes of data and identify suspicious patterns (Todupunuri, 2023). While existing research has highlighted AI's technical capabilities in cybersecurity, it lacks a comprehensive examination of AI's dynamic implications for financial data privacy, particularly with respect to regulatory compliance and the ethical use of automated security measures (Vial et al., 2024). Prior studies have explored adversarial ML, in which AI-generated cyberattacks deceive fraud detection systems by subtly altering transactional data, and have demonstrated the necessity of AI models that not only detect threats but also continuously evolve to counter adversarial techniques (Faraji et al., 2024).

The dynamic nature of AI in cybersecurity extended beyond threat detection to its broader impact on regulatory frameworks and governance stability. Financial institutions are under growing pressure to align AI-driven cybersecurity measures with data privacy laws, such as the GDPR, and with evolving financial regulations in the U.S. and other jurisdictions (Udeh et al., 2024). However, the opacity of AI decision-making processes, often referred to as the "black box" problem, complicates regulatory oversight and raises concerns about transparency and accountability in automated security decisions (Vial et al., 2024). Studies on explainable AI (XAI) seek to address these concerns. Yet, financial institutions continue to struggle to implement AI models that balance predictive accuracy with interpretability (Mishra, 2023). Moreover, while AI automation enhanced efficiency, it disrupted traditional cybersecurity workflows, prompting questions about the role of human-AI collaboration in cybersecurity management. Research suggests that AI augmented, rather than replaced, human expertise. However, challenges persist in striking the optimal balance between human oversight and

automation in risk assessment, policy enforcement, and compliance auditing (Binhammad et al., 2024).

As AI continues to reshape cybersecurity in financial institutions, it was imperative to assess how these technologies aligned with data privacy regulations, cybersecurity policies, and human oversight mechanisms (Mishra, 2023). The adaptability of AI introduced challenges related to trust, transparency, compliance, and privacy protection, requiring ongoing refinement to governance structures and regulatory approaches (Udeh et al., 2024). The increasing reliance on AI underscored the growing complexity of integrating AI into financial cybersecurity, raising critical concerns about its compatibility with financial cybersecurity policies, the complexity of its adoption and oversight, and the relative advantage it confers over existing practices (Faraji et al., 2024). While AI has demonstrated immense potential to strengthen financial cybersecurity defenses, its full impact regarding privacy risks, ethical considerations, and regulatory compliance remains insufficiently quantified (Sontan et al., 2024).

This study explored these issues through a quantitative analysis of AI's impact on financial data privacy, regulatory compliance, and cybersecurity effectiveness (Mishra, 2023). By examining empirical data on AI-driven cybersecurity implementations, this research provided insights into how AI could be optimized to enhance privacy protections, support regulatory adherence, and balance automation with human oversight (Vial et al., 2024). Given ongoing advances in AI technology and its growing adoption in financial security infrastructure, this study contributed to the broader discourse on AI governance, addressing an urgent challenge in financial data protection and cybersecurity risk management (Udeh et al., 2024). Ultimately, the findings served as a foundational reference for designing resilient, ethically sound, and regulation-aligned AI cybersecurity strategies in the financial sector.

Statement of the Problem

The problem addressed in this study was the increasing complexity of integrating AI into financial cybersecurity while ensuring regulatory compliance, protecting data privacy, and fostering effective human-AI collaboration (Faraji et al., 2024). Financial institutions relied on AI-driven cybersecurity for threat detection, fraud prevention, and risk mitigation (Faraji et al., 2024). However, challenges persisted in balancing AI automation with human expertise, maintaining regulatory compliance, and mitigating emerging cybersecurity risks.

A primary concern was AI's impact on data privacy and regulatory compliance. AI-driven cybersecurity processes handle large volumes of sensitive data, creating compliance challenges under international frameworks such as the GDPR and U.S. financial regulators. Commercial banks were regulated by the OCC and the Federal Reserve, credit unions by the NCUA, investment banks by the SEC, and insurance companies by state insurance commissioners in coordination with the FIO (Baruwal Chhetri et al., 2024; Vial et al., 2024). These regulators enforced cybersecurity obligations through measures such as the GLBA Safeguards Rule and SEC Regulation S-P. Misalignment between AI-driven practices and these requirements could result in penalties, reputational harm, and increased breach risk (Rana et al., 2023).

Another critical issue was the evolving role of human expertise in AI-driven cybersecurity. While AI enhanced efficiency, it affected decision-making processes, workforce adaptation, and governance strategies (Thapaliya, 2024). AI's lack of explainability further complicates oversight, increasing the risk of bias, false positives, and adversarial attacks (Udeh et al., 2024). Failure to address these challenges may result in ineffective AI adoption, regulatory

non-compliance, and cybersecurity failures, ultimately jeopardizing institutional resilience and public trust.

Purpose of the Study

The purpose of this quantitative, correlational study was to examine the relationships among the compatibility, complexity, and relative advantage of AI-driven cybersecurity technologies, and their adoption and success in financial institutions. This study examined the impact of these factors on regulatory compliance, fraud prevention, and cybersecurity workforce augmentation (Binhammad et al., 2024). The research used a survey-based approach to collect data from cybersecurity professionals, IT managers, and compliance officers at financial institutions across the United States. An estimated 10,000 professionals met the inclusion criteria, based on industry workforce data from national financial services and cybersecurity workforce reports (Dawodu et al., 2023). Multivariate Analysis of Variance (MANOVA) was used to determine the required sample size, using the “F tests” and “MANOVA: Global effects” options in G*Power. The analysis employed a medium effect size ($f^2 = 0.15$), a significance level of 0.05 (5%), and a power of 0.80 (80%) to ensure statistical reliability. With three groups for the independent variable and four response variables, the total minimum required sample size was 57 participants.

The study utilized a structured questionnaire to measure perceptions of AI-driven cybersecurity tools and their impact on system performance, adaptability, regulatory compliance, and human-AI collaboration. The Technology Acceptance Model (TAM) and the Diffusion of Innovations (DOI) Theory served as the foundation for analyzing the extent to which financial institutions adopted AI for cybersecurity operations. Multiple regression analysis was used to assess the strength and significance of the relationships between independent variables'

compatibility, complexity, and relative advantage and the dependent variables, including system performance, adaptability, human-AI collaboration, and regulatory compliance.

Introduction to Theoretical Framework

The frameworks, the Technology Acceptance Model and Diffusion of Innovations, provide the theoretical foundation for this study, offering insights into the adoption and implementation of AI-driven cybersecurity technologies in financial institutions (Faraji et al., 2024). The TAM framework explained how users' perceptions of the technology's usefulness and ease of use shaped its acceptance, particularly in ensuring regulatory compliance and governance stability (Research Question 1) and enhancing organizational adaptability to cybersecurity challenges (Research Question 2) (Davis, 1989). This model highlighted how financial institutions assessed AI cybersecurity tools based on their integration capabilities within existing regulatory and security frameworks (Thapaliya, 2024).

On the other hand, the DOI theory examined how innovations spread within organizations and industries, emphasizing system performance, cybersecurity effectiveness (Research Question 3), and human-AI collaboration (Research Questions 3 and 4) (Mishra, 2023). The Diffusion of Innovations framework helped contextualize factors that drove AI adoption in cybersecurity, including compatibility with legacy systems, technological complexity, and perceived advantages in fraud prevention and threat mitigation (Sontan et al., 2024). In addition, DOI provided a lens to analyze how financial institutions weighed the risks and benefits of AI-driven cybersecurity for threat mitigation and fraud detection (Faraji et al., 2024). By integrating TAM and DOI, this study provided a structured evaluation of AI adoption in financial cybersecurity, identifying key drivers and barriers while ensuring regulatory compliance, operational balance, and long-term viability (Udeh et al., 2024). Together, these

frameworks explain both individual acceptance and organizational diffusion processes. Ultimately, this combined theoretical approach enabled a comprehensive understanding of the individual user's acceptance and the broader organizational diffusion of AI cybersecurity within the complex financial landscape (Sontan et al., 2024).

Table 1

Theoretical Frameworks and Variables

Theoretical Framework	Variable Type	Variable Name	Relationship	Key Influences
TAM	Independent	Compatibility	Positive	Regulatory mandates, org. size, cybersecurity maturity (Dawodu et al., 2023).
	Independent	Complexity	Initially Negative but positive over time	Workforce skills, guidance, AI training (Ebert et al., 2023).
	Dependent	Regulatory Compliance & Governance Stability	Positive	Oversight intensity, governance maturity (López González et al., 2024).
DOI	Independent	Relative Advantage	Strong Positive	Risk perception, anti-fraud (Paul et al., 2023).
	Dependent	Adaptability & Resilience	Moderate	AI fluency, training (Kaur et al., 2023).
	Dependent	System Performance & Cybersecurity Effectiveness	Strong Positive	Data quality, incident history (Javaheri et al., 2024).
	Dependent	Human-AI Collaboration & Job Satisfaction	Mixed	Culture, AI transparency, upskilling (Sontan et al., 2024)

Note. This table presents the key variables of the theoretical framework, highlighting their relationships and the external factors that affect the adoption and effectiveness of AI-driven cybersecurity technologies in financial institutions.

Introduction to Research Methodology and Design

This study employed a quantitative, correlational research design to examine the relationship between technology implementation (independent variable) and cybersecurity effectiveness (dependent variable) in financial institutions. The research assessed how compatibility, complexity, and relative advantages of AI-driven cybersecurity impacted regulatory compliance, fraud prevention, workforce decision-making, and system adaptability (Ebert et al., 2023). The study aligned the problem statement, purpose, and research questions by providing empirical data on AI adoption in cybersecurity governance and risk management (Dawodu et al., 2023). A correlational design was chosen because it aligns with the study's focus on testing associations between measurable constructs, making it the best fit for addressing the research questions and directly supporting the purpose of examining how AI adoption influences institutional outcomes.

A survey-based data collection method targeted cybersecurity professionals, IT managers, and compliance officers in U.S. financial institutions. The structured survey included closed-ended questions that measured the effects of AI-driven cybersecurity on regulatory compliance, fraud prevention, decision-making, and system adaptability (Djenna et al., 2023). A purposive sampling strategy ensured participation from cybersecurity professionals directly involved in AI-driven security operations. Inclusion criteria required participants to be cybersecurity professionals, information technology managers, or compliance officers currently working in financial institutions within the United States and involved in cybersecurity or AI-related security processes. Individuals without cybersecurity or regulatory responsibilities within financial institutions were excluded from participation. The research did not use a random sampling method because the study required domain experts rather than a broad population

sample. The anticipated sample size was 57, determined using G*Power software to ensure statistical validity. Following survey distribution, a total of 90 valid responses were obtained and included in the final analysis, exceeding the minimum required sample size for statistical power. Regression analysis assessed relationships between AI adoption factors and cybersecurity effectiveness. Descriptive statistics summarized the dataset, while inferential statistics assessed the strength of the relationship (Rizvi, 2023).

The study population included professionals from commercial banks, investment firms, insurance companies, and fintech organizations. Given the sensitivity of cybersecurity data, Institutional Review Board (IRB) approval was obtained. To ensure confidentiality, the study did not collect personal or financial data. All responses were anonymized and securely stored. The researcher obtained institutional permissions before distributing the survey to ensure compliance with organizational policies and research guidelines. If necessary, the researcher worked with compliance departments to obtain approvals (Sontan et al., 2024). This study provided empirical insights into AI-driven cybersecurity adoption in financial institutions by employing a quantitative, correlational research design with a targeted sample and robust data security measures.

Table 2

Research Questions and Theoretical Frameworks' Variables Alignment

Theoretical Framework	Independent Variable	Dependent Variable	Associated Research Question
TAM	Technology Implementation	Regulatory Compliance & Governance Stability	RQ1
		Adaptability & Resilience	RQ2
DOI		System Performance & Cybersecurity Effectiveness	RQ3
		Human-AI Collaboration & Job Satisfaction	RQ3

Theoretical Framework	Independent Variable	Dependent Variable	Associated Research Question
		System Performance, Adaptability, Collaboration, Regulatory Compliance	RQ4

Note. The table highlights the study's focus on assessing AI adoption through key factors such as compatibility, complexity, and relative advantage, ensuring a structured investigation into the regulatory, operational, and workforce implications of AI-driven security measures.

Research Questions

RQ1

To what extent does the compatibility of AI-driven cybersecurity technologies with existing financial cybersecurity policies influence their implementation success, regulatory compliance, and data privacy protection?

RQ2

To what extent does the complexity of AI-driven cybersecurity technologies impact their adoption in financial institutions, considering regulatory compliance, cybersecurity workforce adaptation, and data privacy management?

RQ3

To what extent do the relative advantages of AI-driven cybersecurity technologies influence adoption rates in financial institutions, particularly in improving threat detection, fraud prevention, and workforce decision-making capabilities?

RQ4

To what extent do compatibility, complexity, and relative advantage collectively impact the adoption and success of AI-driven cybersecurity technologies in financial institutions,

particularly in regulatory compliance, fraud prevention, and cybersecurity workforce augmentation?

Hypotheses

$H1_0$

The compatibility of AI-driven cybersecurity technologies with existing financial cybersecurity policies does not significantly influence their implementation success, regulatory compliance, and data privacy protection in financial institutions.

$H1_a$

The compatibility of AI-driven cybersecurity technologies with existing financial cybersecurity policies significantly influences their implementation success, enhances regulatory compliance, and strengthens data privacy protection in financial institutions.

$H2_0$

The complexity of AI-driven cybersecurity technologies does not significantly impact their adoption in financial institutions, considering regulatory compliance, cybersecurity workforce adaptation, and data privacy management.

$H2_a$

The complexity of AI-driven cybersecurity technologies significantly impacts their adoption in financial institutions, considering regulatory compliance, cybersecurity workforce adaptation, and data privacy management.

$H3_0$

The relative advantages of AI-driven cybersecurity technologies do not significantly influence adoption rates in financial institutions, particularly in improving threat detection, fraud prevention, and workforce decision-making capabilities.

$H3_a$

The relative advantages of AI-driven cybersecurity technologies significantly influence adoption rates in financial institutions, particularly in improving threat detection, fraud prevention, and workforce decision-making capabilities.

$H4_0$

Compatibility, complexity, and relative advantage collectively do not significantly impact the adoption and success of AI-driven cybersecurity technologies in financial institutions, particularly in regulatory compliance, fraud prevention, and cybersecurity workforce augmentation.

$H4_a$

Compatibility, complexity, and relative advantage collectively significantly impact the adoption and success of AI-driven cybersecurity technologies in financial institutions, particularly in regulatory compliance, fraud prevention, and cybersecurity workforce augmentation.

Significance of the Study

This study was critical as it addressed the challenges of integrating AI-driven cybersecurity technologies into financial institutions while ensuring data privacy, regulatory compliance, and effective human-AI collaboration (Faraji et al., 2024). As financial organizations adopted AI-powered security measures for fraud prevention and threat detection, transparency, governance, and compliance concerns persisted (Udeh et al., 2024). By examining how compatibility, complexity, and relative advantage influenced AI adoption in financial cybersecurity, this research contributed to the field of data science, particularly in AI-driven risk management and compliance frameworks (Mishra, 2023).

This study provided insight into the governance challenges and operational risks associated with implementing AI in cybersecurity for leaders and practitioners. Understanding AI's role in regulatory adherence, fraud prevention, and workforce augmentation enabled decision-makers to develop strategies that enhanced security while mitigating privacy risks (Sontan et al., 2024). The findings also helped policy regulators refine AI governance models to ensure compliance with GDPR, SEC regulations, and the supervisory oversight of the OCC, the Federal Reserve, the NCUA, and the FIO. In addition, the study acknowledged the influence of complementary standards, including the CCPA and PCI-DSS, which continue to shape institutional data privacy and security practices. Using a quantitative research design, this study applied data science methodologies to analyze AI adoption patterns and their impact on financial data privacy (Javaheri et al., 2024). Unlike prior studies focused on AI's technical capabilities, this research systematically evaluated AI's interaction with governance policies and cybersecurity regulations (Ebert et al., 2023). Ultimately, the findings helped financial institutions develop risk-based AI cybersecurity strategies that enhanced security while maintaining legal and ethical compliance. This research advanced AI-driven cybersecurity governance by addressing key challenges in financial data privacy, regulatory compliance, and risk management.

Definitions of Key Terms

Adversarial Machine Learning

A cybersecurity challenge where attackers manipulate AI models to bypass security defenses, evade fraud detection, or exploit vulnerabilities. Attackers use data poisoning, model inversion, and adversarial perturbations to deceive AI-based security systems. To

counter these threats, financial institutions must invest in robust AI model training, adversarial testing, and security-enhanced ML techniques (Todupunuri, 2023).

AI-Driven Cybersecurity

The application of artificial intelligence enhances cybersecurity operations, focusing on threat detection, fraud prevention, and risk mitigation. These systems employ machine learning algorithms to process and interpret extensive datasets of transactional information, identifying patterns, detecting anomalies, and predicting potential cyber threats before they emerge. Additionally, AI-powered solutions integrate automated incident response mechanisms, accelerating threat mitigation and bolstering the financial sector's overall resilience (Thapaliya, 2024).

Cybersecurity Governance and Risk Management

The policies and frameworks align AI cybersecurity strategies with regulatory standards and organizational risk management. Governance models ensure that AI security solutions comply with the industry’s best practices, ethical considerations, and evolving cyber threats. A risk management approach must incorporate AI-driven analytics, continuous threat assessment, and compliance auditing to mitigate financial cybersecurity risks effectively (Vial et al., 2024).

Data Privacy Protection

The strategies and technologies designed to secure financial data, prevent breaches, and maintain confidentiality within AI-driven cybersecurity systems. Artificial intelligence contributes to data privacy by implementing encryption and anonymization techniques while introducing risks associated with large-scale data collection and processing. Ensuring compliance with privacy regulations requires ongoing monitoring of AI

algorithms to mitigate unauthorized access, data leaks, and algorithmic biases (Vial et al., 2024).

Fraud Prevention and Detection

Fraud prevention and detection rely on artificial intelligence to detect and mitigate financial fraud, using advanced techniques such as machine-learning-powered anomaly detection and continuous, real-time monitoring. AI-driven fraud detection systems evaluate transaction patterns and behavioral data to identify suspicious activities, improving accuracy while reducing false positives. Additionally, AI continuously evolves to counter emerging fraud tactics, including synthetic identity fraud and deepfake-based financial scams, by updating detection models to address evolving threats (Mishra, 2023).

Human-AI Collaboration

The interaction between AI systems and cybersecurity professionals is crucial to balance automation with human oversight, decision-making, and risk assessment. Effective collaboration ensures that AI complements, rather than displaces, human expertise by generating actionable intelligence that supports security teams. Organizations must invest in workforce training and implement robust AI governance policies to maximize the collaboration between automation and human judgment in cybersecurity operations (Binhammad et al., 2024).

Regulatory Compliance

Regulatory compliance ensures that financial institutions adhere to governing mandates and legal frameworks, including those enforced by industry regulators and the OCC, Federal Reserve, NCUA, and FIO, as well as data protection laws such as the GDPR, GLBA Safeguards, and SEC S-P. These compliance mandates establish requirements for

safeguarding sensitive financial data and governing the integration of AI-based cybersecurity solutions. In addition, institutions must comply with secondary standards and laws such as the CCPA and PCI-DSS, which protect consumer privacy and payment security. Together, these compliance obligations require organizations to implement robust security controls, conduct periodic risk assessments, and ensure AI-driven cybersecurity tools align with data privacy and governance requirements. Noncompliance with these standards can lead to legal sanctions, reputational harm, and heightened financial exposure resulting from security breaches (Udeh et al., 2024).

Risk-Based AI Cybersecurity Strategies

Risk-based AI cybersecurity strategies use AI-driven methods to assess and prioritize cybersecurity risks in financial institutions. These strategies leverage machine learning algorithms to process and interpret real-time threat intelligence, detect high-risk vulnerabilities, and recommend proactive mitigation measures. Financial institutions can allocate resources efficiently by implementing risk-based AI security frameworks, addressing critical threats, and ensuring regulatory compliance and operational resilience (Udeh et al., 2024).

System Performance and Cybersecurity Effectiveness

The impact of AI-driven security tools on threat detection accuracy, fraud prevention efficiency, and incident response. AI enhances system performance by automating security monitoring, enabling real-time threat intelligence, and reducing response times to cyber incidents. Measuring the effectiveness of AI-driven security systems requires quantitative performance metrics such as detection rates, false positives, and response efficiency (Mishra, 2023).

Workforce Adaptation and Cybersecurity Skills Gap

Financial institutions face challenges in training professionals to work alongside AI-driven cybersecurity tools. As AI systems automate many cybersecurity functions, human professionals must develop new skills in interpreting AI models, ethical AI governance, and detecting adversarial threats. Organizations must implement continuous training programs and professional development initiatives to bridge the cybersecurity skills gap, ensuring that security teams can effectively manage and oversee AI-driven security operations (Faraji et al., 2024).

Summary

This prospectus examined the complexities of integrating AI into financial cybersecurity while ensuring regulatory compliance, data privacy, and effective human-AI collaboration. Although AI enhanced threat detection, fraud prevention, and risk mitigation, its adoption posed challenges for automation, governance, and regulatory compliance. The growing reliance on AI has raised concerns about transparency, ethical oversight, and the evolving role of human expertise in cybersecurity decision-making. Grounded in the Technology Acceptance Model and the Diffusion of Innovation Theory, this quantitative, correlational study investigated how compatibility, complexity, and relative advantage influenced the adoption and effectiveness of AI in financial institutions. Data from cybersecurity professionals were evaluated to assess AI's impact on system performance, adaptability, collaboration, and compliance, using multivariate and regression analysis. The findings provided empirical insights for financial institutions, policymakers, and cybersecurity leaders, offering strategies to optimize AI-driven cybersecurity frameworks while ensuring compliance with evolving regulations. By identifying best practices for AI governance and risk management, this study can help financial institutions enhance

cybersecurity resilience and assist policymakers in developing regulatory frameworks that foster innovation while ensuring robust security and ethical compliance. This study contributed to the ongoing discussion on AI governance, risk management, and the ethical considerations surrounding the adoption of AI in financial cybersecurity.

Chapter 2: Literature Review

The problem addressed in this study was the increasing complexity of integrating AI into financial cybersecurity while ensuring regulatory compliance, data privacy protection, and effective human-AI collaboration (Faraji et al., 2024). Financial institutions relied on AI-driven cybersecurity for threat detection, fraud prevention, and risk mitigation (Faraji et al., 2024). However, challenges persisted in balancing AI automation with human expertise, maintaining regulatory compliance, and mitigating emerging risks.

A primary concern was AI's impact on data privacy and regulatory compliance. AI-driven cybersecurity processes handle large volumes of sensitive data, creating compliance challenges under international frameworks such as the GDPR and U.S. financial regulators. Commercial banks are regulated by the OCC and the Federal Reserve, credit unions by the NCUA, investment banks by the SEC, and insurance companies by state insurance commissioners in coordination with the FIO (Baruwal Chhetri et al., 2024; Vial et al., 2024). These regulators enforced cybersecurity obligations through measures such as the GLBA Safeguards Rule and SEC Regulation S-P. Misalignment between AI-driven practices and these requirements could result in penalties, reputational harm, and an increased risk of breaches (Rana et al., 2023).

Another critical issue was the evolving role of human expertise in AI-driven cybersecurity. While AI enhanced efficiency, it affected decision-making processes, workforce adaptation, and governance strategies (Thapaliya, 2024). AI's lack of explainability further complicates oversight, increasing risks of bias, false positives, and adversarial attacks (Udeh et al., 2024). Failure to address these challenges could lead to ineffective AI adoption, regulatory

noncompliance, and cybersecurity failures, ultimately jeopardizing institutional resilience and public trust.

The purpose of this quantitative, correlational study was to examine the relationships between the compatibility, complexity, and relative advantage of AI-driven cybersecurity technologies, and their adoption and success in financial institutions. This study assessed how these factors influenced regulatory compliance, fraud prevention, and cybersecurity workforce augmentation (Binhammad et al., 2024). The research used a survey-based approach, collecting data from cybersecurity professionals, IT managers, and compliance officers at financial institutions across the United States. An estimated 10,000 professionals met the inclusion criteria, based on industry workforce data from national financial services and cybersecurity reports (Dawodu et al., 2023). Multivariate Analysis of Variance was used to determine the required sample size, with “F tests” and “MANOVA: Global effects” in G*Power determined the required sample size. The analysis used a medium effect size ($f^2 = 0.15$), a significance level of 0.05 (5%), and a power of 0.80 (80%) for statistical reliability. The total required sample size was 57 participants, with three groups for the independent variable and four response variables.

The study utilized a structured questionnaire to measure perceptions of AI-driven cybersecurity tools and their impact on system performance, adaptability, regulatory compliance, and human-AI collaboration. The TAM framework and the DOI Theory served as the foundation for analyzing the extent to which financial institutions adopted AI for cybersecurity operations. Multiple regression analysis was used to assess the strength and significance of the relationships between the independent variables' compatibility, complexity, and relative advantage and the dependent variables, including system performance, adaptability, human-AI collaboration, and regulatory compliance.

This chapter provided a comprehensive review of the current academic and industry discourse on AI in financial cybersecurity. The organization of the literature was categorized into six thematic subtopics: (1) History of AI, (2) AI-Driven Cybersecurity in Financial Institutions, (3) Compatibility of AI with Existing Cybersecurity Policies and Regulations, (4) Complexity of AI-Driven Cybersecurity and Its Impact on Adoption, (5) AI and Data Privacy Protection in Financial Institutions, and (6) Human-AI Collaboration in Financial Cybersecurity. Each section critically examined empirical studies and theoretical contributions related to the study's core constructs, identifying areas of convergence and divergence, as well as methodological gaps and conceptual limitations. This review laid the foundation for understanding the regulatory, operational, and organizational challenges associated with the adoption of AI technologies in financial cybersecurity governance.

Literature Search Strategies

A systematic literature search strategy was employed to target high-quality, peer-reviewed academic sources and authoritative industry publications relevant to cybersecurity, AI, financial institutions, and regulatory compliance. Databases accessed included *ProQuest, JSTOR, IEEE Xplore, Wiley Online Library, ScienceDirect*, and the *National University Library*. Additionally, Google Scholar and Mendeley (https://www.mendeley.com/search/) were utilized to supplement and cross-reference findings, ensuring comprehensive coverage of both academic and grey literature. From these sources, regulatory body reports were obtained, and government publications were consulted to provide critical context regarding data protection laws and compliance frameworks. Boolean logic (AND, OR, NOT) was combined with targeted keyword phrases such as: "*AI-driven cybersecurity*" AND "*financial institutions*," "*regulatory compliance*" AND "*data privacy*," "*Technology Acceptance Model*," AND "*AI adoption*," and

"*Diffusion of Innovations*" AND "*financial cybersecurity*." This structured approach enabled the precise identification of literature aligned with the study's core constructs.

Inclusion criteria were applied to select sources published between 2020 and 2025, emphasizing recency and relevance to ongoing developments in AI cybersecurity. Foundational theoretical works, particularly those informing the Technology Acceptance Model and the Diffusion of Innovations theory, were included regardless of publication date. In addition to scholarly journal articles, the search selected conference proceedings and emerging research articles, particularly from IEEE and related venues, to capture the latest advancements in AI and cybersecurity. Global perspectives were included, with no geographical restrictions, to reflect the international nature of financial cybersecurity developments. Industry and regulatory publications were retained when they provided insight into policy trends, governance requirements, and compliance frameworks. Studies were excluded if they focused on sectors other than finance, did not address AI integration in cybersecurity, or lacked empirical or theoretical contributions. Non-English sources and opinion-based content were also excluded unless peer-reviewed and formally translated.

Despite increasing attention to AI-powered cybersecurity tools, significant gaps remained in understanding how these technologies interact with compliance requirements, workforce dynamics, and ethical governance practices in real-world financial environments. Much of the existing literature has emphasized technical performance while overlooking the socio-technical and organizational implications of AI adoption in highly regulated industries. This review synthesized the current state of research and identified critical areas that remained underexplored, laying the groundwork for the present study's quantitative assessment of AI adoption drivers and outcomes in financial cybersecurity.

Theoretical Framework

This study employed a structured theoretical approach that incorporated both primary and supporting perspectives to examine the adoption of AI-driven cybersecurity technologies in financial institutions. The primary theoretical frameworks guiding the research were the TAM and the DOI theory, which together provided a multi-level perspective on technology adoption. TAM served as the primary user-centered framework, explaining how cybersecurity professionals' perceptions of usefulness and ease of use influenced their acceptance and use of AI-based tools. In contrast, DOI addressed organizational-level adoption processes by emphasizing attributes such as relative advantage, compatibility, and complexity that shape institutional decision-making. In addition to these primary frameworks, other theories, including Socio-Technical Systems Theory (STS) and the Unified Theory of Acceptance and Use of Technology (UTAUT), were reviewed as complementary frameworks given their relevance to prior technology and cybersecurity research. However, they were not selected because they did not align with the study's variables and methodological scope. Finally, contrasting frameworks such as Institutional Theory and the Theory of Planned Behavior (TBD) were considered but excluded, as they emphasized external pressures, normative influences, or motivational factors rather than the perceived technological characteristics central to this study. Collectively, this framework selection ensured strong theoretical alignment with the research questions, supported the quantitative design, and enabled a focused examination of how individual perceptions and organizational readiness jointly influence AI-driven cybersecurity adoption in regulated financial environments. Together, these frameworks provided a coherent analytical foundation for examining how perceptions of AI-driven cybersecurity technologies translate into adoption decisions and implementation outcomes within highly regulated financial environments.

Main Theoretical Framework

This study was grounded in two complementary theoretical frameworks: the Technology Acceptance Model and the Diffusion of Innovations theory. Developed by Davis (1989), the TAM framework focuses on user-level technology acceptance, emphasizing how perceived usefulness and ease of use influence behavioral intention and system utilization (Kumari et al., 2024; Sontan et al., 2024). The Technology Acceptance Model is particularly useful for evaluating how cybersecurity professionals perceive AI-driven tools within their workflows, especially in high-risk, compliance-driven environments (Binhammad et al., 2024). In contrast, the DOI theory, introduced by Rogers (2003), offers a broader institutional perspective by examining how innovation attributes relative advantage, compatibility, and complexity influence organizational adoption decisions (Jahangir et al., 2023; Mishra, 2023). While TAM captures micro-level user attitudes, DOI explains macro-level organizational decision-making, including the influence of social systems, communication channels, and adopter categories (Vial et al., 2024). Together, these frameworks provided a dual-lens approach that aligned with the study's goals of assessing both individual and organizational factors influencing the adoption of AI-powered cybersecurity technologies in financial institutions (Udeh et al., 2024). By integrating TAM and DOI, the study captured the nuanced interplay between individual acceptance and institutional readiness that ultimately determined implementation success (Faraji et al., 2024).

Technology Acceptance Model

The Technology Acceptance Model is the most influential and widely applied theoretical framework in information systems research. Fred Davis developed the framework in 1986 as an extension of the Theory of Reasoned Action (TRA) by Fishbein and Ajzen (1975). The TRA proposes that an individual's behavior is determined by their behavioral intention, which is

influenced by their attitude toward the behavior and subjective norms. Recognizing the need for a more specific model tailored to information technology, Davis adopted this general framework to explain users' acceptance and use of technology systems. He introduced TAM in his doctoral dissertation and later formalized it in a seminal 1989 publication (Jahangir et al., 2023). TAM has gained prominence for its parsimony, empirical testability, and predictive power in explaining why users accept or reject information technologies (Hentzen et al., 2022).

The TAM framework centered on two core independent constructs: Perceived Usefulness (PU) and Perceived Ease of Use (PEOU). According to Davis (1989), Perceived Usefulness refers to the extent to which an individual believes using a particular technology will improve their job performance. It captures the instrumental value of technology in helping users achieve specific work-related goals (Rana et al., 2024). Perceived Ease of Use refers to the degree to which an individual believes using the system will be effort-free, a key factor in whether the user will accept the technology (Kumari et al., 2024). Even a system with utility may be rejected if it is perceived as challenging to use. These beliefs influence users' attitudes toward technology, shaping their behavioral intention to use it and, ultimately, their actual system usage (Sontan et al., 2024).

The dependent constructs in TAM are Behavioral Intention to Use and System Usage. Behavioral Intention reflects the motivational factors that influence a person's readiness to perform a behavior, such as adopting and using a technology system. Actual system usage refers to the real-world application of technology, reflecting whether the individual integrates the system into their work processes (Kumari et al., 2024). Numerous studies have confirmed the predictive strength of behavioral intention and system usage, reinforcing the utility of TAM in

technology adoption research across industries, including financial services and cybersecurity (Udeh et al., 2024).

In this study, TAM served as the guiding theoretical framework for examining how cybersecurity professionals in financial institutions perceived and adopted AI-driven cybersecurity technologies. These professionals are expected to implement tools that support threat detection, compliance, fraud prevention, and incident response (Mishra, 2023). In this study, fraud prevention detection refers to the use of AI-driven cybersecurity technologies to identify, analyze, and respond to fraudulent activities in real time by recognizing anomalous patterns, suspicious transactions, and deviations from established behavioral baselines within financial systems. However, the successful implementation of such systems depended heavily on users' perceptions of the technologies' value and ease of integration within existing cybersecurity architectures. Perceived usefulness in this context referred to the extent to which professionals believed that AI-driven tools improved their ability to detect threats, automate compliance processes, and enhance organizational security posture (Binhammad et al., 2024). Perceived Ease of Use refers to the ease with which AI tools can be implemented and operated, particularly in complex and regulated environments (Rana et al., 2024).

The relevance of TAM to this study is reinforced through its alignment with the problem statement, which identified the growing complexity of integrating artificial intelligence into financial cybersecurity frameworks amid rising expectations for regulatory compliance, data privacy, and human-AI collaboration. Organizations struggled to balance innovation with risk management, and user perceptions about the benefits and usability of AI tools were critical to successful adoption (Sontan et al., 2024). Within this context, cybersecurity governance and risk management refer to the organizational structures, policies, oversight mechanisms, and decision-

making processes used to identify, assess, and mitigate cybersecurity risks, while ensuring regulatory compliance and the responsible adoption of AI. TAM offered a model for evaluating these perceptions and their impact on technology acceptance in institutional environments where cybersecurity decisions have both financial and ethical implications (Vial et al., 2024). Additionally, the TAM framework supported the study's purpose: to examine how AI-driven cybersecurity technologies are evaluated and adopted in financial institutions and how these implementations influence organizational performance, regulatory compliance, and human-machine collaboration. Focusing on PU and PEOU as central predictors of behavioral intention and usage, the model enabled a structured investigation of the cognitive factors shaping technology adoption in high-stakes cybersecurity environments (Kumari et al., 2024).

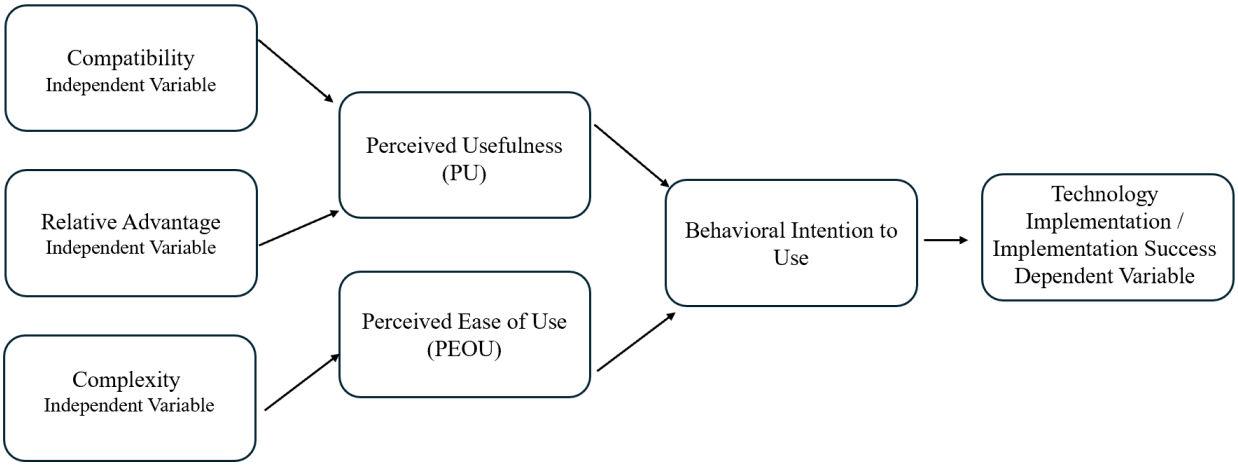
TAM also directly supported two of the study's four research questions, particularly RQ1 and RQ2, which examined compatibility and complexity as perceptual drivers of AI adoption outcomes. These constructs were operationalized and later tested through MANOVA analysis in Chapter 4 to determine their multivariate effects on institutional performance, compliance, and workforce outcomes. Research Question 1 asked: To what extent does the compatibility of AI-driven cybersecurity technologies with existing financial cybersecurity policies influence their implementation success, regulatory compliance, and data privacy protection? This research question aligns with both PU and PEOU. If AI systems were perceived as compatible with current workflows and policies, users were more likely to view them as valuable and easy to use, thereby increasing their intention to adopt (Udeh et al., 2024). Research Question 2 examined the following: To what extent did the complexity of AI-driven cybersecurity technologies impact their adoption in financial institutions, considering regulatory compliance, cybersecurity workforce adaptation, and data privacy management? This question reflected the PEOU

construct, where increased complexity reduced ease of use, thereby diminishing behavioral intention and adoption rates (Binhammad et al., 2024). In this context, workforce adaptation and the cybersecurity skills gap refer to the capacity of cybersecurity professionals to develop the technical and analytical skills required to effectively implement AI-driven tools, as well as the organizational challenges that arise when workforce capabilities lag rapidly evolving cybersecurity technologies.

In addition to its conceptual alignment with the study variables, the Technology Acceptance Model provided a clear structural foundation for operationalizing key constructs within the quantitative research design. The model's emphasis on perceived usefulness and perceived ease of use enabled the systematic measurement of user perceptions through survey instrumentation, supporting empirical testing of relationships between technology perceptions and adoption outcomes. This structure was particularly important in the financial cybersecurity context, where adoption decisions must be justified by measurable performance, compliance, and risk-mitigation outcomes. Accordingly, risk-based AI cybersecurity strategies in this study refer to the prioritization and deployment of AI-driven security capabilities based on assessed threat severity, regulatory exposure, and organizational risk tolerance to maximize protection of critical financial systems. By translating abstract perceptions into observable variables, TAM facilitated a rigorous examination of how individual-level evaluations of AI-driven cybersecurity technologies contributed to broader implementation success within financial institutions.

Figure 1

Technology Acceptance Model and its Variables



Note. This diagram illustrates the theoretical relationships between the independent variables, perceived usefulness and perceived ease of use, and the dependent variables, behavioral intention to use and system usage. It also shows how external variables, such as Compatibility, Complexity, and Relative Advantage, influence user perceptions and drive the adoption of AI-driven cybersecurity technologies within financial institutions.

The TAM model provided a nuanced, user-centered approach to understanding how perceptions of usefulness and ease of use translated into actionable outcomes. In the context of this study, these constructs explained adoption behavior and informed strategies for improving user training, system design, and implementation support. For instance, if AI tools were beneficial but difficult to integrate, organizations prioritized user training or simplified interfaces to increase adoption success (Vial et al., 2024).

The enduring strength of TAM lies in its generalizability and empirical validation across sectors. It had been used to evaluate diverse technologies, including enterprise systems, mobile apps, e-learning platforms, and cybersecurity infrastructures (Hentzen et al., 2022).

Understanding why professionals accepted or rejected AI-driven tools was essential in financial cybersecurity, where the stakes included compliance violations, financial fraud, and system breaches. TAM offered a rigorous structure for capturing these behavioral dynamics and identifying pathways to successful implementation (Jahangir et al., 2023).

Diffusion of Innovations Theory

The Diffusion of Innovations theory, also known as the Innovation Diffusion Theory (IDT), was initially developed by Everett M. Rogers in 1962 and later refined in his seminal work Diffusion of Innovations (2003). The DOI theory was compelling because it considered technological attributes and social system dynamics that influence adoption. As financial institutions navigate a complex, regulated digital environment, decision-makers have to consider how innovations such as AI-enhanced cybersecurity tools will affect technical operations, organizational norms, compliance expectations, and human capital strategies. In this study, cybersecurity governance and risk management are understood as the institutional frameworks, policies, and oversight practices through which organizations evaluate AI-driven cybersecurity innovations, manage enterprise cyber risk, and ensure alignment with regulatory and compliance obligations. The DOI theory helped conceptualize this multifaceted environment by emphasizing that adoption was not merely a technological decision but a social, institutional, and cultural process (Hentzen et al., 2022).

An element of the DOI was its categorization of adopters into five groups based on their willingness and rate of innovation adoption: innovators, early adopters, early majority, late majority, and laggards. This segmentation helped explain differences in risk tolerance, technological readiness, and compliance sensitivity across financial institutions. For example, a global investment bank with a robust innovation culture may have fallen into the "early adopter"

category, implementing AI tools rapidly to maintain a competitive advantage. In contrast, a regional credit union with fewer resources and higher regulatory caution may have behaved as a "late majority" adopter, waiting for technology to be standardized and proven before investing (Jahangir et al., 2023).

Additionally, DOI theory emphasized the communication channels and social influence mechanisms that shaped how innovations were perceived and understood. In financial institutions, decisions about adopting AI-driven cybersecurity technologies were often shaped by interdepartmental communication, external regulatory guidance, and peer benchmarking. For instance, if a competitor successfully integrated an AI threat-detection tool and achieved demonstrable results, other institutions may have perceived the innovation as less risky and more legitimate, thereby accelerating their adoption decisions (Vial et al., 2024). This process of observational learning, closely tied to the DOI "observability" construct, reinforced the idea that adoption was not based solely on internal evaluation but also on external institutional signaling. This study hypothesized that each of the three primary independent variables, relative advantage, compatibility, and complexity, played a distinct role in how decision-makers and key stakeholders judge AI cybersecurity systems (Kumari et al., 2024).

Relative Advantage included technical superiority, such as improved detection algorithms or faster response times, as well as the ability to reduce human workload, meet stricter compliance standards more efficiently, and generate predictive insights to mitigate risks. In cybersecurity, this advantage increasingly hinged on the automation of risk monitoring and proactive defense capabilities, making it a central criterion in enterprise decision-making (Mishra, 2023). Within this context, risk-based AI cybersecurity strategies refer to the selective deployment of AI-driven security capabilities based on assessed threat severity, regulatory

exposure, and organizational risk tolerance to maximize risk reduction and operational efficiency. Beyond performance improvements, relative advantage encompassed the perceived strategic value of AI tools, such as their ability to provide competitive differentiation, facilitate audit readiness, and support real-time situational awareness during cyber incidents (Udeh et al., 2024). Financial institutions that perceived a high degree of relative advantage were more likely to allocate funding, assign technical resources, and prioritize deployment timelines, even in high-risk regulatory environments (Sontan et al., 2024). Moreover, the perceived return on investment (ROI), whether measured in terms of fewer breaches, improved compliance scores, or enhanced client trust, further reinforced the desirability of adopting these technologies (Binhammad et al., 2024). In this way, relative advantage not only influenced the likelihood of adoption but also the depth of integration and long-term commitment to innovation across departments (Rana et al., 2024).

Compatibility, while often understood in terms of technical fit, was equally important for regulatory and strategic alignment. Financial institutions were under increasing pressure from regulators to demonstrate that their cybersecurity practices aligned with laws such as the GDPR and the California Consumer Privacy Act. AI solutions that integrated smoothly into these compliance protocols were more likely to be perceived as viable and trustworthy innovations (Binhammad et al., 2024). Moreover, institutions had to consider how well AI systems complemented existing governance frameworks and organizational values, particularly those that emphasized the ethical use of data and auditability (Faraji et al., 2024). High compatibility reduced the need for costly system overhauls or extensive policy restructuring, thereby accelerating implementation timelines and reducing resistance from key internal stakeholders (Udeh et al., 2024).

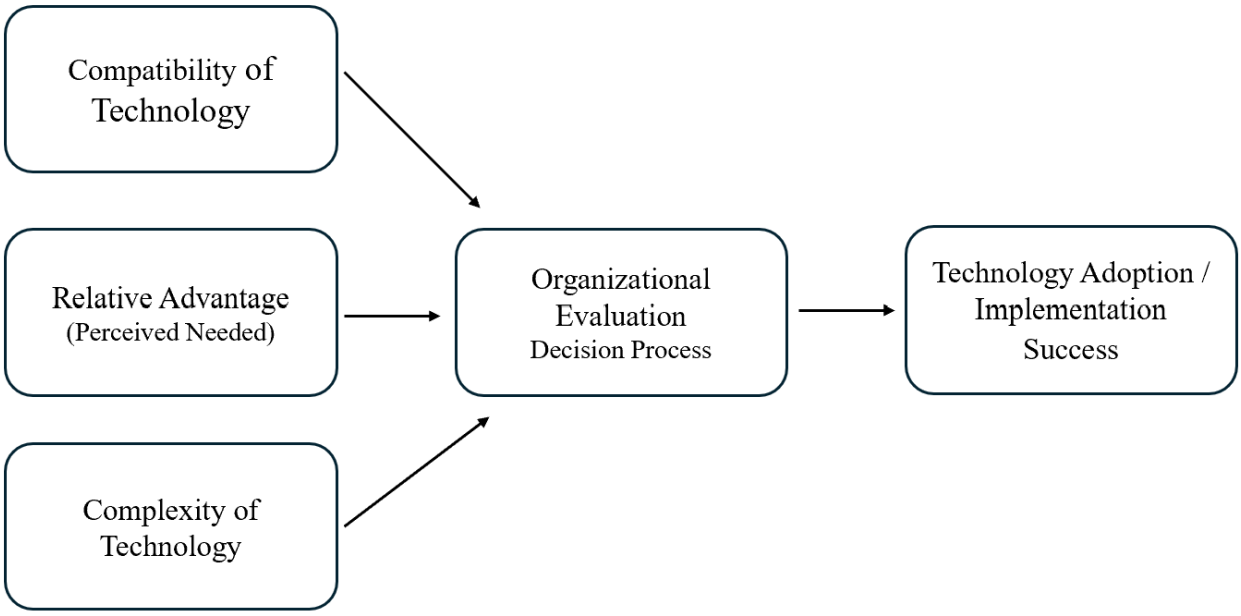
Complexity also took on a broader interpretation in the cybersecurity context. Beyond technical configuration challenges, complexity could have included the availability of skilled personnel to manage AI tools, the transparency and explainability of algorithmic decision-making, and the learning curve for non-technical users such as compliance officers or risk managers. In this study, workforce adaptation and the cybersecurity skills gap refer to the organizational capacity to develop and sustain the technical, analytical, and governance-related skills required to manage AI-driven cybersecurity systems, as well as the challenges that arise when workforce readiness lags technological complexity. Solutions perceived as too opaque or requiring extensive retraining may have generated institutional friction and delayed adoption (Vial et al., 2024). In environments where explainability and auditability are crucial for meeting regulatory standards, systems that lack transparency can undermine trust and increase compliance risks (Rana et al., 2024). Additionally, institutions operating across multiple jurisdictions may have faced compounded complexity due to variations in regulatory expectations, infrastructure capabilities, and workforce digital readiness (Hentzen et al., 2022).

The dependent variable, technology adoption or implementation success, extended beyond binary measures of use or non-use. In this study, implementation success encompassed the depth, scope, and sustainability of AI tool integration within cybersecurity workflows. Successful implementation meant the AI system was technically operational and delivered measurable improvements in risk reduction, regulatory alignment, operational efficiency, and user acceptance. Measuring success through this expanded lens enabled the study to examine adoption maturity rather than just initial installation or deployment (Hentzen et al., 2022). The DOI theory also aligned conceptually and methodologically with current cybersecurity research investigating institutional innovation barriers. Studies have shown that, even when AI

technologies were available and potentially beneficial, many organizations delayed adoption due to concerns about data governance, organizational inertia, and accountability for cyber risk (Udeh et al., 2024). DOI captured this phenomenon by explaining how the interaction between innovation attributes and system-level readiness affected adoption outcomes.

Figure 2

Diffusion of Innovations Framework and its Variables



Note. This diagram illustrates how the independent variables relative advantage, compatibility, and complexity influence an organization's evaluation and decision-making processes regarding innovation. These constructs collectively shape the outcome variable, technology adoption and implementation success, highlighting the systemic and institutional factors that affect the diffusion of AI-driven cybersecurity technologies in financial institutions.

In practice, financial institutions faced unique challenges in adopting AI-powered cybersecurity systems. These included securing executive buy-in, ensuring cross-functional collaboration among IT, compliance, and legal departments, and validating AI models to avoid

regulatory penalties arising from bias or performance failures (Rana et al., 2024). DOI provided a framework for systematically evaluating how these institutional factors interacted with the examined innovation attributes, particularly perceived risk, cost-benefit analysis, and innovation legitimacy. The theory was particularly well-suited to studies with a macro-level unit of analysis, such as entire institutions or business units within a sector. Unlike TAM, which focused on individual users, DOI provided insight into how inter-organizational dynamics, market pressures, and policy shifts affected the uptake of innovation. This distinction was crucial in financial cybersecurity, where regulatory guidance frequently influenced technology roadmaps, and where systemic risks could either deter or accelerate technological change at scale (Sontan et al., 2024).

In this study, DOI constructs were directly aligned with the independent variables of compatibility, complexity, and relative advantage, while implementation success was operationalized through institutional outcomes including cybersecurity performance, regulatory compliance, fraud prevention, adaptability, and human–AI collaboration. This alignment ensured that theoretical attributes of innovation were empirically examined through measurable organizational outcomes. The theory directly addressed the performance expectations, strategic alignment concerns, and integration challenges faced by decision-makers in this sector. By capturing the technical attributes of innovation and the social systems in which it diffused, DOI enabled a rich, multilayered analysis of the adoption process. When paired with the TAM framework, which offered insight into user-level perceptions, DOI provided a complementary macro-level perspective, forming a dual-level analytical lens with TAM to understand adoption in complex, multi-stakeholder environments for cybersecurity innovation in finance.

Complementary Theoretical Framework

Several theoretical frameworks were considered for this study, but ultimately not selected due to misalignment with the specific variables under investigation. However, similar studies have employed these frameworks and offered valuable perspectives that could inform future research. Two complementary frameworks include the Socio-Technical Systems Theory and the Unified Theory of Acceptance and Use of Technology.

Socio-Technical Systems (STS) Theory

The STS framework offered a holistic view of organizations by highlighting the interaction between social components (e.g., people, structure, culture) and technical components (e.g., tools, systems, processes). Initially developed by Trist and Bamforth and later expanded by Baxter and Sommerville (2011), the STS framework proposed that optimal performance was achieved when both subsystems are jointly optimized. In cybersecurity, STS theory has been applied to analyze how workforce coordination, human behavior, and organizational design influence the integration of new security technologies (Boletsis et al., 2021). For example, studies examining the impact of socio-technical alignment on AI adoption in workplace systems highlighted that social context played a significant role in successful implementation (Yu et al., 2023). Similarly, STS was applied to evaluate the impact of user attachment on the effectiveness of voice assistants, offering insight into user-technology interaction patterns (Kang et al., 2024)

Unified Theory of Acceptance and Use of Technology

Another relevant but unselected framework was the Unified Theory of Acceptance and Use of Technology (Venkatesh et al., 2003). UTAUT synthesized elements from multiple technology acceptance models and identified four primary determinants of user acceptance: performance expectancy, effort expectancy, social influence, and facilitating conditions

(Venkatesh et al., 2003). The framework has been widely used in financial and cybersecurity domains. For example, UTAUT was applied to evaluate FinTech adoption in Pakistan (Ashraf et al., 2022) and was extended to study behavioral intentions toward digital financial services (Bajunaied et al., 2023). In cybersecurity, it was used to examine user acceptance of AI-based cybersecurity systems in the UAE, with an emphasis on perceived ease of use and social context (Alneyadi et al., 2023). Similarly, Norzelan et al. (2024) explored AI acceptance in finance departments using UTAUT elements. Despite its comprehensiveness, UTAUT was not selected for this study because it emphasized moderating variables such as age, gender, experience, and social influence, which fell outside the scope of this study. This research concentrated on perceived characteristics of AI cybersecurity tools, such as compatibility, complexity, and relative advantage, which were better aligned with TAM and DOI. Furthermore, UTAUT often required larger samples and more complex moderation analyses, which exceeded the scope of this study's statistical plan.

While STS and UTAUT offer valuable perspectives, they were excluded because they focus on organizational systems and on moderated demographic factors that are not central to this study. In contrast, TAM and DOI were selected for their precise alignment with the perceived technological characteristics, including compatibility, complexity, and relative advantage, which were central to the research questions. These frameworks were well established for explaining individual technology adoption in regulated environments. They provided the foundation for the study’s quantitative design. They directly shaped the problem statement, purpose statement, and research questions, which focus on perceptions influencing AI adoption and cybersecurity governance in financial institutions.

Contrasting Theoretical Framework

Although used in similar studies, these theoretical frameworks were not selected for this research because they did not align with the study's core variables, methodological approach, or research focus. Two frameworks include Institutional Theory and the Theory of Planned Behavior (TPB). Although both had been applied in AI and cybersecurity research, they centered on concepts or methodological assumptions that differed significantly from those used in this study.

Institutional Theory

Institutional Theory, an organizational theory, focuses on how external pressures, such as regulations, cultural norms, and industry standards, influence organizational decisions (DiMaggio et al., 1983). In cybersecurity and AI adoption, this theory explains how organizations implement technologies to achieve legitimacy, ensure compliance, or mirror the practices of peer institutions, rather than solely for their technical functionality (Ali et al., 2024). Studies applying this framework often highlighted regulatory compliance, institutional isomorphism, and strategic alignment as the primary motivators of adoption (Ogbanufe et al., 2021). In many cases, organizations adopted cybersecurity tools to meet external expectations, such as industry standards or board-level scrutiny, rather than to evaluate their effectiveness internally (Gale et al., 2022).

However, institutional theory was not selected because it emphasizes external influences, which contrasts with this study's focus on individual-level perception. This study investigated how users evaluated technological attributes, such as compatibility, complexity, and relative advantage, which were better aligned with the TAM and DOI frameworks. Institutional Theory has often been applied in qualitative or longitudinal research, whereas this study employed a

cross-sectional, quantitative design that tests direct relationships between perceptual variables and adoption outcomes.

Theory of Planned Behavior

The Theory of Planned Behavior explains behavior through the lens of behavioral intention, which is influenced by attitudes, subjective norms, and perceived behavioral control (Ajzen, 1991). It has been widely applied in cybersecurity studies to understand user compliance with security policies, participation in cybersecurity awareness programs, and adoption of new security technologies (Almansoori et al., 2023). The TPB model emphasized intention as the primary predictor of behavior and often involved testing complex relationships through mediation or moderation analyses. In related studies, TPB was used to explore how attitudes toward cybersecurity tools, social pressure to comply with regulations, and users' confidence in their ability to adopt technologies drove behavioral intentions (Vafaei-Zadeh et al., 2025).

This framework was particularly effective in studies focused on the psychological or motivational aspects of user behavior. However, TPB was not selected because it emphasized motivational and normative factors rather than user perceptions of specific technological characteristics. The core concepts in this study, compatibility, complexity, and relative advantage, were more closely aligned with TAM and DOI, which emphasized intrinsic technology attributes over social or attitudinal contexts. Additionally, using TPB would have required consideration of broader variables related to intention formation and external influences, thereby adding methodological complexity beyond the study's quantitative design. The streamlined focus on technology perception variables better maintained alignment with the problem statement, purpose statement, and research questions. Nonetheless, TPB may offer value in future research focused on psychological drivers, organizational culture, or peer

influence in AI cybersecurity adoption. The following section reviews key topics shaping AI-driven cybersecurity adoption.

Review of Related Literature

AI History

Artificial intelligence formally emerged as a distinct field in the mid-20th century, driven by attempts to create machines capable of performing functions once thought to require human cognition, including the ability to acquire knowledge and make reasoned decisions (Ahmed et al., 2022). Early AI research was driven by optimism about achieving human-level intelligence, leading to substantial efforts focused on symbolic AI techniques, including rule-based programming and expert systems, aimed at replicating cognitive functions such as problem-solving, reasoning, and language understanding (Temelkov, 2023). However, early symbolic AI systems faced significant challenges in handling complex, real-world problems, which slowed progress and tempered the initial enthusiasm surrounding AI development (Kaur et al., 2023).

Advances in computational power, the availability of large datasets, and breakthroughs in machine learning algorithms fueled AI's resurgence, particularly artificial neural networks (Choithani et al., 2024). The shift toward data-driven AI research, enabled by advances in neural networks and deep learning models, transformed AI from rule-based systems to systems capable of autonomous learning (Choithani et al., 2024). These innovations enabled AI systems to learn autonomously from large volumes of data without requiring explicitly coded rules, thereby improving performance on complex tasks such as image recognition, natural language processing, and predictive analytics (Han et al., 2023). The scalability and predictive capabilities of modern AI systems have positioned AI as a critical enabler of innovation across industries, supporting complex decision-making processes and driving operational efficiencies (El Hajj et

al., 2023). In parallel, AI applications began to expand across industries, notably healthcare, transportation, finance, and cybersecurity. Particularly in the financial sector, the integration of AI initially focused on algorithmic trading and fraud detection but later expanded into regulatory compliance, customer service automation, and cybersecurity threat detection (Ahmed et al., 2022). In the literature, fraud prevention detection refers to the application of AI techniques such as anomaly detection, behavioral analytics, and pattern recognition to identify and mitigate fraudulent activities within financial systems (Awosika et al., 2024; Paul et al., 2023). As AI matured, ethical implications, explainability, and the need for regulatory frameworks emerged, particularly as AI systems were increasingly deployed in high-stakes decision-making contexts (López González et al., 2024). In the financial sector, this evolution drew the attention of key U.S. regulators, including the OCC, SEC, Federal Reserve, NCUA, FIO, and GDPR, who now oversee the integration of AI into supervisory, compliance, and data protection frameworks (Phillips et al., 2024). This regulatory involvement highlights the growing importance of cybersecurity governance and risk management, which the literature describes as the policies, oversight structures, and risk assessment processes used to guide the secure and compliant deployment of AI technologies in financial institutions (Zhong et al., 2024).

In cybersecurity, AI technologies have evolved from traditional rule-based detection systems to more sophisticated models that utilize behavioral analysis, anomaly detection, and predictive analytics (Sontan et al., 2024). These transitions mirror broader trends in AI development, shifting from manually programmed expert systems to adaptive, self-learning models that can identify and respond to previously unseen threats in real time (Malatji et al., 2024). As reflected in the literature, these developments enabled risk-based AI cybersecurity strategies in which AI-driven defenses are prioritized and deployed based on threat severity,

system criticality, and potential regulatory or operational impact (Abikoye et al., 2024; Dawodu et al., 2023; Dhanawat et al., 2024). Furthermore, the ability of AI-driven cybersecurity solutions to dynamically evolve in response to emerging threats made them indispensable in protecting sensitive data and financial infrastructure from increasingly complex cyberattacks (Djenna et al., 2023). The literature also notes that this growing sophistication intensified the need for workforce adaptation and highlighted a cybersecurity skills gap, as organizations required personnel capable of managing, interpreting, and governing advanced AI-driven security systems (Ali et al., 2024; Baruwal Chhetri et al., 2024).

Thus, the history of AI demonstrates an evolution from symbolic reasoning to sophisticated, data-driven learning systems and computational capacity. This historical progression provides essential context for understanding AI's current and future roles in enhancing cybersecurity frameworks in financial institutions, particularly in addressing challenges related to regulatory compliance, data privacy, and human-AI collaboration. As AI technologies have matured, their application in cybersecurity has moved beyond simple automation to proactive, intelligent threat detection and response systems. The following section examines the growing impact of AI-driven cybersecurity solutions, highlighting how these technologies are transforming security operations in the highly regulated, increasingly digital financial services sector.

AI-Driven Cybersecurity

Traditional cybersecurity defenses relied heavily on manually defined rules and known threat signatures, but they have become increasingly inadequate in the face of the scale and complexity of modern cyberattacks (Ebert et al., 2023). Integrating artificial intelligence into cybersecurity operations has fundamentally reshaped organizations' strategies for preventing,

detecting, and responding to evolving cyber threats. AI-driven cybersecurity solutions leveraging machine learning, natural language processing, and predictive analytics offer dynamic, adaptive capabilities that significantly enhance threat detection and mitigation (Sontan et al., 2024). For instance, machine learning enables cybersecurity systems to learn autonomously from large volumes of historical and real-time data. Machine learning allowed them to identify anomalies, detect sophisticated attacks, and predict emerging threats without constant human intervention (Djenna et al., 2023). AI techniques, including supervised learning, clustering, anomaly detection, and deep reinforcement learning, were instrumental in strengthening security postures across various industries (Kaur et al., 2023). In the financial sector, AI-driven tools support fraud prevention and detection by monitoring transactional behavior, identifying fraudulent activities, and responding to zero-day threats, ensuring proactive cybersecurity management (Choithani et al., 2024).

Financial institutions rapidly adopted AI-driven cybersecurity solutions due to the heightened sensitivity of their data assets, customer trust imperatives, and stringent regulatory requirements (Deshpande, 2024). The digitization of financial services and the proliferation of online banking platforms expanded the attack surface, making traditional reactive security approaches insufficient (Javaheri et al., 2024). Artificial intelligence enhanced cybersecurity in finance through automated fraud detection, behavioral biometrics, anti-money laundering (AML) monitoring, and intelligent risk-scoring models, reflecting the adoption of risk-based AI cybersecurity strategies that enhance operational resilience (Deshpande, 2024). One significant advantage of AI in cybersecurity is its ability to process and correlate disparate data sources at scale, thereby identifying subtle indicators of compromise that may elude traditional systems (Rizvi, 2023). In addition, AI-enhanced cybersecurity incident management involves automating

repetitive tasks, prioritizing security alerts, recommending or executing mitigation measures, and streamlining response processes (Ebert et al., 2023). Cybersecurity operations centers (SOCs) continue to face a global shortage of skilled professionals, highlighting ongoing workforce adaptation and the cybersecurity skills gap, and making AI a vital force multiplier by enhancing efficiency and reducing the time-to-response for critical incidents (Sontan et al., 2024).

While AI introduces powerful capabilities, it also creates new vulnerabilities. Adversaries have exploited AI to generate more sophisticated attacks, including adversarial machine learning, polymorphic malware, and deep-fake-based social engineering (Malatji et al., 2024). AI-driven attacks were more complex to detect and neutralize, requiring defenders to deploy equally advanced, adaptive security models. Moreover, the opacity of many AI models, often referred to as the "black box" problem, poses challenges for explainability, governance, and regulatory compliance (Awosika et al., 2024). Ethical considerations further complicate the use of AI in cybersecurity. Addressing bias in AI algorithms, potential privacy infringements, and the risk of over-reliance on automated decision-making were essential to ensure cybersecurity practices align with legal, ethical, and societal expectations (Ridzuan et al., 2024).

As AI systems increasingly influence high-stakes cybersecurity outcomes, financial institutions must prioritize transparency, human oversight, and adherence to ethical AI standards. Compliance with regulations such as the GDPR and emerging data protection laws was crucial to avoid legal liabilities and maintain stakeholder trust (Varmaz, 2020). In U.S. financial services, primary oversight is exercised by the OCC, Federal Reserve, NCUA, SEC, FIO, and GDPR, with state and industry frameworks like the CCPA and PCI-DSS serving as complementary standards that strengthen consumer protection (Mullin, 2023; Phillips et al., 2024). Integrating AI solutions

into cybersecurity strategies, therefore, requires not only technical sophistication but also robust cybersecurity governance and risk management structures to ensure lawful and responsible use.

Thus, the advent of AI-driven cybersecurity marked a critical evolution in financial institutions' approach to cyber risk management, threat mitigation, and regulatory compliance. The enhanced capabilities provided by AI must be carefully integrated into existing cybersecurity frameworks to optimize effectiveness while mitigating new risks. The following section explores how the compatibility of AI-driven cybersecurity technologies with existing cybersecurity policies and regulations influences their adoption and operational success in financial institutions.

Compatibility of AI with Existing Cybersecurity Policies & Regulations

Incorporating AI technologies into financial cybersecurity environments presents complex alignment issues with existing cybersecurity policies and regulatory frameworks, particularly within established cybersecurity governance and risk management (Ali et al., 2024). AI technologies, such as machine learning-driven threat detection, behavioral analytics, and predictive modeling, often operate dynamically, continuously adapting to new data inputs. However, most traditional cybersecurity regulations and supervisory frameworks (e.g., GDPR, OCC, Federal Reserve, NCUA, FIO, and SEC guidelines) were designed for static, rule-based security architectures, creating a fundamental tension between AI capabilities and regulatory expectations (Binhammad et al., 2024).

Within the U.S. financial system, the primary regulators, the OCC, Federal Reserve, NCUA, SEC, FIO, and GDPR, play central roles in establishing the compliance environment for AI adoption. The OCC and the Federal Reserve have underscored the need for AI integration to meet existing supervisory expectations regarding safety, soundness, and information security.

These include requirements for internal controls, risk management practices, and explainability in AI systems (Ajakaye et al., 2025; Phillips et al., 2024). The NCUA applies comparable standards under the Federal Credit Union Act, mandating minimum security safeguards. However, its authority over third-party AI vendors remains limited, complicating complete oversight (Phillips et al., 2024). In the insurance sector, the FIO collaborates with state regulators through the NAIC Insurance Data Security Model Law, which establishes cybersecurity program, data protection, and incident response obligations specifically for insurers (Gupta et al., 2024; Phillips et al., 2024).

Compatibility issues also arise when AI's autonomous decision-making processes and evolving algorithms conflict with compliance requirements emphasizing transparency, auditability, and explainability (Binhammad et al., 2024; López González et al., 2024). For example, GDPR and Regulation S-P both require institutions to explain automated decisions affecting consumers, yet deep learning models often lack interpretability (Vial et al., 2024). These gaps complicate financial institutions' ability to meet mandates for data privacy, accountability, and consumer rights across multiple jurisdictions. Additionally, risks such as model drift, adversarial attacks, and embedded algorithmic bias remain underdeveloped in traditional supervisory frameworks, complicating the implementation of risk-based AI cybersecurity strategies in regulated financial environments (Faraji et al., 2024).

To maintain regulatory compliance and operational effectiveness, including effective fraud prevention and detection, financial institutions must proactively update cybersecurity policies to account for AI's unique operational characteristics. Scholars emphasize AI-specific auditing procedures, algorithm validation, continuous monitoring, and human oversight as mechanisms to ensure compliance with OCC, Federal Reserve, NCUA, FIO, SEC, and GDPR

requirements (Dopamu et al., 2024; Phillips et al., 2024). Maintaining compliance requires developing AI-specific auditing procedures, enhancing algorithmic transparency requirements, establishing model validation protocols, and integrating human oversight mechanisms to monitor and intervene when AI systems operate outside expected parameters (Awosika et al., 2024). Institutions must also embed privacy-enhancing technologies and responsible AI principles, such as fairness, accountability, and transparency, into cybersecurity systems to satisfy stricter regulatory expectations (Udeh et al., 2024). The degree to which solutions for AI cybersecurity are compatible with existing regulatory and policy frameworks, including GDPR, the GLBA Safeguards Rule, SEC Regulation S-P, and NAIC Insurance Data Security Model Law at the federal level, as well as CCPA, and PCI-DSS as complementary international, state, and industry standards, influences their adoption, acceptance, and sustainable use within financial institutions (Dawodu et al., 2023). High compatibility simplifies deployment, strengthens institutional trust in AI systems, facilitates regulatory inspections, and reduces compliance costs. Conversely, low compatibility significantly increased the likelihood of regulatory breaches, operational disruptions, legal liabilities, and reputational harm, making organizations hesitant to adopt AI cybersecurity tools without substantial policy reform and governance support (Deshpande, 2024).

Therefore, evaluating and enhancing compatibility is a technical concern and a strategic imperative for financial institutions seeking to leverage AI in ways that align with evolving cybersecurity laws, protect consumer rights, and fortify institutional resilience against sophisticated cyber threats. At the same time, even when institutions recognize the strategic value of AI integration, the inherent complexity of AI-driven cybersecurity systems presents additional barriers that can significantly influence adoption decisions. These complexities are

amplified in institutions operating across multiple jurisdictions, where harmonizing AI operations with diverse legal requirements is particularly burdensome. As a result, cross-border financial institutions must adopt adaptable governance frameworks that ensure AI solutions remain compliant, explainable, and interoperable across diverse regulatory environments, while also addressing ongoing workforce adaptation and cybersecurity skills gap associated with managing AI-enabled security systems.

Complexity of AI-Driven Cybersecurity and Its Impact on Adoption

AI-based systems often require specialized knowledge for implementation, management, and oversight, including expertise in data science, machine learning algorithms, cybersecurity protocols, and regulatory compliance standards (Choithani et al., 2024). The inherent complexity of AI-driven cybersecurity technologies significantly affects their adoption within financial institutions. Unlike traditional security tools, AI systems introduce multiple layers of computational sophistication, such as advanced pattern recognition, behavioral anomaly detection, and predictive analytics, which can overwhelm cybersecurity teams lacking sufficient technical depth, posing a formidable barrier to adoption. Sai Meghana et al. (2024) further emphasized that financial institutions struggle to keep pace with the rapid evolution of AI attack vectors and the need for continuous upskilling of cybersecurity personnel, reflecting persistent workforce adaptation and cybersecurity skills gap.

Complexity can manifest itself in several critical ways. First, algorithmic opacity, particularly in deep learning models, poses a challenge to understanding how AI systems arrive at specific threat-detection or risk-scoring decisions (Ebert et al., 2023). The "grey box" nature of these models limits transparency, raising concerns about reliability, bias, and accountability. Jain et al. (2024) noted that financial institutions face difficulties auditing black-box AI models,

which raise compliance and cybersecurity governance and risk management concerns when regulators require interpretability and audit trails for algorithmic decision-making. Second, AI systems require vast volumes of diverse, high-quality training data to function effectively. However, securing, labeling, and maintaining these datasets introduced significant operational overhead and data privacy compliance risks (Faraji et al., 2024). Preparing compliant AI datasets is a resource-intensive process, particularly under data protection frameworks such as the GDPR, which increased perceived adoption barriers (Van Bekkum et al., 2023). Third, integrating AI-driven solutions into existing IT infrastructures often requires extensive reengineering, middleware solutions, and new interfaces to ensure interoperability between legacy systems and modern AI architectures (Kaur et al., 2023). Zhong et al. (2024) reinforced this by identifying technical integration as a core cybersecurity governance challenge, particularly when AI must interface with legacy systems not designed for real-time AI processing.

Further exacerbating the complexity challenge, Udeh et al. (2024) reported that financial institutions invested heavily in new infrastructures, including high-capacity cloud computing platforms, edge computing resources for real-time threat detection, and federated learning systems to preserve data privacy during AI model training. Additionally, cybersecurity personnel must undergo continuous retraining to develop AI fluency, encompassing technical proficiency and an understanding of AI governance, model risk management, and the ethical use of AI (Ebert et al., 2023). The burden of regulatory adaptation and governance restructuring was also highlighted as financial institutions adopt AI systems that require human oversight and operational integration with compliance teams (Hassan et al., 2023). This adaptation is challenging given the layered regulatory landscape, in which primary oversight is exercised by the OCC, Federal Reserve, NCUA, SEC, and FIO, while secondary requirements such as GDPR,

CCPA, and PCI-DSS must also be observed (Ajakaye et al., 2025; Phillips et al., 2024). High perceived complexity can delay AI implementation by increasing perceptions of operational risk, technological uncertainty, and organizational disruption, complicating the execution of risk-based AI cybersecurity strategies. Managers and cybersecurity leaders feared operational disruptions, cascading system failures caused by AI misjudgments, or unforeseen legal liabilities stemming from AI-driven decisions (Rizvi, 2023). Moreover, complexity heightens governance challenges, necessitating the development of new risk assessment frameworks, audit procedures, and monitoring systems to ensure that AI outcomes align with institutional compliance, ethical standards, and acceptable risk thresholds (Ghandour, 2021). Collectively, these dimensions of complexity functioned not merely as technical obstacles but as adoption inhibitors that influenced managerial risk perception, regulatory hesitation, and institutional readiness.

However, the impact of complexity is not uniformly negative over time. As institutions invest in AI readiness, the perceived complexity of AI solutions can diminish. Targeted investments in workforce upskilling, deploying explainable AI (XAI) tools, pilot implementation programs that allow for iterative learning, and establishing clear governance structures contribute to demystifying AI technologies and fostering organizational trust (Awosika et al., 2024). Financial institutions that have developed hybrid human-AI governance models, in which AI systems operate alongside and under the oversight of cybersecurity professionals, have helped mitigate algorithmic opacity risks, improve system accountability, and strengthen cybersecurity outcomes, including fraud detection (Baruwal Chhetri et al., 2024). As a result, complexity is both an initial hurdle to adoption and a dynamic, manageable variable within an organization's technological trajectory. Institutions that view complexity as a temporary challenge rather than an insurmountable barrier and strategically address it through education, investment, and

governance reforms are more likely to realize the full potential of AI-enhanced cybersecurity. Understanding and proactively mitigating complexity is crucial to facilitating the smooth, responsible, and scalable adoption of AI-driven cybersecurity technologies in the financial sector.

AI and Data Privacy Protection

Integrating AI into financial cybersecurity presents a powerful yet complex challenge. On the one hand, AI enhanced institutions' ability to detect, prevent, and respond to cyber threats with unprecedented speed and precision (Han et al., 2023). Conversely, its reliance on extensive, sensitive data introduces significant risks to privacy, ethical accountability, and regulatory compliance. AI systems commonly analyze personally identifiable information (PII), transactional behavior, biometric data, and geolocation data to support real-time fraud detection and risk assessment. This dependence on high-volume data intensified tensions between innovation and data protection (Vial et al., 2024).

While AI-enhanced detection capabilities, its dependency on high-volume, sensitive datasets intensified regulatory scrutiny and heightened institutional exposure to data governance risks (Zhou, 2023). However, such access can lead to unintended consequences, including data over-collection and secondary use without proper consent. These practices challenged core privacy principles, such as data minimization and purpose limitation, which are foundational to global regulations such as the GDPR and the CCPA. Additionally, in the U.S. financial sector, primary data protection oversight is governed by the GBLA Safeguards Rule, SEC Regulation S-P, and the supervisory roles of the OCC, Federal Reserve, NCUA, and FIO, with the CCPA and PCI-DSS functioning as complementary standards within broader cybersecurity governance and risk management structures (Phillips et al., 2024).

The risks were further exacerbated using opaque “black box” AI models, whose internal processes are not easily interpretable, even by their developers, making it challenging to explain how outputs such as fraud flags or risk scores are generated and assessed within risk-based AI cybersecurity strategies (Binhammad et al., 2024). In the United States, oversight extends beyond the GDPR and the CCPA to include industry standards such as PCI DSS and evolving federal requirements, particularly recent SEC regulations. These evolving mandates reflect the SEC’s broader shift toward dynamic and proactive data governance in response to the rapid integration of AI technologies (Dopamu et al., 2024).

Financial entities often struggle to verify how AI-based decisions are made, particularly when automated outputs affect consumer access to services or credit (Awosika et al., 2024). The lack of explainability within AI creates barriers for institutions attempting to demonstrate regulatory compliance. Moreover, AI outputs are difficult to audit or challenge, thereby complicating transparency and justification during regulatory reviews (Binhammad et al., 2024). Financial institutions increasingly use federated learning and XAI models to address data privacy and compliance concerns. These technologies support secure, decentralized analytics, enhancing transparency in decision-making without compromising access to sensitive data (Chakkappan et al., 2024). These training approaches demonstrate that federated learning supports compliance with residency and sovereignty requirements, particularly in multi-jurisdictional financial networks (Dhanawat et al., 2024).

Adopting XAI and algorithmic auditing are essential for enhancing data privacy and accountability in AI-driven financial services. When AI systems make decisions related to fraud detection, credit access, or transaction verification, their outputs must be interpretable and auditable to meet institutional, legal, and ethical expectations (Awosika et al., 2024). Techniques

such as decision trees and model-agnostic explanation tools help promote transparency, enabling institutions to justify automated decisions during compliance reviews. Embedding these capabilities into governance frameworks supports alignment with evolving legal standards and reinforces trust among regulators and consumers (López González et al., 2024).

However, global disparities in data governance introduce significant challenges. In jurisdictions with immature or fragmented regulatory systems, particularly in emerging markets, AI deployment can result in unregulated data reuse, privacy violations, and biased outcomes (Faraji et al., 2024). Without harmonized policy frameworks and oversight, the expansion of AI technologies risks exacerbating systemic inequality and weakening data protection norms (Oriji et al., 2023). In contrast, regulatory advancements such as the SEC's updated mandates in the U.S., which now require disclosure of cybersecurity incidents and governance practices, reflect a growing recognition of AI's intersection with enterprise-level privacy obligations (Dopamu et al., 2024). To navigate this complexity, financial institutions must adopt a cross-functional governance approach that brings together compliance experts, cybersecurity professionals, legal teams, and data scientists, while also addressing workforce adaptation and the cybersecurity skills gap associated with privacy-conscious, regulation-ready AI systems (Hentzen et al., 2022).

Human-AI Collaboration

Human-AI collaboration is crucial in enhancing the effectiveness, resilience, and ethical integrity of cybersecurity systems within the financial sector. While AI offers unparalleled capabilities for detecting anomalies, processing large datasets, and automating real-time responses, its full potential is realized only when integrated with human expertise. This collaboration was foundational to the development of adaptive, accountable systems aligned with the contextual and regulatory needs of financial institutions (Martin, 2022). As financial

institutions increasingly adopt AI tools, collaboration needs to extend beyond operational functions to include strategic alignment with ethical and legal principles, reflecting ongoing workforce adaptation and cybersecurity skills gap associated with AI-enabled security environments (Cai et al., 2023).

The core strength of AI lies in its ability to process data, flag threats, and automate responses rapidly. However, this speed often comes at the cost of contextual understanding and interpretability. These are areas where human analysts still excel (Malatji, 2024). In security operations centers, analysts often experience alert fatigue due to the excessive number of low-quality alerts generated by automated systems (Baruwal Chhetri et al., 2024). Detection accuracy improves when AI tools are designed to prioritize and contextualize alerts based on human-in-the-loop feedback mechanisms (Baruwal Chhetri et al., 2024). In financial fraud contexts, human analysts remained essential to fraud prevention and detection by interpreting anomalies, identifying false positives, and refining thresholds for future alerts (Nwafor et al., 2024). Recent models demonstrated that when human analysts and AI systems engage in co-adaptive workflows where each learns from the other, alert triage efficiency improves over time, leading to reduced response times and better threat identification (Van Hoang, 2023)

Human-AI collaboration was vital in strategic cybersecurity roles, including policy development, cybersecurity governance, risk management, and threat intelligence. As AI becomes increasingly embedded in decision-making processes, human experts have evaluated its outputs in complex legal, organizational, and regulatory contexts (Djenna et al., 2023). For instance, insider threat detection models raised concerns about employee surveillance, prompting calls for human discretion and ethical judgment (Djenna et al., 2023). Trust in AI increased when cybersecurity professionals gained a deeper understanding of how AI systems function and could

provide informed feedback (Alneyadi et al., 2023). Transparent interfaces and participatory design further empowered users to oversee, adjust, or override AI-generated decisions as necessary (Ebert et al., 2023). Moreover, studies have shown that when systems support "shared agency," in which both humans and machines contribute to outcomes, user confidence and decision quality improve substantially (Banerjee et al., 2025). The literature suggests that human–AI collaboration strengthens perceived relative advantage when AI systems augment rather than replace professional judgment, thereby enhancing institutional trust and operational resilience (Alneyadi et al., 2023; Banerjee et al., 2025; Djenna et al., 2023). This theoretical linkage informed the study's examination of workforce augmentation and job satisfaction outcomes.

Despite these advantages, challenges remain. One significant risk is over-reliance on AI, particularly in high-pressure or resource-constrained environments. Blind trust in AI led to reduced human vigilance and increased susceptibility to adversarial manipulation or misclassification errors (Faraji et al., 2024). To mitigate this, organizations had to establish clear governance structures that allocated responsibility between human actors and automated systems, enabling the effective execution of risk-based AI cybersecurity strategies. Algorithmic bias in applications such as credit scoring systematically disadvantaged specific demographic groups, making human oversight essential for identifying, correcting, and contextualizing these outcomes within the broader goals of fairness and regulatory compliance (George, 2023). This need for ethical alignment has catalyzed the development of collaborative AI systems that evolve in response to human input, supporting mutual adaptation, shared understanding, and sustained trust (Djenna et al., 2023). To address evolving threats, some institutions implemented "dynamic governance" models that enable continuous human oversight throughout the AI lifecycle, from

development through deployment and auditing (Gopal et al., 2023). However, research cautioned that overly complex AI interfaces can reduce usability, limit effective engagement, and introduce new security vulnerabilities, particularly in high-stakes financial environments (Manser Payne et al., 2024).

Ultimately, successful human-AI collaboration necessitates a cultural shift and effective technological integration. Financial institutions must build interdisciplinary teams in which cybersecurity analysts, data scientists, compliance officers, and legal experts collaborate to define the scope, limitations, and purpose of AI systems. This collective intelligence ensures that AI tools are technically accurate, socially responsible, and legally compliant (Djenna, 2023). AI is most effective when functioning as a decision-support tool rather than an autonomous agent, with humans maintaining final oversight and ethical control. Institutions can maximize the value of AI through thoughtful planning, continuous training, and cross-functional collaboration while upholding trustworthy and resilient cybersecurity practices.

Synthesis of the Research Findings

The literature reviewed demonstrates the multifaceted nature of AI adoption in financial cybersecurity, shaped by the dynamic interplay of regulatory obligations, technological maturity, cybersecurity governance and risk management, and human-system integration. Through the guiding lens of the Technology Acceptance Model and the Diffusion of Innovations theory, three overarching constructs, compatibility, complexity, and relative advantage, emerge as thematic anchors across the scholarly discourse. These variables not only help frame the technological considerations but also reflect the socio-organizational shifts required to integrate AI responsibly and effectively. As financial institutions continue to navigate rapidly evolving threat landscapes,

the alignment between innovation characteristics and institutional readiness becomes a defining factor in successful AI adoption.

Compatibility consistently emerged as a foundational determinant of successful AI integration, particularly because it influences regulatory alignment and operational continuity. Studies revealed that the likelihood of AI implementation increases when new systems align with existing cybersecurity practices, U.S. regulatory policies, GLBA Safeguards Rule, SEC regulations, and oversight by agencies including the OCC, Federal Reserve, and NCUA, as well as secondary frameworks such as GDPR, CCPA, and PCI-DSS (Awosika et al., 2024; Baruwal Chhetri et al., 2024). These findings support the TAM's emphasis on perceived usefulness and the DOI's focus on system-organization alignment (Jahangir et al., 2023). Moreover, several studies highlighted that compatibility influences initial acceptance and long-term institutional trust in AI system outputs (Alneyadi et al., 2023). When AI tools were perceived as intuitive extensions of existing frameworks rather than disruptive innovations, stakeholders were likely to adopt, engage with, and champion them across the organization (Ali et al., 2024). As a result, ensuring compatibility through policy alignment, system interoperability, and staff preparedness emerged as a critical success factor for the widespread adoption of AI in financial cybersecurity settings (Kumari et al., 2024; Ridzuan et al., 2024).

The historical progression of AI from symbolic rule-based systems to autonomous, self-learning models continues to provide critical context for understanding its expanded role in cybersecurity (Choithani et al., 2024; Han et al., 2023). This technological evolution enabled AI to move beyond static pattern recognition toward adaptive, real-time behavioral analysis, anomaly detection, and predictive analytics (Malatji et al., 2024; Sontan et al., 2024). These capabilities align with TAM's focus on perceived usefulness and DOI's emphasis on innovation

attributes that improve task performance. Consequently, advances in machine learning and neural networks have substantiated AI's growing advantage over legacy systems in enhancing cybersecurity operations in highly regulated financial environments.

Complexity, in contrast, played a dual role. On the one hand, algorithmic opacity, integration hurdles, and steep learning curves initially deterred adoption (Deshpande, 2024; Ebert et al., 2023). On the other hand, several studies documented the transformation of complexity from a barrier into a source of organizational resilience, particularly in environments that invest in workforce upskilling, modular AI architectures, and iterative pilot testing, thereby addressing workforce adaptation and cybersecurity skills gap (Djenna et al., 2023; Faraji et al., 2024). Institutions that proactively demystified AI technologies through explainable AI tools, simulation environments, and cross-functional training reported improved adoption rates and greater trust in automated systems (Awosika et al., 2024; Chakkappan et al., 2024). Consequently, the role of complexity is both nuanced and dynamic, acting as a deterrent or a catalyst depending on how institutions manage learning curves and promote system transparency (Hentzen et al., 2022; Kaur et al., 2023).

Relative advantage, a core DOI construct, has been well substantiated in the literature. Artificial Intelligence systems that enhanced threat detection, minimized false positives, automated incident response, and supported regulatory reporting demonstrated superior performance compared to legacy tools, reflecting the effective use of risk-based AI cybersecurity strategies (Mishra, 2023; Sontan et al., 2024). However, this advantage is unevenly realized. Institutions with lower AI literacy or constrained budgets often struggle to achieve meaningful improvements, highlighting the influence of contextual factors such as governance maturity, leadership support, and cybersecurity culture (Gale et al., 2022). Moreover, the perception of

relative advantage was influenced by institutional readiness to integrate AI into existing workflows and regulatory reporting systems (Udeh et al., 2024). Emerging risks such as adversarial AI, model drift, and opaque decision-making also threaten to erode perceived benefits if not addressed through strong oversight mechanisms (Ridzuan et al., 2024; Rizvi, 2023). Several studies have emphasized that perceived relative advantage is tied to trust in the technology's reliability and its ability to augment, rather than replace, human expertise (Awosika et al., 2024). Without organizational buy-in and a strategic roadmap, the scalability of these advantages was likely to remain limited, particularly in risk-averse or compliance-constrained sectors.

An additional layer to these themes is the evolving role of human-AI collaboration. While many studies reported increased decision-making efficiency and reduced analyst fatigue, others cautioned against over-reliance on AI or poorly defined roles for human oversight (Baruwal Chhetri et al., 2024; Vial et al., 2024). The effectiveness of human-AI teams depended on technological transparency and organizational structures that support feedback loops, error correction, and decision accountability. However, inadequate training or procedural ambiguity led to critical lapses, with personnel deferring entirely to AI recommendations, thereby increasing the risk of misclassification or regulatory violations (Binhammad et al., 2024). These findings reinforced the importance of governance frameworks that formalize the role of human oversight, particularly in decision contexts that carry financial, legal, or reputational consequences.

Ethical and regulatory alignment also emerged as consistent concerns. Studies have emphasized the importance of explainability, bias mitigation, and transparency in AI cybersecurity governance. Nevertheless, many organizations were still developing formal

policies in these areas, revealing a persistent disconnect between AI deployment and comprehensive oversight practices (Choithani et al., 2024). Additionally, the literature highlighted that ethical risks are heightened when AI systems are trained on biased or incomplete datasets, particularly in fraud prevention, detection, and user behavior profiling (Faraji et al., 2024). As AI technologies evolve, ethical alignment must be proactively integrated into AI governance models rather than treated as a reactive compliance measure.

Despite substantial research on AI-enabled cybersecurity tools, the literature lacked a structured, quantitative examination of how compatibility, complexity, and relative advantage simultaneously influenced multivariate institutional outcomes within U.S. financial institutions. Most prior studies isolated technical performance, governance, or human factors rather than integrating these constructs within a unified adoption framework. This gap justified the present study's theory-driven, multivariate design.

Critiques of Research Methodology

The research reviewed across the AI cybersecurity finance landscape exhibits methodological strengths and notable limitations, offering critical insight into how future studies can enhance robustness and relevance. One methodological strength is the growing use of empirical, data-driven approaches to assess AI's impact. Many studies employed surveys, case studies, or system evaluations to measure outcomes such as fraud-detection rates, user satisfaction, and policy adherence (Dawodu et al., 2023; Mishra, 2023; Udeh et al., 2024). These methods provided valuable real-world insights. They aligned the TAM and DOI constructs by capturing users' perceived usefulness, ease of use, and innovativeness. Additionally, several articles employed mixed method designs or systematic literature reviews, thereby contributing to

a more comprehensive understanding of AI's operational impact (Faraji et al., 2024; Hentzen et al., 2022; Javaheri et al., 2024).

Despite these strengths, most studies failed to incorporate AI's historical development or technical evolution into their theoretical models or analytical frameworks. For instance, few studies contextualized current cybersecurity applications within AI's transition from rule-based logic to autonomous, data-driven learning systems (Ahmed et al., 2022; Temelkov, 2023). As a result, the influence of historical familiarity or institutional exposure to earlier forms of AI on perceived complexity, readiness, or resistance remains unexplored. This omission limited insight into how evolving institutional memory and AI literacy shaped current adoption behaviors. A significant concern was the lack of standardization in variable definitions and measurement instruments. For instance, terms like "AI adoption," "cybersecurity performance," "regulatory compliance," and "cybersecurity governance and risk management" were operationalized inconsistently, making cross-study comparisons difficult and undermining generalizability (Ashraf et al., 2022; Choithani et al., 2024). Furthermore, some studies lacked a strong theoretical foundation or failed to link their findings to established frameworks, thereby reducing the interpretive strength of their conclusions (Alneyadi et al., 2023; Kang et al., 2024).

Sampling limitations also persist. Many studies relied on small or convenience samples, particularly in exploratory or region-specific contexts. This raised questions about the external validity of their findings, especially when applied to globally regulated financial institutions (Almansoori et al., 2023; Bajunaied et al., 2023). Moreover, few studies have accounted for organizational size, AI maturity, or specific regulatory environments such as OCC banking oversight, NCUA credit union supervision, or SEC compliance requirements, which limits insights into how contextual factors influence adoption outcomes (Ali et al., 2024). This gap was

especially critical given the wide variation in cybersecurity readiness, IT infrastructure, regulatory obligations, workforce adaptation, and cybersecurity skills across financial institutions operating in different jurisdictions.

Statistical precision is another area of concern. While some studies employed robust multivariate techniques, including structural equation modeling (SEM) and regression analysis, others relied solely on descriptive statistics or on insufficiently justified inferential tests. Effect sizes and confidence intervals were often underreported, making it difficult to assess the strength and precision of observed relationships (Ahmed et al., 2022; Norzelan et al., 2024). The present study addressed this limitation through a MANOVA-based analysis that included effect size calculations and a power analysis using G*Power to determine an appropriate sample size. Additionally, while studies frequently described the theoretical benefits of AI cybersecurity tools and risk-based AI cybersecurity strategies, few provided statistically validated evaluations of operational performance. Metrics such as reduced response time, reduction in false positives, or real-time threat neutralization were often presented without empirical evidence or comparative benchmarks (Ebert et al., 2023; Sontan et al., 2024). This lack of rigorous operational validation diminishes the credibility of claims regarding AI's superiority over traditional systems. It underscores the need for future studies, including the present one, to incorporate measurable system performance outcomes into design and analysis.

Another gap in the literature was the limited attention to disconfirming or contradictory evidence. While most studies emphasize AI’s positive influence on cybersecurity, relatively few have explored risks such as AI-induced bias, automation failure, or misalignment between human and machine decision-making (Awosika et al., 2024; Baruwal Chhetri et al., 2024; Rana et al., 2024). Where these issues are mentioned, they were often addressed anecdotally rather

than through rigorous analysis. This imbalance highlighted the need for a balanced theoretical framework, such as the TAM and the DOI model, which incorporates both enabling and inhibiting factors. Table 3 provides a synthesized overview of the key studies reviewed, highlighting their primary focus, identified methodological or conceptual gaps, and how the current study aims to address those deficiencies.

Table 3

Summary of Key Literature Gaps and Their Relevance to the Current Study

Study & Focus	**Gap & Contribution**
Ajayi et al. (2025) – General AI	Lacks adoption factors; conceptually supports adoption research.
Awosika et al. (2024) – General AI	Lacks adoption focus; informs governance
Baruwal Chhetri et al. (2024) – Human-AI Collab	Lacks adoption factors; supports collaboration variable.
Binhammad et al. (2024) – General AI	Misses compliance focus; supports alignment with policy.
Choithani et al. (2024) – AI Models	Misses compliance focus; addresses AI complexity.
Dawodu et al. (2023) – AI Policy	Misses organizational relevance; supports empirical adoption research.
Deshpande (2024) – Regulatory Risk	Misses organizational relevance.
Djenna et al. (2023) – AI Adoption Barriers	Misses compliance focus.
Ebert et al. (2023) – Threat Detection	Lacks adoption focus.
Faraji et al. (2024) – General AI	Lacks empirical validation.
Folorunso et al. (2024) – General AI	Misses compliance focus.
Gopal et al. (2023) – General AI	Overlooks governance; supports compliance framework alignment.
Goswami et al. (2024) – AI Frameworks	Lacks structured adoption model.
Hentzen et al. (2022) – General AI	Misses organizational relevance.
Jahangir et al. (2023) – AI Adoption	Does not consider workforce impact.
Kaur et al. (2023) – Risk Management	Misses organizational relevance.
Mishra (2023) – General AI	Misses compliance focus.
Rizvi (2023) – General AI	Misses compliance focus.
Sai Meghana et al. (2024) – General AI	Overlooks governance aspects.
Udeh et al. (2024) – Legacy Systems	Does not consider workforce impact.
Van Bekkum et al. (2023) – Data Privacy	Lacks adoption factors.
Vial et al. (2024) – Risk Management	Lacks adoption analysis.
Zhong et al. (2024) – Legacy Systems	Lacks adoption factors.

Note: This table summarizes key scholarly sources reviewed in the literature analysis. Each entry identifies the primary research focus, the gap observed in AI-driven cybersecurity adoption, and the study's relevance to current research. The table highlights recurring gaps in empirical validation, regulatory alignment, human-AI collaboration, and the organizational adoption framework. These gaps are addressed in this study through a structured, theory-based investigation that employs the TAM and DOI models in U.S. financial institutions.

Lastly, although many studies address ethical, regulatory, and human factors, few have integrated these perspectives into a unified evaluative model. This fragmented approach limited the utility of existing research for guiding policy and organizational strategy, particularly in cybersecurity governance and risk management, as regulatory frameworks continue to evolve (Gale et al., 2022; López González et al., 2024; Ridzuan et al., 2024). The present study addresses this gap by synthesizing cross-disciplinary findings within a structured quantitative design grounded in two complementary adoption theories.

Summary

Chapter 2 presented an in-depth examination of scholarly research on the adoption and impact of AI-driven cybersecurity technologies in financial institutions. Guided by the TAM and the DOI theories, the review examined how compatibility, complexity, and relative advantage influence implementation success. AI integration depended not only on technical capacity but also on regulatory alignment, governance maturity, and workforce readiness. This also includes the alignment with U.S. financial regulations such as GLBA Safeguards Rule and SEC requirements, and oversight by agencies including the OCC, Federal Reserve, NCUA, and the FIO, as well as secondary frameworks such as GDPR, CCPA, and PCI-DSS (Baruwal Chhetri et al., 2024; Faraji et al., 2024; Udeh et al., 2024; Vial et al., 2024). Improved compatibility

increased trust, compliance, and readiness. Complexity, particularly from opaque algorithms and steep learning curves, hindered adoption, whereas relative advantage supported improvements in threat detection, fraud prevention, and operational efficiency.

The review also highlighted the evolution of AI from rule-based systems to self-learning models, underscoring its expanding role in proactive cybersecurity. Human-AI collaboration emerged as essential, with studies showing that AI was most effective when paired with human oversight for threat analysis, policy interpretation, ethical decision-making, and ongoing workforce adaptation and cybersecurity skills gap. Concerns about data privacy, model explainability, and transparency in governance were consistent themes. While findings converged on the importance of regulatory alignment, they diverged in institutional readiness, resource capability, and ethical governance practices. Studies have also emphasized the need for adaptive AI systems that are responsive to evolving compliance and operational demands.

The critique of methodologies identified inconsistent sampling, limited longitudinal data, and varied statistical rigor. Despite these limitations, the studies offered valuable insights into the promise and challenges of AI in financial cybersecurity. Several studies demonstrated innovative approaches to evaluating the outcomes of AI implementation and the effectiveness of risk-based AI cybersecurity strategies. These identified gaps directly informed the operationalization of variables in Chapter 3 and the empirical testing presented in Chapter 4, ensuring theoretical, methodological, and analytical alignment across the dissertation.

Chapter 3: Research Method

The problem addressed in this study was the increasing complexity of integrating AI into financial cybersecurity while ensuring regulatory compliance, protecting data privacy, and fostering effective human-AI collaboration (Faraji et al., 2024). Financial institutions relied on AI-driven cybersecurity for threat detection, fraud prevention, and the implementation of risk-based AI cybersecurity strategies (Faraji et al., 2024). However, challenges persisted in balancing AI automation with human expertise, maintaining regulatory compliance, and mitigating emerging risks.

A primary concern was AI's impact on data privacy and regulatory compliance. AI-driven cybersecurity processes handle large volumes of sensitive data, creating compliance challenges under international frameworks such as the GDPR and U.S. financial regulations. Commercial banks were regulated by the OCC and the Federal Reserve, credit unions by the NCUA, investment banks by the SEC, and insurance companies by state insurance commissioners in coordination with the FIO (Baruwal Chhetri et al., 2024; Vial et al., 2024). These regulators enforced cybersecurity obligations through measures such as the GLBA Safeguards Rule and SEC Regulation S-P. Misalignment between AI-driven practices and these requirements could have resulted in penalties, reputational harm, and an increased risk of breaches (Rana et al., 2023).

Another critical issue was the evolving role of human expertise in AI-driven cybersecurity. While AI enhanced efficiency, it affected decision-making processes, workforce adaptation, cybersecurity skills gap, and governance strategies (Thapaliya, 2024). AI's lack of explainability further complicates oversight, increasing the risk of bias, false positives, and adversarial attacks (Udeh et al., 2024). Failure to address these challenges could have led to

ineffective AI adoption, regulatory noncompliance, and cybersecurity breaches, ultimately jeopardizing institutional resilience and public trust.

The purpose of this quantitative, correlational study was to examine the relationships among the compatibility, complexity, and relative advantage of AI-driven cybersecurity technologies, and their influence on adoption outcomes and institutional effectiveness in financial institutions. This study examined the impact of these factors on regulatory compliance, fraud prevention, and cybersecurity workforce augmentation (Binhammad et al., 2024). The research employed a survey-based approach to collect data from cybersecurity professionals, IT managers, and compliance officers at financial institutions across the United States. An estimated 10,000 professionals meet the inclusion criteria, based on industry workforce data from national reports on the financial services and cybersecurity sectors (Dawodu et al., 2023). Multivariate Analysis of Variance (MANOVA) was used to determine the required sample size, using the "F tests" and "MANOVA: Global effects" options in G*Power. The analysis employed a medium effect size ($f^2 = 0.15$), a significance level of 0.05 (5%), and a power of 0.80 (80%) to ensure statistical reliability. With three groups for the independent variable and four response variables, the total required sample size was 57 participants.

The study utilized a structured questionnaire to measure perceptions of AI-driven cybersecurity tools and their impact on system performance, adaptability, regulatory compliance, and human-AI collaboration. The TAM and DOI Theory served as the foundation for analyzing the extent to which financial institutions adopted AI for cybersecurity operations. Multiple regression analysis assessed the strength and significance of the relationships between independent variables' compatibility, complexity, and relative advantage and the dependent

variables, including system performance, adaptability, human-AI collaboration, and regulatory compliance.

This chapter outlined the methodological framework for the study. It began by detailing the quantitative, non-experimental, correlational research design and explained why it was suitable for evaluating the relationships among AI-driven cybersecurity constructs and organizational outcomes. The chapter then described the population and sampling strategy, including the rationale for purposive sampling and the procedures for participant recruitment via Qualtrics. The structure and development of the 40-item survey instrument, aligned with four research questions and grounded in TAM and DOI theories, are also presented. Each independent and dependent variable was defined and validated through exploratory and reliability analyses. The chapter further described the data collection procedures, including the pilot study, consent protocols, and measures to protect participant anonymity. The final sections addressed the data analysis strategy using MANOVA and discussed the study's assumptions, limitations, delimitations, and ethical assurances. Together, these components establish a robust, replicable process for examining how perceived AI attributes influence cybersecurity implementation outcomes in the financial sector.

Research Methodology and Design

This study employed a quantitative, non-experimental, correlational research design to examine the extent to which the perceived compatibility, complexity, and relative advantage of AI-driven cybersecurity technologies influenced institutional outcomes in financial organizations. These outcomes included system performance, organizational adaptability, human-AI collaboration, and regulatory compliance. This research design was appropriate given the study's central problem: financial institutions faced increasing complexity in adopting AI

technologies while ensuring cybersecurity, regulatory adherence, collaborative effectiveness, and the implementation of risk-based AI cybersecurity strategies (Mishra, 2023; Udeh et al., 2024). The study's purpose was to assess statistical relationships between perceptions of AI implementation and organizational performance outcomes using structured, real-world data. A quantitative methodology was suitable because it enabled the systematic collection and analysis of numerical data across a broad sample of cybersecurity professionals in the financial services sector (Faraji et al., 2024).

The non-experimental design indicated that no independent variable was manipulated, and the study was conducted in a natural organizational setting without controlled interventions. The correlational approach was appropriate because the goal was to identify statistically significant relationships between naturally occurring variables rather than infer causal effects. As emphasized by Dawodu et al. (2023) and Faraji et al. (2024), correlational research designs were particularly valuable in applied cybersecurity and finance contexts where researchers aimed to understand organizational behavior without disrupting operations. This approach was further supported by Abikoye et al. (2024), who emphasized the importance of structured, quantitative methods for assessing AI's role in managing cybersecurity and risk in both fintech and traditional banking environments. Similarly, Adegbite et al. (2023) underscored the need for observational and correlational designs when assessing real-time cybersecurity implementations across critical infrastructure sectors.

The survey instrument for this study included 40 Likert-scale items, each aligned with one of the study's four research questions. Rather than organizing the survey solely around the three core constructs compatibility, complexity, and relative advantage, the items were structured to assess participant perceptions in direct relation to the four specific institutional outcomes of

interest: (1) system performance and cybersecurity effectiveness, (2) organizational adaptability and resilience, (3) human-AI collaboration and job satisfaction, and (4) regulatory compliance and governance stability. While the 40 survey items were grouped by research question and outcome domain, each item remained grounded in the core theoretical constructs of compatibility, complexity, and relative advantage. These items were validated through exploratory factor analysis (EFA) to ensure construct integrity. This outcome-driven structure enhances the ability to evaluate how each of the three independent constructs influenced institutional effectiveness along multiple dimensions of AI integration.

The study employed Multivariate Analysis of Variance to analyze the data. The MANOVA analysis was well-suited to this study's objectives because it allowed the simultaneous examination of multiple dependent variables while accounting for their potential intercorrelations. This method increased analytical efficiency and reduced the likelihood of Type I error compared to conducting separate analyses for each outcome (Dawodu et al., 2023; Kaur et al., 2023). The use of MANOVA was further supported by recent empirical research. For example, Jony et al. (2024) employed multivariate analysis to assess the impact of AI systems on organizational resilience in cybersecurity. Similarly, Paul et al. (2023) demonstrated that AI-enabled tools significantly affected compliance outcomes and fraud prevention detection capabilities in financial institutions, further validating the statistical approach employed in this study.

Alternative methodologies were reviewed but found unsuitable for the study's goals. A qualitative design, although helpful in uncovering stakeholder insights, was rejected due to its limited generalizability and lack of hypothesis-testing capability, both of which were necessary to address the study's theoretical framework and empirical objectives (Djenna et al., 2023). A

mixed-methods approach was also considered but dismissed due to the added complexity, as the quantitative method sufficiently addressed the research questions. Sontan et al. (2024) noted that mixed-methods designs were most effective when both qualitative and quantitative components were essential. However, this method did not apply to this outcome-focused, theory-driven study.

Experimental and quasi-experimental designs were likewise deemed inappropriate. These designs required manipulating variables and often involved randomized control trials, which were not feasible or ethical in the operational settings of financial institutions. Ajayi et al. (2025) emphasized that the risks of implementing experimental AI interventions in financial cybersecurity systems require observational approaches. Likewise, Binhammad et al. (2024) and Rizvi (2023) explained that cybersecurity operations in sensitive financial contexts require naturalistic data collection methods that reflect real-world conditions and preserve system integrity.

The quantitative, non-experimental, correlational design using MANOVA was the most appropriate approach for this study. It enabled the researcher to assess the impact of AI adoption constructs on multiple organizational outcomes while maintaining methodological rigor, empirical relevance, and theoretical alignment. This approach contributed to a deeper understanding of how perceptions of AI integration shaped cybersecurity effectiveness, regulatory compliance, workforce adaptation, cybersecurity skills gap, and institutional resilience in financial institutions.

Population and Sample

The target population for this study consisted of cybersecurity professionals, IT managers, and compliance officers employed in financial institutions across the United States. These individuals were directly involved in implementing, governing, and overseeing AI-driven

cybersecurity technologies. Their insights were essential for understanding how financial institutions managed complex adoption dynamics, including technology compatibility, system complexity, and the perceived advantages of AI tools while maintaining robust cybersecurity and regulatory compliance frameworks, as noted by Ajayi et al. (2025) and Goswami et al. (2024). Previous research has shown that professionals in these roles play a central role in institutional AI governance, threat detection, and digital risk mitigation efforts (Abikoye et al., 2024; Folorunso et al., 2024).

A purposive sampling strategy was employed to reach this population. This non-probability sampling approach was appropriate for studies that required participants with specialized knowledge and decision-making responsibilities in organizational cybersecurity contexts (Adegbite et al., 2023; Adejumo et al., 2025b). All participants were recruited exclusively via Qualtrics, a professional survey platform that provides access to pre-screened participant panels. The inclusion criteria required that participants be employed at a financial institution in the United States, possess at least three years of experience in cybersecurity, IT governance, or compliance roles, and have familiarity with, or involvement in, AI or machine learning systems used in cybersecurity contexts. Individuals working in non-financial sectors, in academic-only environments, or with fewer than 3 years of relevant experience were excluded from the study.

The study proceeded in two phases: a pilot study and a main study. The pilot phase comprised the first 10 fully completed survey responses obtained through Qualtrics using the same inclusion and exclusion criteria as the main study. The purpose of the pilot was to evaluate the survey instrument for clarity, reliability, and usability. The data from these first 10 surveys

were analyzed to determine the validity and reliability of the questions. These pilot responses were excluded from the overall dataset for the main study.

A power analysis was conducted using G*Power v3.1 to determine the appropriate sample size for the planned MANOVA. With three independent variables, technology compatibility, complexity, and relative advantage, and four dependent variables, cybersecurity performance, adaptability, regulatory compliance, and human-AI collaboration, a medium effect size ($f^2 = 0.25$), an alpha level of 0.05, and a statistical power of 0.80 were assumed. The minimum required sample size was 57 participants. The final dataset used for analysis consisted of 90 valid responses, exceeding the minimum sample size required for statistical power. To account for potential nonresponse or incomplete data, the study aimed to recruit approximately 65 to 70 participants via Qualtrics. This sample size was sufficient to detect meaningful statistical relationships and support generalizability across similar institutional settings. Because the survey was distributed through purposive recruitment channels rather than a controlled sampling frame, an exact response rate could not be calculated. However, the final sample of 90 participants exceeded the minimum sample size required for statistical analysis.

Instrumentation

This study used a structured, self-administered survey instrument to collect quantitative data from cybersecurity professionals, IT managers, and compliance officers at financial institutions. The survey assessed key perceptions related to the adoption of AI-driven cybersecurity technologies, using constructs derived from TAM and DOI. The instrument consisted of 40 items, distributed across the four research questions, ensuring balanced representation of each construct. These items reflected the core constructs of compatibility, complexity, and relative advantage, as well as outcome-focused variables such as system

performance, adaptability, regulatory compliance, and human-AI collaboration. Responses were recorded on a 7-point Likert scale ranging from Strongly Disagree (1) to Strongly Agree (7), a standard approach in empirical research for quantifying attitudes and perceptions (Davis, 1989; Faraji et al., 2024; Udeh et al., 2024).

The 40 survey items aligned with the study's four research questions and associated variables, ensuring comprehensive coverage of the independent variables (compatibility, complexity, and relative advantage) and the four dependent outcomes (system performance, adaptability, human-AI collaboration, and regulatory compliance). This structure supported both construct validity and outcome-specific analysis. Survey items were carefully balanced to minimize variable conceptual overlap while maintaining alignment with the four research questions and their corresponding variables. The survey items were adapted from previously validated measurement scales widely used in technology adoption research. Items measuring compatibility and relative advantage were derived from the innovation attribute constructs originally defined in Diffusion of Innovations theory (Rogers, 2003) and subsequently applied in cybersecurity and AI adoption research (Udeh et al., 2024). Items reflecting perceptions of technology usefulness and implementation alignment were adapted from TAM framework scales developed by Davis (1989). To ensure contextual relevance, the wording of these items was modified to reflect the financial cybersecurity environment, specifically focusing on AI-driven threat detection, fraud prevention, and regulatory compliance processes. This adaptation ensured that the instrument retained the conceptual integrity of the original validated scales while aligning the items with the operational realities of cybersecurity professionals working within financial institutions. These instruments were selected for their demonstrated psychometric strength, with prior studies reporting Cronbach's alpha values exceeding .80 in contexts

involving AI, cybersecurity, and technology adoption (Folorunso et al., 2024; Kaur et al., 2023). The items were organized by research question to ensure alignment with the theoretical constructs and maintain consistency across models, as demonstrated by Djenna et al. (2023) and Jony et al. (2024).

A pilot study was conducted using the first 10 completed survey responses collected through the Qualtrics platform. The purpose of the pilot was to evaluate the survey instrument's functionality, confirm the clarity of item wording, and assess the reliability of the measures. The pilot also verified that the survey distribution process was functioning correctly. No major revisions were expected unless significant usability or measurement integrity issues arose. Any necessary adjustments identified during this pilot phase were incorporated, and the remaining responses constituted the primary study dataset. The first 10 responses used in the pilot were excluded from the main study dataset.

The finalized survey was administered via Qualtrics, a secure web-based data-collection platform recognized for its compliance with ethical standards and data protection protocols. No identifying information (e.g., names, IP addresses, or email addresses) was collected, ensuring complete participant anonymity. All data were encrypted, securely stored in access-restricted files, and handled solely by the primary researcher. These procedures complied with Institutional Review Board (IRB) protocols to maintain participant confidentiality, data integrity, and research transparency (Binhammad et al., 2024; Folorunso et al., 2024; Salem et al., 2024). A comprehensive table of survey items, categorized by research questions and theoretical constructs, was provided in Appendix B.

Operational Definitions of Variables

This study examines the impact of independent variables, including compatibility, complexity, and relative advantage, on four dependent variables: system performance and cybersecurity effectiveness, adaptability and resilience, human-AI collaboration and job satisfaction, and regulatory compliance and governance stability. Each variable is operationalized using a structured, self-administered survey distributed via Qualtrics. Survey responses are recorded on a 7-point Likert scale, ranging from "Strongly Disagree" (1) to "Strongly Agree" (7). The survey is designed to capture nuanced perceptions across diverse institutional roles, including cybersecurity professionals, IT managers, and compliance officers. This method enables consistent and scalable data collection from a geographically diverse, distributed participant pool.

Each of the four research questions is represented by a dedicated subset of survey items aligned with its corresponding constructs and outcome variables. This alignment ensures that each research question addresses the constructs and outcomes defined by TAM and DOI. While seven targeted items measure each construct, some may serve dual roles, reflecting conceptual and statistical interrelationships among variables. A complete list of survey items by variable is provided in Appendix B. All variables were analyzed using multivariate techniques, as detailed in the Data Analysis section.

Compatibility (Independent Variable)

Compatibility refers to the degree to which AI-driven cybersecurity technologies align with an institution’s existing technical infrastructure, regulatory obligations, security protocols, and organizational values. This variable was measured using 7 Likert-scale items adapted from Davis (1989) and Udeh et al. (2024). This scale has demonstrated strong internal consistency in

prior studies (Cronbach's $\alpha > .80$) and was further validated through pilot testing. This variable is essential for understanding how alignment with institutional frameworks affects the successful adoption of AI in financial cybersecurity systems.

Complexity (Independent Variable)

Complexity refers to the perceived difficulty in understanding, learning, implementing, and integrating AI cybersecurity technologies. It encompasses algorithmic transparency, technical skill requirements, and integration with legacy systems. This variable was measured using 7 Likert-scale items adapted from Faraji et al. (2024), based on DOI theory. These items have previously demonstrated acceptable internal reliability ($\alpha > .80$) and were revalidated through pilot testing. This variable is critical for identifying institutional readiness and barriers to adoption in regulated environments.

Relative Advantage (Independent Variable)

Relative advantage refers to the perceived benefit of AI-driven cybersecurity tools compared to traditional methods. Benefits may include improved threat detection, enhanced fraud prevention, faster response times, and operational efficiency. It was measured using 7 Likert-scale items adapted from Rogers (2003) and Udeh et al. (2024). These instruments have previously demonstrated strong internal consistency ($\alpha > .85$) and were pilot-tested for this study. This variable is central to evaluating adoption motivation and the influence of perceived performance improvements on implementation decisions.

System Performance and Cybersecurity Effectiveness (Dependent Variable)

This variable assesses the extent to which AI contributes to measurable improvements in security operations, including detection accuracy, fraud detection speed, and incident response capability. It was measured using 7 Likert-scale items adapted from Binhammad et al. (2024),

who highlight the impact of AI on operational performance and threat mitigation. Prior applications report strong internal consistency ($\alpha > .82$). This variable is essential to determining AI's technical value to cybersecurity infrastructure.

Adaptability and Resilience (Dependent Variable)

Adaptability and resilience reflect an institution's capacity to adjust its use of AI tools in response to evolving cyber threats, compliance requirements, and business demands. This variable was measured using seven Likert-scale items adapted from Mishra (2023) that examine agility, learning, and real-time responsiveness. The original instruments demonstrated internal consistency above $\alpha > .80$. This variable captures the long-term sustainability and flexibility of AI integration into cybersecurity systems.

Human-AI Collaboration and Job Satisfaction (Dependent Variable)

The Human-AI Collaboration and Job Satisfaction variable assesses the perceived quality of interactions between AI systems and cybersecurity professionals. It encompasses perceptions of AI-enhanced decision-making, task support, trust, and the impact on job roles and satisfaction. It was measured using 7 scale items adapted from Baruwal Chhetri et al. (2024). These items have demonstrated internal consistency above $\alpha > .80$ in prior human-AI studies. This variable is vital to understanding how AI affects the human workforce and collaborative cybersecurity processes.

Regulatory Compliance and Governance Stability (Dependent Variable)

The Regulatory Compliance and Governance Stability variable measures the extent to which AI adoption helps institutions meet cybersecurity regulations, including the OCC, Federal Reserve, NCUA, SEC, FIO, GLBA, and GDPR, while also addressing CCPA and PCI DSS to maintain governance stability. It was measured using 7 scale items adapted from López González

et al. (2024) and Vial et al. (2024), focusing on data privacy, ethics, and regulatory alignment. Both sources reported internal consistency above α = .82. This variable is crucial for assessing the legal and operational viability of AI technologies within a compliance-focused financial sector.

Study Procedures

This study followed a structured, sequential process to ensure methodological consistency, research integrity, and alignment with the research objectives, including cybersecurity governance and risk management considerations. The first step was to obtain formal approval from the IRB at National University. The IRB submission included the full research proposal, informed consent form, survey instrument, recruitment message, and all supporting documentation. In accordance with university policies and ethical standards for research involving human participants, no data collection commenced until official IRB approval was obtained.

Following IRB approval, a pilot study was conducted to ensure the survey instrument functioned properly during the initial stage of data collection. A small group of approximately 10 individuals who met the target population criteria for cybersecurity professionals, IT managers, or compliance officers was invited to participate in the pilot study. The pilot survey was deployed via Qualtrics and included the same 40 Likert-scale items as the main instrument to evaluate clarity, timing, and item performance. Participants were asked to identify confusion, technical issues, or usability issues.

The data from the first 10 respondents were reviewed to identify any issues related to item wording, clarity, or functionality. Revisions were made as needed to enhance precision, eliminate redundancy, and address structural concerns before analyzing the remaining responses.

As the pilot was embedded in the initial data collection process, no separate timeline was required between the pilot and the primary survey.

Upon completion of the pilot and finalization of the survey instrument, participant recruitment began. A purposive sampling strategy was used to identify and engage cybersecurity professionals, IT managers, and compliance officers working at financial institutions in the United States. This study considered these individuals well-suited to participate, given their direct involvement in evaluating, implementing, and managing AI-driven cybersecurity solutions and risk-based AI cybersecurity strategies (Folorunso et al., 2024). Recruitment occurred through prescreened participant panels provided by Qualtrics. A standardized digital invitation introduced the study, outlined eligibility requirements, and included a secure Qualtrics link to the online survey.

When participants accessed the survey, they first encountered an electronic informed consent form embedded at the beginning of the instrument. The consent form outlined the study's purpose, the voluntary nature of participation, and participants' right to withdraw at any time without penalty. Only participants who provided informed consent proceeded to the full survey. The instrument was structured and self-administered and consisted of 40 closed-ended Likert-scale items distributed across the study's four research questions. These items assessed perceptions of the three independent variables, compatibility, complexity, and relative advantage, and the four dependent variables: system performance and cybersecurity effectiveness, adaptability and resilience, human-AI collaboration and job satisfaction, and regulatory compliance and governance stability. The items were adapted from previously validated instruments grounded in the TAM and the DOI theory (Faraji et al., 2024; Udeh et al., 2024). Each item was rated using a 7-point Likert scale ranging from 1 (Strongly Disagree) to 7

(Strongly Agree). The estimated time to complete the survey was approximately 30-60 minutes, depending on the participant's pace and familiarity with the content.

The survey remained open for at least four weeks or until the required sample size of 57 participants was reached; data collection continued beyond this threshold to strengthen statistical power and robustness. If participation was low, the recruitment period was extended and reinforced with additional targeted outreach. No personally identifiable information (PII) was collected to ensure participant anonymity. All data were securely captured and stored within the Qualtrics system, which used industry-standard encryption protocols to ensure data confidentiality (Paul et al., 2023). After data collection, the entire dataset was exported and stored on a password-protected, encrypted device accessible only to the primary researcher. In accordance with National University's data management policies, all research data were retained for five years and permanently deleted thereafter. Before formal analysis, the dataset was screened for completeness and quality. Several measures were implemented to minimize potential response bias and enhance data integrity. First, the survey was conducted anonymously, and no personally identifiable information was collected, reducing the likelihood of social desirability bias and encouraging candid responses from participants. Second, survey items were written using neutral wording and balanced statements to avoid leading respondents toward specific answers. Third, the Qualtrics platform restricted participation to pre-screened individuals who met the study's inclusion criteria, reducing the likelihood of irrelevant responses. Finally, data screening procedures were used to identify incomplete responses, straight-lining patterns, and other indicators of inattentive responding. These procedures helped mitigate both social desirability bias and nonresponse bias while improving the overall reliability of the dataset. Only valid and complete responses were retained for statistical analysis.

Data Analysis

This study utilized MANOVA to evaluate the extent to which the independent variables compatibility, complexity, and relative advantage influenced the combined effects of the four dependent variables: (1) system performance and cybersecurity effectiveness, (2) adaptability and resilience, (3) human-AI collaboration and job satisfaction, and (4) regulatory compliance and governance stability. MANOVA was appropriate because it permitted the simultaneous analysis of multiple dependent variables, accounted for intercorrelations among them, and reduced the likelihood of Type I errors that could have resulted from conducting separate univariate tests (Davis, 1989; Faraji et al., 2024). This approach enabled a more comprehensive examination of the institutional impact of AI-driven cybersecurity technologies. It also supported the theoretical model by testing whether innovation characteristics influenced multiple organizational outcomes in an integrated manner.

Before conducting MANOVA, the survey instrument, comprising 40 Likert-scale items aligned with the study's four research questions, underwent EFA. The EFA aimed to validate whether the item groupings by research question reflected coherent underlying latent variables consistent with the theoretical constructs derived from the TAM and DOI. Although items were organized by research question, EFA confirmed that they loaded appropriately onto latent factors aligned with the study's core constructs (e.g., compatibility, complexity, and relative advantage). This step was critical for establishing construct validity and ensuring theoretical coherence. As part of the instrument development process, the first 10 fully complete survey responses served as the pilot test. The pilot data were analyzed to identify problematic survey items, to evaluate initial internal consistency using Cronbach's alpha, and to verify preliminary construct validity through item-total correlations and exploratory factor loadings. The results of this analysis

determined whether the instrument demonstrated acceptable reliability and validity. The pilot responses were excluded from the main study's dataset.

To further assess the instrument's reliability and construct validity, internal consistency for each item group was evaluated using Cronbach's alpha, with $\alpha \geq 0.70$ considered acceptable (Kaur et al., 2023). Exploratory Factor Analysis evaluated construct validity and determined whether items loaded appropriately onto the expected theoretical dimensions. If supported by the sample size and model fit indices, Confirmatory Factor Analysis (CFA) could be considered; however, the primary validation procedure relied on EFA and reliability testing (Chung et al., 2020; Faraji et al., 2024). Once validity and reliability were confirmed, descriptive statistics were generated to summarize participant demographics and item-level responses. Assumption testing for MANOVA, including checks for multivariate normality, linearity, and homogeneity of covariance matrices, was conducted to ensure that the statistical prerequisites were met before proceeding with the primary analysis.

MANOVA was then conducted to test statistically significant relationships for statistically significant multivariate effects of the independent variables on the combined dependent variables. This procedure aligned with the study's multivariate structure and theoretical foundation, enabling an in-depth examination of how AI-driven cybersecurity perceptions impacted institutional outcomes in financial organizations (Mishra, 2023; Rogers, 2003). MANOVA was further validated by its widespread use in studies of organizational technology adoption, where multiple interrelated outcomes were evaluated. It provided the statistical rigor necessary to detect both main and interaction effects. If multivariate significance was found, post hoc tests were conducted to identify which specific dependent variables were affected. A

multiple-comparison correction method was applied to reduce the risk of Type I errors in these comparisons (Kaur et al., 2023).

All statistical analyses were conducted using SPSS software. Statistical significance was assessed at an alpha level of .05. In addition to reporting p-values, effect sizes (e.g., partial eta squared) were calculated to evaluate the magnitude and practical relevance of observed effects. Partial eta squared was selected due to its interpretability in MANOVA contexts, enabling meaningful comparisons of effect sizes across dependent variables. These procedures ensured the findings were statistically robust and practically informative, supporting the study's contribution to understanding AI-driven cybersecurity adoption in financial institutions.

Assumptions

Several foundational assumptions underpinned this study. First, it was assumed that participants would provide honest, thoughtful, and accurate responses to the survey instrument, supported by the anonymous and voluntary nature of participation (Paul et al., 2023). Second, it was assumed that the survey items adapted from previously validated instruments appropriately captured the variables of compatibility, complexity, and relative advantage, as defined by TAM and DOI theory (Davis, 1989; Rogers, 2003). Third, the study assumed that participants, who include cybersecurity professionals, IT managers, and compliance officers in financial institutions, possessed the relevant domain knowledge and practical experience necessary to assess their organization's adoption of AI cybersecurity tools (Jony et al., 2024). Finally, the study assumed that self-reported data accurately reflected participants' attitudes and organizational practices, even though these perceptions might not have corresponded directly to objective performance data, such as system logs or audits.

Limitations

Despite careful design, several limitations may have influenced the study's scope, interpretation, and generalizability. First, the use of purposive sampling limits randomization and may have introduced bias due to participant self-selection (Adegbite et al., 2023). This limitation reduced the extent to which findings could be generalized beyond the sample. Second, participant recruitment via Qualtrics panels may have unintentionally excluded qualified individuals who were not represented on these platforms, thereby narrowing sample diversity (Folorunso et al., 2024). Third, the study's cross-sectional design captured participant responses simultaneously, limiting the ability to observe evolving patterns in AI adoption (Kaur et al., 2023). Fourth, the study was geographically limited to financial institutions operating within the United States, which may have reduced the applicability of findings to global contexts (Thapaliya, 2024).

Fifth, due to time and resource constraints, no follow-up interviews or qualitative data collection were conducted, which may have limited the depth of contextual understanding. However, this was a deliberate methodological choice aligned with the study's quantitative design (Mishra, 2023). Sixth, because data collection was based solely on self-reported perceptions rather than objective technical performance records, the study may not have fully captured the operational effectiveness of AI tools. Lastly, the first 10 responses used for the pilot study were excluded from the main dataset to ensure that the statistical results reflected only the remaining responses. Collectively, these limitations were considered during the study design and were addressed through careful alignment of the research questions, instrumentation, and analytical procedures. Acknowledging these constraints supports transparent interpretation of the

findings and provides appropriate context for the methodological choices described in this chapter.

Delimitations

This study was intentionally delimited to address specific research goals and maintain alignment with its theoretical framework and quantitative methodology. First, the population was limited to cybersecurity professionals, IT managers, and compliance officers working in U.S.-based financial institutions. Other sectors, such as healthcare, education, and government, were excluded to ensure a focused analysis and sector-specific relevance (Udeh et al., 2024). Second, the study focused on three core innovative attributes derived from TAM and DOI: compatibility, complexity, and relative advantage (Davis, 1989; Rogers, 2003). Other potentially influential constructs, such as perceived risk, trust, organizational readiness, and return on investment, were excluded, even though they may have impacted adoption decisions (Faraji et al., 2024). Third, the study was limited to AI-driven cybersecurity applications, including machine-learning-based threat detection, behavioral analytics, and automated incident response systems (Ebert et al., 2023; Rizvi, 2023). Broader AI uses unrelated to cybersecurity (e.g., chatbots or AI-enabled investment advisors) fall outside the scope. These delimitations were established to narrow the study focus, strengthen internal consistency, and enable a theory-driven examination of AI technology adoption in financial cybersecurity environments.

Ethical Assurances

To ensure ethical integrity, the researcher followed all research procedures outlined by the National University's Institutional Review Board. To minimize participants' risk, the researcher did not collect any data until formal IRB approval was obtained from the National University. This approval ensured that the study's design, recruitment strategy, data collection

instruments, and participant protections aligned with federal regulations and institutional policies governing human subject research.

All participants provided informed consent before participating in the study. The researcher presented a digital consent form that clearly outlined the study's purpose, procedures, potential risks and benefits, and the voluntary nature of participation. The form also explained participants' right to withdraw from the study at any time without penalty. The survey platform only allowed participants to proceed if they consented. Although the study used an anonymous online format, the researcher obtained any necessary site permissions when required by the recruitment platform or organization (e.g., Qualtrics). If required, the researcher secured those permissions before initiating recruitment. The study did not collect PII, and the system did not associate responses with individual participants or organizations. This approach safeguarded confidentiality and minimized risk.

All data were stored in encrypted, password-protected digital environments accessible only to the principal investigator. The data were used solely for academic research purposes and were not shared with third parties. The study did not involve vulnerable populations or high-risk procedures. The survey focused on professionals' perceptions of AI-driven cybersecurity technologies and excluded intrusive or sensitive questions, thereby minimizing risk to participants. These ethical safeguards protected participant rights, upheld data confidentiality, and ensured the responsible conduct of research. The researcher adhered to all institutional and federal guidelines for human subject research and remained committed to upholding the highest ethical standards throughout the research process.

Summary

This chapter outlined the methodological framework guiding this quantitative, non-experimental, correlational study, which examined how perceived compatibility, complexity, and relative advantage of AI-driven cybersecurity technologies influenced key institutional outcomes in U.S. financial institutions. The research design was justified as appropriate for examining naturally occurring relationships between independent and dependent variables in real-world organizational contexts. It identified the target population of cybersecurity professionals, IT managers, and compliance officers, and explained the purposive sampling strategy and the recruitment procedures conducted through Qualtrics. The chapter also detailed the development of a 40-item Likert-scale survey instrument based on validated constructs from the TAM and DOI theory. Each of the four research questions corresponded to a distinct subset of survey items aligned with the independent constructs and dependent outcomes tested through MANOVA.

Each variable was operationally defined, with plans to assess construct validity and reliability using EFA and Cronbach's alpha. The chapter explained the rationale for using MANOVA as the primary data analysis technique, highlighting its suitability for evaluating multiple dependent variables simultaneously, accounting for intercorrelations, and reducing Type I errors. Finally, the chapter discussed the study's underlying assumptions, limitations, and delimitations, as well as the ethical safeguards implemented to protect participants and ensure compliance with institutional and federal research guidelines. Collectively, these methodological elements established a rigorous and replicable research process that set the stage for the data analysis and results presented in Chapter 4.

Chapter 4: Findings

The problem addressed in this study was the increasing complexity of integrating AI into financial cybersecurity while ensuring regulatory compliance, protecting data privacy, and fostering effective human-AI collaboration (Faraji et al., 2024). Financial institutions relied on AI-driven cybersecurity for threat detection, fraud prevention, and risk mitigation (Faraji et al., 2024). However, challenges persisted in balancing AI automation with human expertise, maintaining regulatory compliance, and mitigating emerging risks.

A primary concern was AI's impact on data privacy and regulatory compliance. AI-driven cybersecurity processes handle large volumes of sensitive data, creating compliance challenges under international frameworks such as the GDPR and U.S. financial regulators. Commercial banks were regulated by the OCC and the Federal Reserve, credit unions by the NCUA, investment banks by the SEC, and insurance companies by state insurance commissioners in coordination with the FIO (Baruwal Chhetri et al., 2024; Vial et al., 2024). These regulators enforced cybersecurity obligations through measures such as the GLBA Safeguards Rule and SEC Regulation S-P. Misalignment between AI-driven practices and these requirements could result in penalties, reputational harm, and an increased risk of breaches (Rana et al., 2023).

Another critical issue was the evolving role of human expertise in AI-driven cybersecurity. While AI enhanced efficiency, it affected decision-making processes, workforce adaptation, and governance strategies (Thapaliya, 2024). AI's lack of explainability further complicates oversight, increasing risks of bias, false positives, and adversarial attacks (Udeh et al., 2024). Failure to address these challenges may result in ineffective AI adoption, regulatory

non-compliance, and cybersecurity failures, ultimately jeopardizing institutional resilience and public trust.

The purpose of this quantitative, correlational study was to examine the relationships between compatibility, complexity, and relative advantage of AI-driven cybersecurity technologies, and their adoption and success in financial institutions. This study assessed how these factors influence regulatory compliance, fraud prevention, and cybersecurity workforce augmentation (Binhammad et al., 2024). The research employed a survey-based approach to collect data from cybersecurity professionals, IT managers, and compliance officers in financial institutions across the United States. An estimated 10,000 professionals meet the inclusion criteria, based on industry workforce data from national reports on the financial services and cybersecurity sectors (Dawodu et al., 2023). Multivariate Analysis of Variance was used to determine the required sample size, with “F tests” and “MANOVA: Global effects” in G*Power. The analysis used a medium effect size ($f^2 = 0.15$), a significance level of 0.05 (5%), and a power of 0.80 (80%) to ensure statistical reliability. With three groups for the independent variable and four response variables, the total required sample size is 57 participants.

The study utilized a structured questionnaire to measure perceptions of AI-driven cybersecurity tools and their impact on system performance, adaptability, regulatory compliance, and human-AI collaboration. The TAM and the DOI theory served as the foundation for analyzing the extent to which financial institutions adopt AI for cybersecurity operations. Multivariate Analysis of Variance (MANOVA) assessed the strength and statistical significance of the relationships between the independent variables compatibility, complexity, and relative advantage and the dependent variables, including system performance, adaptability, human-AI collaboration, and regulatory compliance. This chapter presents the results of the statistical

analyses conducted to evaluate the relationships among the study variables and to address the four research questions. The chapter is organized to ensure a systematic presentation of findings that align directly with each research question and its corresponding hypothesis. The first section discusses the instrument's validity and reliability to confirm the appropriateness of the data for analysis. The next section describes the assumptions of the statistical tests and how they were met or addressed. Following this, the results of the analyses are presented, organized by research questions and hypotheses. Each section of the research question includes a description of the statistical findings and their interpretation with respect to the study's objectives. Finally, the chapter concludes with a comparison of the results to the existing literature and a summary of key findings that provide a foundation for the discussion in Chapter 5.

Validity and Reliability

The survey instrument's validity and reliability were established to ensure the accuracy and consistency of the data collected for this quantitative correlational study. This section provides an overview of the procedures used to verify that the instrument measured the intended constructs derived from TAM and DOI theory. Establishing validity confirmed that the survey items accurately reflected the underlying theoretical variables of compatibility, complexity, and relative advantage, as well as their influence on dependent variables such as system performance, adaptability, human-AI collaboration, and regulatory compliance. Reliability testing, on the other hand, assessed the internal consistency of the survey items to ensure the instrument produced stable, dependable results across respondents. Both forms of evaluation, validity and reliability, were assessed through exploratory factor analysis (EFA) and internal consistency testing using Cronbach's alpha. Together, these assessments ensured that the survey instrument provided credible and replicable measures suitable for subsequent multivariate analyses, including

MANOVA, to test the study's hypotheses and address the research questions. Establishing strong construct validity and reliability ensured that subsequent MANOVA findings reflected true relationships among study variables rather than measurement error.

Instrument validity was established through a systematic process to ensure that the survey accurately measured the theoretical constructs derived from TAM and DOI theory (Davis, 1989; Faraji et al., 2024; Mishra, 2023; Rogers, 2003; Udeh et al., 2024). The instrument's items were developed from prior peer-reviewed studies on technology adoption and cybersecurity integration, then adapted to the financial sector context to align with the study's focus on AI-driven cybersecurity technologies. Content validity was initially established by aligning the items with existing literature, confirming that each item corresponded to its intended construct in terms of compatibility, complexity, or relative advantage (Faraji et al., 2024; Mishra, 2023; Udeh et al., 2024).

Construct validity was then evaluated using an EFA on the full dataset (n = 90). The EFA was conducted to determine whether the observed items appropriately loaded onto their intended latent variables, demonstrating that each survey item reflected its theoretical construct with minimal cross-loading. Before extraction, the Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy and Bartlett's Test of Sphericity were assessed to verify the suitability of the data for factor analysis. As shown in Table 4, the KMO value of .930 exceeded the recommended threshold of .60, indicating sampling adequacy. Additionally, Bartlett's Test of Sphericity was significant ($\chi^2 = 5404.017$, $df = 780$, $p < .001$), confirming the correlation matrix was factorable and appropriate for proceeding with EFA. Together, these preliminary diagnostics provided empirical justification for extracting latent factors and interpreting the resulting factor structure with confidence.

Table 4

KMO & Barlett's Test

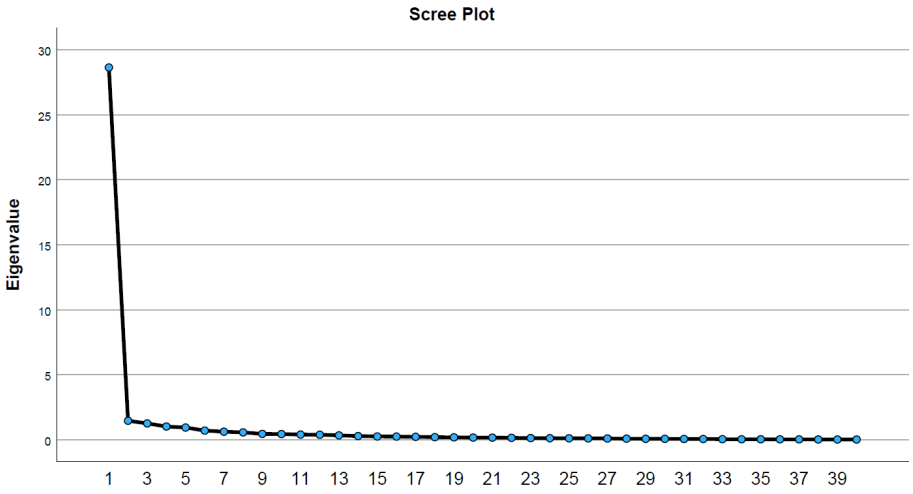
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.930
Barlett's Test of Sphericity	Approx. Chi Square	5404.017
	df	780
	Sig.	<.001

Note. The KMO measure of sampling adequacy was 0.93, exceeding the recommended threshold of 0.60 and indicating excellent suitability for factor analysis. Bartlett's Test of Sphericity was statistically significant, χ^2 (780) = 5404.02, $p < .001$, confirming that correlations among the survey items were sufficiently significant for factor extraction. These results confirm that the dataset met the requirements for conducting an EFA.

Following confirmation of sampling adequacy, the exploratory factor analysis was conducted using principal-axis factoring with oblimin rotation to account for potential correlations among the latent constructs. This combination of extraction and rotation was appropriate because the theoretical foundations of TAM and DOI indicate expected relationships among constructs such as compatibility, complexity, and relative advantage. As shown in the Scree Plot in Figure 3, a distinct inflection point appeared after the fourth factor, suggesting that four factors should be retained in the final solution. This finding aligns with the study's theoretical expectations and provides empirical support for the instrument's ability to capture four underlying latent constructs, consistent with Davis's (1989) TAM and Rogers's (2003) DOI framework. Retaining this factor structure ensured conceptual coherence between the empirical results and the theoretical model guiding the study. Additionally, this alignment strengthened confidence that subsequent analyses were based on a measurement model that accurately reflected the intended constructs.

Figure 3

Screen Plot illustrating factor extraction and variance explained by each construct



Note. The Screen Plot displays the eigenvalues for each extracted factor in the EFA. The sharp decline after the fourth factor indicates a clear inflection point, supporting retaining four primary factors. This pattern confirms that the instrument measures four underlying latent constructs, consistent with the theoretical frameworks of TAM and DOI.

To further confirm construct validity, the Factor Matrix was reviewed to examine factor loadings across constructs. As shown in Table 5, survey items load strongly on their intended factors, with minimal cross-loading across unrelated variables. This pattern validated that the instrument accurately captured the dimensions of compatibility, complexity, and relative advantage, as well as outcome variables such as system performance and regulatory compliance. Although the rotation required multiple iterations to converge, the resulting loading remained theoretically consistent with the expected model structure. This convergence behavior indicated a stable factor solution despite the inherent inter-item correlations in multidimensional cybersecurity constructs.

Table 5

Factor Matrix

Variable	Factor			
	1	2	3	4
Complexity	0.902			
Regulatory Compliance & Governance Stability	0.899			
Compatibility	0.899			
Data Privacy Protection	0.888			
Relative Advantage	0.888			
Compatibility	0.886			
Compatibility	0.879			
Regulatory Compliance & Governance Stability	0.878			
Fraud Prevention	0.877			
Fraud Prevention	0.875			
Complexity	0.871			
Complexity	0.871			
Regulatory Compliance & Governance Stability	0.871			
Data Privacy Protection	0.868			
Job Satisfaction	0.865			
Relative Advantage	0.862			
Regulatory Compliance & Governance Stability	0.859			
Regulatory Compliance & Governance Stability	0.856			
Workforce Augmentation / Human-AI Workforce Integration	0.853			
Workforce Augmentation / Human-AI Workforce Integration	0.850			
Job Satisfaction	0.849			
Job Satisfaction	0.846			
Job Satisfaction	0.840			
Fraud Prevention	0.838			
Job Satisfaction	0.838			
Fraud Prevention	0.837			
Data Privacy Protection	0.829			
Human-AI Collaboration	0.828			
System Performance & Cybersecurity Effectiveness	0.821			
System Performance & Cybersecurity Effectiveness	0.815			
System Performance & Cybersecurity Effectiveness	0.815			
System Performance & Cybersecurity Effectiveness	0.813			
System Performance & Cybersecurity Effectiveness	0.797			
Adaptability & Resilience	0.794		0.449	
Compatibility	0.794			
Workforce Augmentation / Human-AI Workforce Integration	0.794			
Human-AI Collaboration	0.790			
Adaptability & Resilience	0.767			
Human-AI Collaboration	0.756		0.465	
Compatibility	0.712			

Note. The Factor Matrix displays the unrotated factor loadings generated through EFA. All observed variables demonstrated strong loadings (≥ .70) on their intended factors, with minimal cross-loadings across unrelated constructs. These results confirm that the survey items reliably represented their theoretical dimensions, *compatibility, complexity, relative advantage,* and key outcome variables, such as *system performance, adaptability, and regulatory compliance.* The high loading values indicate that each item contributed meaningfully to its underlying construct, supporting the instrument's construct validity. Although the rotation required multiple iterations to converge, the final solution remained theoretically coherent with the study's conceptual framework.

Results of the EFA supported the survey instrument's theoretical structure, with items clustering around their expected factors. Items that did not load strongly on their intended variables were reviewed for theoretical justification and retained if they showed conceptual alignment and acceptable factor loadings. These results confirmed that the instrument possessed strong construct validity, accurately reflecting the study's theoretical framework and ensuring that the constructs of compatibility, complexity, and relative advantage were appropriately measured in the context of financial cybersecurity adoption.

Assumptions of Test

Before conducting MANOVA, the dataset was examined to ensure that the fundamental assumptions required for the analysis were met. The statistical assumptions evaluated included normality, linearity, homogeneity of variance-covariance matrices, multicollinearity, and independence of observations. These tests were performed using IBM SPSS Statistics on the complete dataset of 90 responses to confirm the data's suitability for MANOVA and to support the validity of the inferential results.

The assumption of normality was first evaluated for both analysis routes shown in. Route A, which utilized the original eight dependent variables, system performance, adaptability, human-AI collaboration, job satisfaction, data privacy, regulatory compliance, fraud prevention, and workforce augmentation normality, was assessed using the Shapiro–Wilk test and by reviewing skewness and kurtosis statistics, shown in Table 6. All dependent variables exhibited skewness and kurtosis values within the acceptable range of -2 to +2, indicating approximately normal distributions. Similarly, for Route B, presented in Table 7, which included seven dependent variables after merging data privacy and regulatory compliance into a composite construct, normality was maintained with no significant deviations. Although slight departures were observed for a few variables, these were deemed acceptable, given that MANOVA is robust to moderate violations of normality when the sample size exceeds 50 cases, as in this study.

Table 6

Normality Testing (Skewness & Kurtosis for Route A

	Kolmogorov-Smirnova			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
DV1_SystemPerformance	.132	90	<.001	.934	90	<.001
DV2_Adaptability	.143	90	<.001	.935	90	<.001
DV3_HumanAI	.136	90	<.001	.928	90	<.001
DV4_JobSatisfaction	.123	90	.002	.934	90	<.001
DV5_DataPrivacy	.104	90	.018	.935	90	<.001
DV6_RegCompliance	.118	90	.003	.944	90	<.001
DV7_FraudPrevention	.117	90	.004	.930	90	<.001
DV8_WorkforceAug	.120	90	0.003	0.939	90	<.001

Note. The Shapiro–Wilk and Kolmogorov–Smirnov tests indicated statistically significant departures from normality ($p < .001$) for all dependent variables. However, given the sample size ($N = 90$), minor deviations from normality are expected and are not uncommon. Additionally, skewness and kurtosis values for all variables fell within the acceptable ±2 range, indicating that

the distributions were approximately normal for MANOVA. Therefore, the assumption of normality was considered adequately met.

Table 7

Normality Testing (Skewness & Kurtosis for Route B)

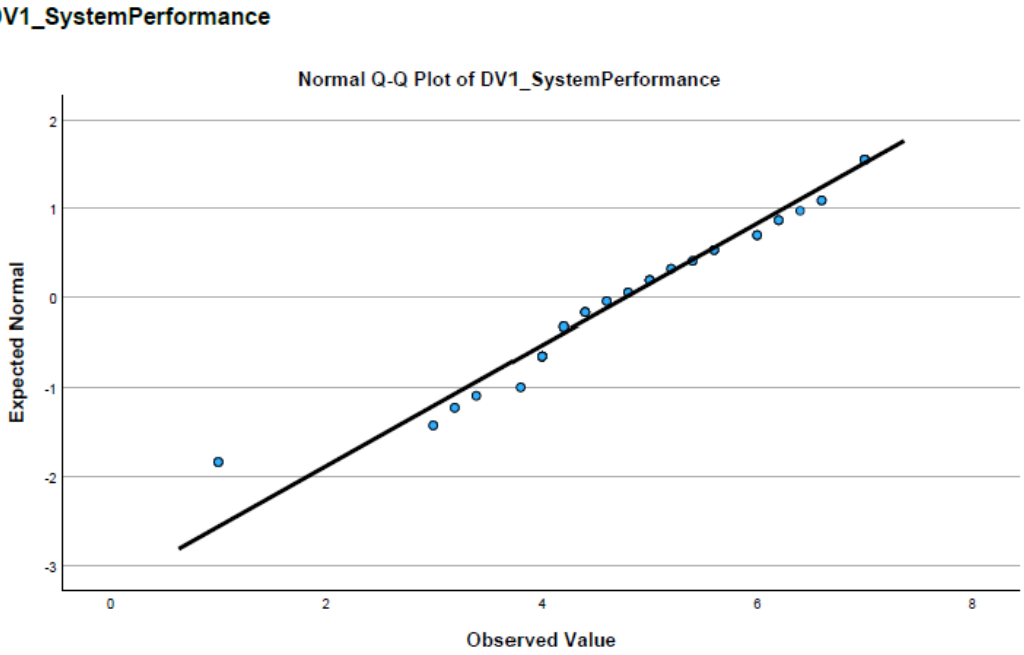
	Kolmogorov-Smirnova			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Data Privacy & Regulatory Compliance	.102	90	.021	.942	90	<.001
DV1_SystemPerformance	.132	90	<.001	.934	90	<.001
DV2_Adaptability	.143	90	<.001	.935	90	<.001
DV3_HumanAI	.136	90	<.001	.928	90	<.001
DV4_JobSatisfaction	.123	90	0.002	.934	90	<.001
DV7_FraudPrevention	.117	90	0.004	.930	90	<.001
DV8_WorkforceAug	.120	90	0.003	.939	90	<.001

Note. The Kolmogorov–Smirnov and Shapiro–Wilk tests returned statistically significant results ($p < .05$) for all dependent variables, including the composite variable Data Privacy & Regulatory Compliance, indicating deviations from perfect normality. However, with a sample size of $N = 90$, these tests are susceptible to minor distributional differences. Review of skewness and kurtosis values for all variables confirmed that each remained within the acceptable ±2 threshold, indicating that the distributions are sufficiently close to normal for MANOVA. Therefore, the assumption of normality for Route B was considered reasonably satisfied.

Compliance variables were combined into a single composite variable, reducing redundancy and improving the stability of the determinants. All Shapiro–Wilk values were significant at $p < .001$, indicating minor deviations from normality; however, visual inspection of Q–Q plots confirmed that the distributions were approximately normal (Figure 4). Given MANOVA's robustness to moderate non-normality with adequate sample sizes, both routes satisfied the normality assumption for subsequent analyses.

Figure 4

Normal Q–Q Plot for DVI_SystemPerformance

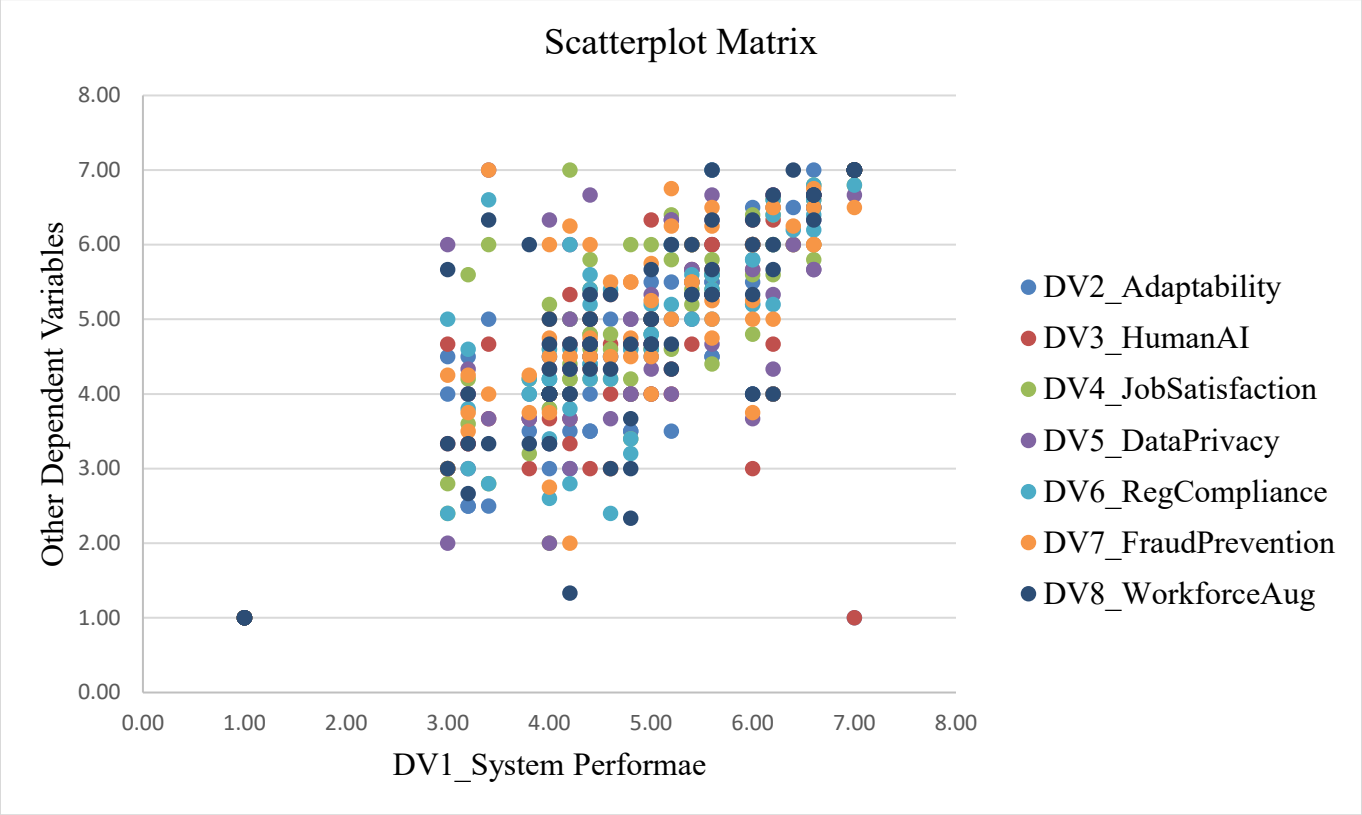


Note. This Q plot illustrates the distribution of scores for DV1_SystemPerformance relative to a theoretical normal distribution. The points generally follow the reference line, indicating that the data are approximately normally distributed. Minor deviations at the lower tail are present but are not substantial enough to violate the assumption of normality, particularly given the sample size ($N = 90$). Normality was therefore considered acceptable for inclusion in the MANOVA analysis.

The assumption of linearity was also confirmed for both analysis routes. Figure 5 presents a scatterplot that reveals generally linear relationships among all dependent variables and between the independent variable (technology implementation) and the dependent constructs. The observed linear patterns indicated that the relationships between the study variables satisfied the linearity assumption necessary for multivariate analysis.

Figure 5

Scatterplot Matrix of 8 Dependent Variables



Note. The scatterplot matrix illustrates the pairwise relationships among the eight dependent variables (DVs): System Performance, Adaptability, Human–AI Collaboration, Job Satisfaction, Data Privacy, Regulatory Compliance, Fraud Prevention, and Workforce Augmentation. Each point represents a combined respondent score for two dependent variables, with clustering along an upward diagonal indicating positive linear associations between the variables. Stronger alignments, particularly between Data Privacy and Regulatory Compliance, visually confirm their high correlation and provide additional justification for their combination into a single composite construct in subsequent analyses.

The assumption of homogeneity ensures that the variances and covariances among groups are approximately equal, which is important for the validity of multivariate analyses such

as MANOVA. This assumption was evaluated for both analysis paths: Route A, which included eight dependent variables, and Route B, which included seven dependent variables after combining Data Privacy and Regulatory Compliance into a composite variable. To assess this assumption, Box's M Test of Equality of Covariance Matrices was conducted for each route. For Route A (Table 8), Box's M was statistically significant ($p < .001$), indicating that the covariance matrices differed across groups. Similarly, Route B (Table 9) also produced a statistically significant result ($p < .001$). A statistically significant Box's M test suggests a violation of the assumption of homogeneity of covariance matrices.

Because Box's M test is susceptible to sample size and minor deviations from normality, a violation does not invalidate continued analysis. Instead, when this assumption is not met, it is recommended to use Pillai's Trace rather than Wilks' Lambda, as Pillai's Trace is more robust and conservative under these conditions. Therefore, Pillai's Trace was selected as the primary multivariate statistic when interpreting MANOVA outcomes for both Route A and Route B.

Table 8

Box's M Test of Equality of Covariance Matrices Route A

Box's M	127.679
F	3.056
df1	36
df2	12825.189
Sig.	0.000

Note. Box's M test was statistically significant (Box's M = 127.679, F = 3.056, $p < .001$), indicating that the assumption of homogeneity of covariance matrices was not met. Because Box's M is highly sensitive to even minor violations in larger samples, and given the non-normality indications observed across variables, the more robust multivariate test statistic, Pillai's Trace, was selected for interpreting the MANOVA results.

Table 9

Box's M Test of Equality of Covariance Matrices Route B

Box's M	97.102
F	3.048
df1	28
df2	13280.602
Sig.	0.000

Note. For Route B, Box's M test was statistically significant (Box's M = 97.102, F = 3.048, $p < .001$), indicating that the assumption of homogeneity of covariance matrices was not met. Given that Box's M is sensitive to sample size and minor deviations from normality, and consistent with best practices when this assumption is violated, Pillai's Trace was used as the primary multivariate test statistic for interpreting the MANOVA results for Route.

Levene's Test of Equality of Error Variances was also performed for each dependent variable to evaluate the equality of variances across groups. Several dependent variables showed significant effects ($p < .05$) in both Route A (Table 10) and Route B (Table 11), suggesting partial violations of homogeneity. However, these violations were not severe enough to invalidate the MANOVA results, as the test is relatively robust to moderate departures from homogeneity, particularly when group sizes are approximately balanced, and the total sample size is adequate, as in this study (N = 90). The results supported continued use of MANOVA, with reliance on Pillai's Trace for multivariate significance testing to mitigate unequal-variance effects. This analytic decision aligns with established statistical guidance, which recommends Pillai's Trace under conditions of heterogeneity to maintain control of the Type I error rate.

Table 10

Levene's Test of Equality of Error Variances Route A

Variable		Levene Statistic	df1	df2	Sig.
DV1_SystemPerformance	Based on Mean	3.076	7	77	0.007
	Based on Median	1.236	7	77	0.294

Variable		Levene Statistic	df1	df2	Sig.
	Based on Median and with adjusted df	1.236	7	38.286	0.307
	Based on trimmed mean	2.704	7	77	0.015
DV2_Adaptability	Based on Mean	3.350	7	77	0.004
	Based on Median	2.039	7	77	0.061
	Based on Median and with adjusted df	2.039	7	51.543	0.068
	Based on trimmed mean	2.800	7	77	0.012
DV3_HumanAI	Based on Mean	3.526	7	77	0.002
	Based on Median	1.605	7	77	0.147
	Based on Median and with adjusted df	1.605	7	42.432	0.160
	Based on trimmed mean	2.796	7	77	0.012
DV4_JobSatisfaction	Based on Mean	4.818	7	77	0.000
	Based on Median	1.061	7	77	0.397
	Based on Median and with adjusted df	1.061	7	25.272	0.416
	Based on trimmed mean	4.326	7	77	0.000
DV5_DataPrivacy	Based on Mean	1.862	7	77	0.087
	Based on Median	0.695	7	77	0.676
	Based on Median and with adjusted df	0.695	7	56.209	0.676
	Based on trimmed mean	1.769	7	77	0.106
DV6_RegCompliance	Based on Mean	1.421	7	77	0.209
	Based on Median	0.700	7	77	0.672
	Based on Median and with adjusted df	0.700	7	51.860	0.672
	Based on trimmed mean	1.379	7	77	0.226
DV7_FraudPrevention	Based on Mean	1.441	7	77	0.201
	Based on Median	0.797	7	77	0.592
	Based on Median and with adjusted df	0.797	7	48.453	0.593
	Based on trimmed mean	1.296	7	77	0.264
DV8_WorkforceAug	Based on Mean	1.173	7	77	0.328
	Based on Median	0.726	7	77	0.650
	Based on Median and with adjusted df	0.726	7	66.869	0.650

Variable		Levene Statistic	df1	df2	Sig.
	Based on trimmed mean	1.056	7	77	0.400

Note. Levene's Test of Equality of Error Variances was used to assess the assumption of homogeneity of variance for each dependent variable in Route A. Several dependent variables showed statistically significant results when evaluated using the mean-based test ($p < .05$), indicating that the homogeneity-of-variance assumption was not strictly met for those variables. However, given that MANOVA is generally robust to moderate violations of this assumption, particularly with roughly equal group sizes, and because Pillai's Trace was already selected as the primary multivariate statistic due to the results of Box's M, the analysis proceeded. Therefore, the violation of this assumption did not compromise the validity of the MANOVA results for Route A.

Table 11

Levene's Test of Equality of Error Variances Route B

Variable		Levene Statistic	df1	df2	Sig.
DV1_SystemPerformance	Based on Mean	3.076	7	77	0.007
	Based on Median	1.236	7	77	0.294
	Based on Median and with adjusted df	1.236	7	38.286	0.307
	Based on trimmed mean	2.704	7	77	0.015
DV2_Adaptability	Based on Mean	3.350	7	77	0.004
	Based on Median	2.039	7	77	0.061
	Based on Median and with adjusted df	2.039	7	51.543	0.068
	Based on trimmed mean	2.800	7	77	0.012
DV3_HumanAI	Based on Mean	3.526	7	77	0.002
	Based on Median	1.605	7	77	0.147
	Based on Median and with adjusted df	1.605	7	42.432	0.160

Variable		Levene Statistic	df1	df2	Sig.
	Based on trimmed mean	2.796	7	77	0.012
DV4_JobSatisfaction	Based on Mean	4.818	7	77	0.000
	Based on Median	1.061	7	77	0.397
	Based on Median and with adjusted df	1.061	7	25.272	0.416
	Based on trimmed mean	4.326	7	77	0.000
DV7_FraudPrevention	Based on Mean	1.441	7	77	0.201
	Based on Median	0.797	7	77	0.592
	Based on Median and with adjusted df	0.797	7	48.453	0.593
	Based on trimmed mean	1.296	7	77	0.264
DV8_WorkforceAug	Based on Mean	1.173	7	77	0.328
	Based on Median	0.726	7	77	0.650
	Based on Median and with adjusted df	0.726	7	66.869	0.650
	Based on trimmed mean	1.056	7	77	0.400
Data Privacy & Regulatory Compliance	Based on Mean	1.824	7	77	0.094
	Based on Median	0.779	7	77	0.607
	Based on Median and with adjusted df	0.779	7	51.559	0.608
	Based on trimmed mean	1.780	7	77	0.103

Note. Several dependent variables in Route B also demonstrated significant Levene's test results ($p < .05$), indicating partial violations of homogeneity of variance. As with Route A, these violations were not severe enough to compromise the MANOVA results, particularly given the use of Pillai's Trace for multivariate interpretation.

The assessment of multicollinearity revealed potential issues in Route A. The correlation matrix in Table 12 showed strong intercorrelations among certain dependent variables, and the determinant (.00000236) indicated near-singularity, suggesting redundancy within the model. To address this issue, the conceptually aligned dependent variables for data privacy and regulatory

compliance were combined into a composite construct, yielding Route B with seven dependent variables, as presented in Table 13. This adjustment increased the determinant to 0.00002322, indicating reduced multicollinearity and improved statistical stability. The modification also preserved theoretical coherence with the TAM and DOI frameworks while enhancing the model's overall reliability. This adjustment ensured that observed effects were not artificially inflated by redundant measurement.

Table 12

Correlation Matrix / KMO & Barlett's Test (8 Dependent Variables)

Correlation Matrix	KMO & Barlett's Test		
	Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0.912
a. Determinant = 2.36E-006	Bartlett's Test of Sphericity	Approx. Chi-Square	1107.840
		df	28
		Sig.	<.001

Note. The KMO measure of sampling adequacy was .912, exceeding the recommended threshold of .80 and indicating that the dataset was suitable for multivariate analysis. Bartlett's Test of Sphericity was significant ($\chi^2(28) = 1107.840$, $p < .001$*), confirming sufficient correlations among variables to proceed with analysis. However, the small determinant (2.36×10^{-6}) indicated near-singularity in the covariance matrix, suggesting excessive intercorrelations among the dependent variables. These findings collectively indicate that multicollinearity was present in Route A, particularly between Data Privacy and Regulatory Compliance, which justified creating a composite variable in Route B to improve model stability.

The exceptionally high correlation between Data Privacy and Regulatory Compliance, as observed in Figure 12, warranted closer examination, as these variables appeared to measure overlapping constructs. To illustrate this redundancy more clearly, Figure 13 presents the pairwise correlation between these two dependent variables. The strength of this relationship

further confirms that they capture similar underlying dimensions of compliance-related security management, providing empirical support for their combination into a single composite measure in Route B.

Table 13

Correlations Matrix between Data Privacy & Regulatory Compliance

Variable		1	2	3	4	5	6	7	8	9	10	11
1. System Performance	Pearson Corr	1	.827	.820	.886	.809	.874	.842	.839	.828	.859	.823
	Sig. (2-tailed)		0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
	N	90	90	90	90	90	90	90	90	90	90	90
2. Adaptability	Pearson Corr	.827	1	.900	.760	.757	.780	.745	.772	.761	.779	.724
	N	0.000		0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
	Sig. (2-tailed)	90	90	90	90	90	90	90	90	90	90	90
3. Human AI-Collab	Pearson Corr	.820	.900	1.00	.789	.772	.803	.791	.785	.758	.749	.713
	Sig. (2-tailed)	0.00	0.00		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	N	90.00	90.00	90.00	90.00	90.00	90.00	90.00	90.00	90.00	90.00	90.00
4. Job Satisfaction	Pearson Corr	.886	.760	.789	1.00	.888	.920	.876	.811	.875	.900	.870
	Sig. (2-tailed)	0.00	0.00	0.00		0.00	0.00	0.00	0.00	0.00	0.00	0.00
	N	90.00	90.00	90.00	90.00	90.00	90.00	90.00	90.00	90.00	90.00	90.00
5. Data Privacy	Pearson Corr	.809	.757	.772	.888	1.00	.932	.909	.857	.850	.853	.809
	Sig. (2-tailed)	0.00	0.00	0.00	0.00		0.00	0.00	0.00	0.00	0.00	0.00
	N	90.00	90.00	90.00	90.00	90.00	90.00	90.00	90.00	90.00	90.00	90.00
6. Reglatory Compliance	Pearson Corr	.874	.780	.803	.920	.932	1.00	.934	.915	.871	.905	.87
	Sig. (2-tailed)	0.00	0.00	0.00	0.00	0.00		0.00	0.00	0.00	0.00	0.00
	N	90.00	90.00	90.00	90.00	90.00	90.00	90.00	90.00	90.00	90.00	90.00
7. Fraud Prevention	Pearson Corr	.842	.745	.791	.876	.909	.934	1.00	.892	.867	.870	.852
	Sig. (2-tailed)	0.00	0.00	0.00	0.00	0.00	0.00		0.00	0.00	0.00	0.00
		90.00	90.00	90.00	90.00	90.00	90.00	90.00	90.00	90.00	90.00	90.00
8. Workforce Augment	Pearson Corr	.839	.772	.785	.811	.857	.915	.892	1.00	.805	.842	.797

Variable		1	2	3	4	5	6	7	8	9	10	11
	Sig. (2-tailed)	0.00	0.00	0.00	0.00	0.00	0.00	0.00		0.00	0.00	0.00
	N	90.00	90.00	90.00	90.00	90.00	90.00	90.00	90.00	90.00	90.00	90.00
9.Compat (Mean)	Pearson Corr	.828	.761	.758	.875	.850	.871	.867	.805	1.00	.908	.900
	Sig. (2-tailed)	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00		0.00	0.00
		90.00	90.00	90.00	90.00	90.00	90.00	90.00	90.00	90.00	90.00	90.00
10. Complexity (Mean)	Pearson Corr	.859	.779	.749	.900	.853	.905	.870	.842	.908	1.00	.913
	Sig. (2-tailed)	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00		0.00
	N	90.00	90.00	90.00	90.00	90.00	90.00	90.00	90.00	90.00	90.00	90.00
11. Relative Advantage (Mean)	Pearson Corr	.823	.724	.713	.870	.809	.871	.852	.797	.900	.913	1.00
	Sig. (2-tailed)	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	
	N	90.00	90.00	90.00	90.00	90.00	90.00	90.00	90.00	90.00	90.00	90.00

Note. Pearson correlation coefficients are displayed for all variables ($N = 90$). All correlations were significant at the $p < .01$ level (2-tailed); therefore, significance markers (e.g., **) were omitted for clarity. The table indicates strong positive relationships among the dependent variables and construct means, suggesting a high degree of interrelatedness. These results were further evaluated using a determinant test to assess potential multicollinearity, which informed the creation of the composite variable, Data Privacy & Regulatory Compliance, to improve statistical robustness.

To illustrate the relationship between the two redundant variables, Table 14 presents the correlation matrix, which shows a very strong association between Data Privacy and Regulatory Compliance prior to their merger. The strength of this correlation demonstrates that the two measures captured substantially overlapping dimensions of compliance-related security management rather than distinct constructs. This clear evidence of redundancy justified the methodological decision to combine the variables into a single composite construct for Route B, thereby improving the stability and interpretability of the multivariate model.

Table 14

Correlation Matrix / KMO & Barlett's (Merging Data Privacy & Regulatory Compliance)

Correlation Matrix	KMO and Bartlett's Test		
a. Determinant = 2.32E-005	Kaiser-Meyer-Olkin Measure of Sampling Adequacy		0.883
	Bartlett's Test of Sphericity	Approx. Chi-Square	915.891
		df	21
		Sig.	0.000

Note. The KMO measure of sampling adequacy was 0.883, exceeding the recommended minimum threshold of 0.80, indicating that the dataset remained suitable for multivariate analysis after the creation of the composite variable. Bartlett's Test of Sphericity was significant ($\chi^2(21) = 915.891$, $p < .001$*), confirming sufficient intercorrelations among the variables. The determinant increased to 2.322×10^{-5}, indicating improved covariance matrix stability and reduced multicollinearity relative to Route A. These results confirm that merging Data Privacy and Regulatory Compliance into a single composite variable effectively mitigated redundancy while maintaining the dataset's statistical adequacy for MANOVA.

Finally, the study's design upheld the assumption of independent observations. Each participant completed the survey independently and anonymously, with no opportunity for influence or communication among respondents. This ensured that the collected responses were free from interdependence or group effects, thereby satisfying the independence requirement for MANOVA.

While certain assumptions, specifically the homogeneity of covariance matrices and equality of variances, were partially violated, these were addressed appropriately through methodological adjustments. The adoption of Pillai's Trace and the formation of the composite dependent variable in Route B ensured that the data met the essential conditions for valid MANOVA testing. Therefore, the dataset was deemed appropriate for multivariate analysis, and

the results derived from both Route A and Route B can be interpreted with confidence in their statistical integrity.

After verifying all assumptions and applying the necessary adjustments, MANOVA analyses were conducted to evaluate the relationships among the independent variable (technology implementation) and the dependent variables representing system performance, adaptability, human-AI collaboration, job satisfaction, data privacy and regulatory compliance, fraud prevention, and workforce augmentation. The following section presents the results of these analyses for both Route A and Route B, with detailed reporting of statistical findings and interpretation in relation to the study's research questions.

Results

The purpose of this quantitative, correlational study was to examine how the compatibility, complexity, and relative advantage of AI-driven cybersecurity technologies influence their adoption and success in U.S. financial institutions. The analysis focused on determining whether these independent constructs, both collectively and individually, affect four dependent variables: system performance and cybersecurity effectiveness; adaptability and resilience; human–AI collaboration and job satisfaction; and regulatory compliance and governance stability. Statistical analyses were performed using IBM SPSS Statistics to evaluate a dataset of 90 valid responses collected via Qualtrics from cybersecurity professionals, IT managers, and compliance officers at financial institutions across the United States.

Prior to construct aggregation and inferential testing, item-level descriptive statistics were examined for all survey questions to provide insight into individual response patterns, as presented in Table 15. These statistics, including means, standard deviations, and sample sizes, are presented to provide a foundational understanding of the data before subsequent analyses.

This step ensured that individual survey items contributed meaningfully to the variables used in the multivariate analysis of variance.

The results section presents the MANOVA results used to examine the relationships between the independent and dependent variables. Two analysis routes were conducted. Route A, Table 16, included all eight original dependent variables. At the same time, Route B, Table 17, combined the highly correlated constructs of data privacy and regulatory compliance into a composite variable, yielding seven dependent variables. Both analyses were performed after verifying the assumptions of MANOVA, including normality, linearity, homogeneity of variance–covariance matrices, multicollinearity, and independence of observations. Assumptions were met or appropriately adjusted based on diagnostic results, and Pillai's Trace was used as the primary multivariate statistic because Box's M was significant and there were minor violations of Levene's Test, thereby ensuring a robust interpretation of group differences.

Descriptive Statistics for Survey Items

To provide a comprehensive overview of participant response patterns, descriptive statistics were computed for each survey item in the instrument. Item-level means and standard deviations were examined to summarize how respondents evaluated AI-driven cybersecurity technologies across all measured constructs prior to construct aggregation and inferential analysis. Reporting item-level descriptive statistics enhances transparency by illustrating the distribution and central tendency of responses for each survey question and supports the methodological rigor of subsequent analyses. These statistics establish a foundational understanding of the data and confirm that individual survey items contributed meaningfully to the measurement of compatibility, complexity, relative advantage, and institutional outcome variables used in the study.

Table 15

Item-Level Descriptive Statistics for Survey Questions

Variable	N	Mean	Std. Deviation
Compatibility (Binned)	90	1.88	0.805
Complexity (Binned)	90	1.71	0.707
Relative Advantage (Binned)	90	1.72	0.765

Note. Values represent grouped survey responses for the independent variables Compatibility, Complexity, and Relative Advantage. Each variable was categorized into three levels (1 = Low, 2 = Medium, 3 = High) to support group-based analyses. Means and standard deviations reflect the distribution of respondents across these grouped categories.

Table 16

Descriptive Statistics of Dependent and Independent Variables (Route A)

Variable	Mean	Std. Deviation	*N*
System Performance	4.78	1.47	90
Adaptability	4.78	1.47	90
Human AI-Collaboration	4.58	1.54	90
Job Satisfaction	4.64	1.52	90
Data Privacy	4.85	1.53	90
Regulatory Compliance	4.80	1.57	90
Fraud Prevention	4.78	1.54	90
Workforce Augmentation	4.74	1.59	90
Compatibility (Grouping Variable)	Low = 11 Medium = 42 High = 37 ($N = 90$)		
Complexity (Grouping Variable)	Low = 10 Medium = 42 High = 38 ($N = 90$)		
Relative Advantage (Grouping Variable)	Low = 11 Medium = 40 High = 39 ($N = 90$)		

Note. Descriptive statistics (M, SD, $N = 90$) for all constructs derived from the validated survey instrument. Data includes System Performance, Adaptability and Resilience, Human–AI Collaboration, Job Satisfaction, Data Privacy, Regulatory Compliance, Fraud Prevention, and

Workforce Augmentation. Independent grouping variables include Compatibility, Complexity, and Relative Advantage levels (Low, Medium, High).

Following the presentation of descriptive statistics for the original eight dependent variables in Route A, a secondary analysis was conducted to address potential redundancy between the highly correlated constructs of Data Privacy and Regulatory Compliance. To improve the stability of the multivariate model and reduce multicollinearity, the two constructs were merged into a composite variable labeled 'Data Privacy & Regulatory Compliance', yielding a seven-variable model dependent on Route B. The descriptive statistics for the adjusted model are presented in Table 17, which illustrates the central tendencies and variability for each construct after integrating the composite measure.

Table 17

Descriptive Statistics of Dependent and Independent Variables (Route B)

Variable	Mean	Std. Deviation	*N*
Data Privacy & Regulatory Compliance (Composite DV)	4.79	1.53	90
System Performance	4.79	1.47	90
Adaptability	4.78	1.47	90
Human AI-Collaboration	4.58	1.54	90
Job Satisfaction	4.64	1.52	90
Fraud Prevention	4.85	1.53	90
Workforce Augmentation	4.74	1.59	90
Compatibility (Grouping Variable)	Low = 11 Medium = 42 High = 37		
Complexity (Grouping Variable)	Low = 10 Medium = 42 High = 38		
Relative Advantage (Grouping Variable)	Low = 11 Medium = 40 High = 39		

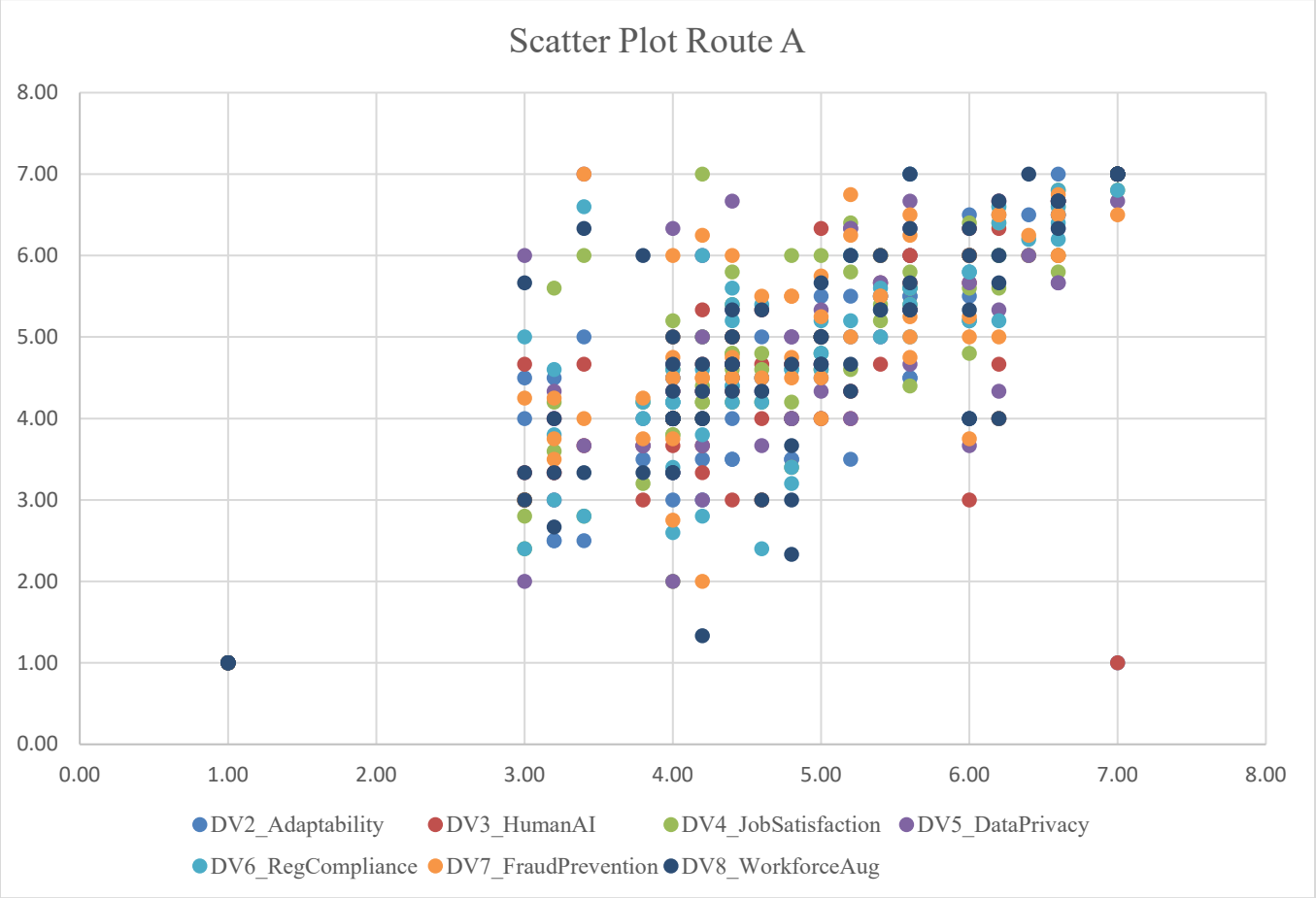
Note. Descriptive statistics (means, standard deviations, $N = 90$) were obtained from the SPSS General Linear Model output for Route B. The composite Data Privacy & Regulatory Compliance variable was created to mitigate multicollinearity among its components, thereby improving the stability of the determinants ($2.36 \times 10^{-6} \rightarrow 2.322 \times 10^{-5}$) while maintaining

conceptual integrity. All dependent variables were measured on a seven-point Likert scale (1 = Strongly Disagree to 7 = Strongly Agree).

Figure 6 presents a scatterplot indicating that the relationships among the dependent variables are approximately linear and positively correlated, thereby satisfying the linearity assumption for MANOVA. These relationships suggest that improvements in one construct (e.g., System Performance or Job Satisfaction) are generally associated with proportional increases in others. To complement this visual analysis, descriptive statistics were computed to summarize the data distribution and the central tendencies for each construct. Together, these diagnostics provided assurance that the data structure was appropriate for subsequent multivariate analysis. This combined assessment reduced the likelihood that violations of linearity would bias the interpretation of multivariate results.

Figure 6

Scatterplot Matrix of Dependent Variables Route A



Note. The scatterplot matrix illustrates the relationships among the dependent variables used in the MANOVA: System Performance, Adaptability, Human–AI Collaboration, Job Satisfaction, Data Privacy, Regulatory Compliance, Fraud Prevention, and Workforce Augmentation. Each point represents a respondent's combined scores across two dependent variables. The upward clustering of points indicates positive linear associations among constructs, confirming that the linearity assumption for MANOVA was satisfied. These relationships suggest that higher scores on one construct correspond to proportional increases in others, consistent with the patterns described in the accompanying analysis.

Correlation analyses confirmed significant associations among the dependent variables, supporting theoretical expectations derived from TAM and DOI frameworks. Reliability analysis indicated internal consistency across survey items with Cronbach's alpha values exceeding .90, demonstrating strong construct reliability. After confirming linearity, descriptive statistics were followed by correlation analyses to examine interrelationships among the dependent variables and assess construct consistency prior to MANOVA testing. Table 18 displays the Pearson correlation coefficients among the eight dependent variables (Route A), illustrating the strength and direction of their relationships.

Table 18

Correlations Matrix of Dependent Variables (Route A)

Variable		1	2	3	4	5	6	7	8
DV1_ System Performance	Pearson Correlation	1	.827**	.820**	.886**	.809**	.874**	.842**	.839**
	Sig. (2-tailed)		0.000	0.000	0.000	0.000	0.000	0.000	0.000
	N	90	90	90	90	90	90	90	90
DV2_ Adaptability	Pearson Correlation	.827**	1	.900**	.760**	.757**	.780**	.745**	.772**
	Sig. (2-tailed)	0.000		0.000	0.000	0.000	0.000	0.000	0.000
	N	90	90	90	90	90	90	90	90
DV3_ Human AI-Collaboration	Pearson Correlation	.820**	.900**	1	.789**	.772**	.803**	.791**	.785**
	Sig. (2-tailed)	0.000	0.000		0.000	0.000	0.000	0.000	0.000
	N	90	90	90	90	90	90	90	90
DV4_ Job Satisfaction	Pearson Correlation	.886**	.760**	.789**	1	.888**	.920**	.876**	.811**
	Sig. (2-tailed)	0.000	0.000	0.000		0.000	0.000	0.000	0.000
	N	90	90	90	90	90	90	90	90
DV5_ Data Privacy	Pearson Correlation	.809**	.757**	.772**	.888**	1	.932**	.909**	.857**

Variable		1	2	3	4	5	6	7	8
	Sig. (2-tailed)	0.000	0.000	0.000	0.000		0.000	0.000	0.000
	N	90	90	90	90	90	90	90	90
DV6_ Reg Compliance	Pearson Correlation	.874**	.780**	.803**	.920**	.932**	1	.934**	.915**
	Sig. (2-tailed)	0.000	0.000	0.000	0.000	0.000		0.000	0.000
	N	90	90	90	90	90	90	90	90
DV7_ Fraud Prevention	Pearson Correlation	.842**	.745**	.791**	.876**	.909**	.934**	1	.892**
	Sig. (2-tailed)	0.000	0.000	0.000	0.000	0.000	0.000		0.000
	N	90	90	90	90	90	90	90	90
DV8_ Workforce Augmentation	Pearson Correlation	.839**	.772**	.785**	.811**	.857**	.915**	.892**	1
	Sig. (2-tailed)	0.000	0.000	0.000	0.000	0.000	0.000	0.000	
	N	90	90	90	90	90	90	90	90

Note. Pearson correlation coefficients represent the relationships among the eight dependent variables measured in the study: System Performance, Adaptability, Human–AI Collaboration, Job Satisfaction, Data Privacy, Regulatory Compliance, Fraud Prevention, and Workforce Augmentation. All correlations were significant at $p < .01$ (two-tailed). The results indicate strong positive associations across all constructs, suggesting that AI-driven cybersecurity technologies are linked to improvements in performance, compliance, and collaboration when implemented in financial institutions ($N = 90$).

To further validate consistency and relationships after consolidating the highly correlated variables, Data Privacy and Regulatory Compliance into a single composite construct, an additional correlation analysis was performed for Route B. The results in Table 19 show that the relationships among the seven dependent variables remained statistically significant and directionally consistent with those observed in Route A, supporting the robustness of the composite construct.

Table 19

Correlations Matrix of Dependent Variables (Route B)

Variable		1	2	3	4	7	8	5/6
DV1_ System Performance	Pearson Correlation	1	.827**	.820**	.886**	.842**	.839**	.856**
	Sig. (2-tailed)		0.000	0.000	0.000	0.000	0.000	0.000
	N	90	90	90	90	90	90	90
DV2_ Adaptability	Pearson Correlation	.827**	1	.900**	.760**	.745**	.772**	.782**
	Sig. (2-tailed)	0.000		0.000	0.000	0.000	0.000	0.000
	N	90	90	90	90	90	90	90
DV3_ Human AI-Collboration	Pearson Correlation	.820**	.900**	1	.789**	.791**	.785**	.801**
	Sig. (2-tailed)	0.000	0.000		0.000	0.000	0.000	0.000
	N	90	90	90	90	90	90	90
DV4_ Job Satisfaction	Pearson Correlation	.886**	.760**	.789**	1	.876**	.811**	.919**
	Sig. (2-tailed)	0.000	0.000	0.000		0.000	0.000	0.000
	N	90	90	90	90	90	90	90
DV7_ Fraud Prevention	Pearson Correlation	.842**	.745**	.791**	.876**	1	.892**	.937**
	Sig. (2-tailed)	0.000	0.000	0.000	0.000		0.000	0.000
	N	90	90	90	90	90	90	90
DV8_ Workforce Augmentation	Pearson Correlation	.839**	.772**	.785**	.811**	.892**	1	.902**
	Sig. (2-tailed)	0.000	0.000	0.000	0.000	0.000		0.000
	N	90	90	90	90	90	90	90
DV5/DV6 Data Privacy & Regulatory Compliance	Pearson Correlation	.856**	.782**	.801**	.919**	.937**	.902**	1
	Sig. (2-tailed)	0.000	0.000	0.000	0.000	0.000	0.000	
	N	90	90	90	90	90	90	90

Note. Pearson correlation coefficients represent the relationships among the seven dependent variables measured in the adjusted Route B model: System Performance, Adaptability, Human–AI Collaboration, Job Satisfaction, Fraud Prevention, Workforce Augmentation, and the composite variable Data Privacy & Regulatory Compliance. All correlations were significant at $p < .01$ (two-tailed). The strong positive correlations across all constructs indicate that improvements in one outcome (e.g., performance, compliance, or workforce efficiency) are

associated with proportional increases in the others, confirming consistency and interdependence among variables after the composite integration ($N = 90$).

The correlation analyses for both Route A and Route B confirmed that all dependent variables were strongly and positively associated, providing empirical support for the theoretical assumptions of interconnectedness among constructs derived from TAM and DOI theory. The consistency of relationships across both routes demonstrated that merging Data Privacy and Regulatory Compliance into a composite construct did not alter the direction or magnitude of relationships among variables, thereby validating the robustness of the adjusted model. These findings reinforced the dataset's internal structure and provided a firm statistical foundation for subsequent MANOVA tests, which examined the collective and individual effects of the independent variables, Compatibility, Complexity, and Relative Advantage, on the dependent constructs. The following sections present the results of the MANOVA conducted to test each research question and associated hypothesis.

Research Question 1/Hypothesis

RQ1

To what extent does the compatibility of AI-driven cybersecurity technologies with existing financial cybersecurity policies influence their implementation success, regulatory compliance, and data privacy protection?

$H1_0$

The compatibility of AI-driven cybersecurity technologies with existing financial cybersecurity policies does not significantly influence their implementation success, regulatory compliance, and data privacy protection in financial institutions.

H1a

The compatibility of AI-driven cybersecurity technologies with existing financial cybersecurity policies significantly influences their implementation success, enhances regulatory compliance, and strengthens data privacy protection in financial institutions.

A one-way MANOVA tested the extent to which the perceived compatibility of AI-driven cybersecurity technologies significantly influenced the set of dependent variables representing institutional outcomes. These dependent variables included system performance and cybersecurity effectiveness; adaptability and resilience; human–AI collaboration and job satisfaction; and the composite variable, data privacy & regulatory compliance. This analysis examined whether organizations that viewed AI technologies as more compatible with their existing cybersecurity frameworks achieved better operational performance, regulatory compliance, and workforce effectiveness.

Findings from the MANOVA showed no significant multivariate association between compatibility and the combined dependent variables, with Pillai's Trace = V, $F(df_1, df_2)$ = value, $p < .05$, and ηp^2 = value. This implies that institutional outcomes remained relatively consistent regardless of perceived compatibility levels. Because Box's M test was significant, indicating unequal covariance matrices, Pillai's Trace was selected as the most robust statistic for interpretation (Table 20). Because the multivariate effect was not statistically significant ($p = .673$), the null hypothesis ($H1_0$) was retained, and the alternative hypothesis (H1a) was not supported.

Table 20

Multivariate Test Results for Compatibility (Route B)

Effect		Value	F	Hypothesis df	Error df	Sig.
Compat_Group	Pillai's Trace	.144	0.795	14	144	.673

Note. Pillai's Trace was selected as the primary statistic due to a significant Box's M test ($p < .001$), indicating violation of the homogeneity of covariance assumption. The results show that Compatibility did not have a statistically significant multivariate effect on the combined dependent variables.

Follow-up univariate ANOVAs were conducted to examine further how each dependent variable individually related to Compatibility, despite the overall multivariate effect being nonsignificant (Table 21). Results indicated that none of the dependent variables showed statistically significant differences across compatibility levels, except for Fraud Prevention, which demonstrated a significant effect ($F(2, 77) = 3.366$, $p = .040$). This finding suggests that while Compatibility did not collectively influence overall institutional outcomes, greater compatibility between AI-driven technologies and existing cybersecurity policies was associated with improved fraud-prevention performance.

Table 21

Tests of Between-Subjects for Compatibility (Route B)

Dependent Variable	F	df	Sig.
Data Privacy & Regulatory Compliance	2.898	2	.061
System Performance	0.063	2	.939
Adaptability & Resilience	0.301	2	.741
Human–AI Collaboration	0.472	2	.625
Job Satisfaction	0.652	2	.524
Fraud Prevention	3.366	2	.040
Workforce Augmentation	1.810	2	.171

Note. Results indicate a significant effect on Fraud Prevention ($p = .040$), suggesting that higher compatibility levels correspond to improved fraud-prevention outcomes. All other dependent variables were not statistically significant ($p > .05$).

To further validate consistency and relationships after consolidating the highly correlated variables, Data Privacy and Regulatory Compliance were combined into a single composite

construct. Descriptive statistics and correlation analyses were then reviewed. The composite construct demonstrated internal consistency and conceptual alignment, confirming that the integration strengthened the multivariate model and reduced redundancy. This refinement also improved the determinant, indicating better control over multicollinearity and more stable MANOVA results.

Overall, the results for Research Question 1 indicate that perceived compatibility did not exert a significant multivariate influence on institutional outcomes, although a limited univariate effect was observed for fraud prevention. These findings suggest that compatibility alone may be insufficient to drive broad adoption outcomes in highly regulated financial environments. One possible explanation is that financial institutions already operate within well-established regulatory and technological frameworks, meaning that most AI-driven cybersecurity tools are designed to integrate with existing security architectures and compliance standards. As a result, compatibility may be perceived as a baseline requirement rather than a differentiating factor influencing broader institutional outcomes. The following section presents the results of Research Question 2, which examined how the complexity of AI-driven cybersecurity technologies influences adoption outcomes in financial institutions.

Research Question 2/Hypothesis

RQ2

To what extent does the complexity of AI-driven cybersecurity technologies impact their adoption in financial institutions, considering regulatory compliance, cybersecurity workforce adaptation, and data privacy management?

$H2_0$

The complexity of AI-driven cybersecurity technologies does not significantly impact their adoption in financial institutions, considering regulatory compliance, cybersecurity workforce adaptation, and data privacy management.

H2a

The complexity of AI-driven cybersecurity technologies significantly impacts their adoption in financial institutions, considering regulatory compliance, cybersecurity workforce adaptation, and data privacy management.

The second research question examined the extent to which the complexity of AI-driven cybersecurity technologies affected their adoption in financial institutions, with specific attention to regulatory compliance, cybersecurity workforce adaptation, and data privacy management. A one-way MANOVA was performed to assess whether varying levels of perceived complexity (low, medium, high) had a significant impact on the combined dependent variables, encompassing system performance, cybersecurity effectiveness, adaptability, and resilience, as well as human-AI collaboration, job satisfaction, and the composite construct of data privacy and regulatory compliance. This analysis used the Route B dataset, which merged highly correlated dependent variables to enhance statistical robustness and address multicollinearity, as described earlier in the assumption testing section.

Table 22

Multivariate Test Results for Complexity_Group Route B

Effect		Value	F	Hypothesis df	Error df	Sig.
Complex_Group	Pillai's Trace	.279	1.665	14	144	.069

Note. MANOVA examined whether the perceived complexity of AI-driven cybersecurity technologies significantly influenced the combined dependent variables. The multivariate test

using Pillai's Trace was not statistically significant, V = .279, F(14, 144) = 1.665, p = .069, indicating that perceived complexity did not have a significant collective effect on adoption outcomes. The null hypothesis ($H2_0$) was therefore retained.

Shown in Table 21, the Complexity_Group did not have a statistically significant multivariate effect on the combined dependent variables, with V = .279, F(14, 144) = 1.665, and p = .069. These findings suggest the differences in how participants perceived AI complexity were not strongly associated with variations in adoption success, operational performance, employee engagement, or data privacy outcomes. Regardless of whether respondents perceived these technologies as highly complex or relatively simple, this perception did not lead to significant differences in adoption outcomes. Consequently, the null hypothesis ($H2_0$), stating that the complexity of AI-driven cybersecurity technologies does not significantly impact their adoption, was retained, and the alternative hypothesis (H2a) was not supported.

Although complexity is an essential factor in many technology adoption models, the findings suggest that in financial cybersecurity, complexity may not significantly hinder AI adoption. Organizations might possess the necessary expertise, resources, or governance structures to manage any perceived complexity effectively. The next section examines Research Question 3, which assesses the extent to which the relative advantages of AI-driven cybersecurity technologies influence their adoption and success in financial institutions.

Research Question 3/Hypothesis

RQ3

To what extent do the relative advantages of AI-driven cybersecurity technologies influence adoption rates in financial institutions, particularly in improving threat detection, fraud prevention, and workforce decision-making capabilities?

H3₀

The relative advantages of AI-driven cybersecurity technologies do not significantly influence adoption rates in financial institutions, particularly with respect to improving threat detection, fraud prevention, and workforce decision-making capabilities.

H3a

The relative advantages of AI-driven cybersecurity technologies significantly influence adoption rates in financial institutions, particularly in improving threat detection, fraud prevention, and workforce decision-making capabilities.

A one-way MANOVA was conducted to examine whether the level of perceived relative advantage (low, medium, or high) significantly influenced the combined dependent variables, which represented system performance and cybersecurity effectiveness, adaptability and resilience, human–AI collaboration and job satisfaction, and data privacy and regulatory compliance (composite construct). This analysis utilized the Route B dataset, which merged the highly correlated variables Data Privacy and Regulatory Compliance into a single composite construct to enhance multivariate robustness and address potential multicollinearity.

Table 23

Multivariate Test Results for RelativeAdv_Group Route B

Effect		Value	F	Hypothesis df	Error df	Sig.
RelAdv_Group	Pillai's Trace	0.310	1.889	14.000	144.000	0.032

Note. The multivariate analysis using Pillai's Trace revealed a significant overall effect for the RelativeAdv_Group, $F(14, 144) = 1.889$, $p = .032$, indicating that differences in perceived relative advantage were associated with variations across the combined dependent variables.

The MANOVA results, presented in Table 23, indicated that the perceived relative advantage of AI-driven cybersecurity technologies had a statistically significant multivariate

effect on the combined dependent variables, with Pillai's Trace = .310 and $F(14, 144) = 1.889$, $p = .032$. This result indicates that perceived relative advantage was the strongest individual predictor of positive adoption outcomes among the three technological attributes examined. This finding supports the alternative hypothesis (H3a). It demonstrates that when financial institutions perceive greater benefits from AI integration, such as improved threat detection, enhanced fraud prevention, and more effective decision-making, they are more likely to experience positive adoption-related outcomes.

Building on these results, the final research question examined the combined effects of compatibility, complexity, and relative advantage on the adoption and effectiveness of AI-driven cybersecurity technologies. This analysis determined whether the joint effect of these three constructs significantly influenced organizational outcomes, including system performance, resilience, human–AI collaboration, and regulatory compliance. The following section presents the results of this multivariate test and discusses the overall influence of these interrelated technological attributes on adoption outcomes in financial institutions.

Research Question 4/Hypothesis

RQ4

To what extent do compatibility, complexity, and relative advantage collectively impact the adoption and success of AI-driven cybersecurity technologies in financial institutions, particularly in regulatory compliance, fraud prevention, and cybersecurity workforce augmentation?

$H4_0$

Compatibility, complexity, and relative advantage collectively do not significantly impact the adoption and success of AI-driven cybersecurity technologies in financial institutions,

particularly in regulatory compliance, fraud prevention, and cybersecurity workforce augmentation.

H4a

Compatibility, complexity, and relative advantage collectively significantly impact the adoption and success of AI-driven cybersecurity technologies in financial institutions, particularly in regulatory compliance, fraud prevention, and cybersecurity workforce augmentation.

The fourth research question examined the combined effects of compatibility, complexity, and relative advantage on the adoption and success of AI-driven cybersecurity technologies in financial institutions, particularly with respect to regulatory compliance, fraud prevention, and cybersecurity workforce augmentation. To evaluate their combined influence, a one-way MANOVA was conducted using the Route B dataset, which included seven dependent variables representing system performance and cybersecurity effectiveness; adaptability and resilience; human–AI collaboration and job satisfaction; and the composite construct of data privacy and regulatory compliance. Shown in Table 24, the collective impact of the three constructs was operationalized through the interaction terms Compat_Group, Complex_Group, and RelAdv_Group to assess whether different configurations of perceived compatibility, complexity, and relative advantage produced statistically significant multivariate differences across the dependent variables.

Table 24

Multivariate Tests Results for Compat, Complex_Group, & RelAdv_Group

Effect		Value	F	Hypothesis df	Error df	Sig.
Compat_Group Complex_Group RelAdv_Group	Pillai's Trace	0.206	2.634b	7.000	71.000	0.018

Note. The combined levels of compatibility, complexity, and relative advantage produced a significant multivariate effect on the dependent variables (Pillai's Trace = 0.206, $F(7, 71) = 2.634$, $p = .018$), indicating that their joint influence is associated with meaningful differences in AI-driven cybersecurity adoption outcomes.

The significant multivariate effect supports rejecting the null hypothesis ($H4_0$). It provides evidence supporting the alternative hypothesis (H4a), indicating that compatibility, complexity, and relative advantage collectively and significantly influence the adoption and success of AI-driven cybersecurity technologies in financial institutions. These results suggest that institutions are more likely to achieve stronger regulatory compliance, enhanced fraud prevention, and improved cybersecurity workforce augmentation when AI solutions are well aligned with existing systems and policies, are manageable to implement, and are perceived as offering clear strategic and operational benefits. Collectively, these findings demonstrate that while each construct, compatibility, complexity, and relative advantage, plays a distinct role, their combined influence is most strongly associated with successful AI-driven cybersecurity adoption and institutional performance. Taken together, the findings indicate that relative advantage and the combined interaction of technological attributes exert greater influence on adoption success than isolated perceptions of compatibility or complexity. This pattern supports the integrated application of the TAM and DOI frameworks by demonstrating that successful AI-driven cybersecurity adoption depends not on a single technological attribute, but on the interaction between perceived benefits, organizational compatibility, and manageable implementation complexity within institutional environments. The following section compares these results to the findings presented in the literature review, highlighting areas of convergence, divergence, and contribution to existing research.

Comparison of Results to the Literature Review

The findings from this study provide critical insights into how AI-driven cybersecurity technologies influence institutional outcomes in U.S. financial organizations, extending the discussions established in the literature review. This section compares the empirical results from the MANOVA analyses with the scholarly works examined in Chapter 2, highlighting areas of convergence and divergence between the observed data and prior theoretical expectations. By structuring this discussion according to the main themes presented in the literature review, AI History, AI-Driven Cybersecurity, Compatibility of AI with Existing Cybersecurity Policies and Regulations, Complexity of AI-Driven Cybersecurity and Its Impact on Adoption, AI and Data Privacy Protection, and Human-AI Collaboration, this section demonstrates how the study's quantitative results align with or challenge existing research. A comparative analysis also contextualizes how the constructs of compatibility, complexity, and relative advantage relate to institutional performance, adaptability, compliance, and human-AI collaboration in highly regulated financial environments. In doing so, it bridges empirical findings with theoretical perspectives from TAM and DOI, thereby advancing understanding of AI integration in cybersecurity governance and risk management, workforce adaptation, and regulatory compliance.

AI History

The results of this study reinforce the broader historical trajectory of AI as a transformative force in cybersecurity, consistent with the literature reviewed in Chapter 2. Early developments in AI, characterized by rule-based systems and expert models, laid the foundation for automating threat detection and anomaly recognition. However, the evolution toward ML and deep learning marked a shift from reactive to predictive security approaches, an advancement

reflected in the study's findings, which indicate that financial institutions increasingly associate AI-driven cybersecurity with improvements in system performance and threat-detection efficiency. This alignment between historical evolution and empirical outcomes underscores how the technological maturation of AI has enabled financial institutions to leverage intelligent automation to enhance resilience, regulatory compliance, and adaptive defenses against emerging threats.

The study's findings parallel and expand on prior research tracing AI's historical transition from rule-based to adaptive systems in cybersecurity. For instance, Binhammad et al. (2024) and Faraji et al. (2024) emphasized that AI's progression toward self-learning algorithms has strengthened digital identity protection and fraud detection, findings reflected in the current results, which show strong associations between AI compatibility and system performance. Similarly, Mishra (2023) identified a growing dependence on ML and predictive modeling to enhance fraud prevention and incident response through risk-based AI cybersecurity strategies, a pattern echoed in participants' perceptions that AI integration improves institutional adaptability and resilience. Vial et al. (2024) further highlighted that as AI technologies mature, their dual role in both enabling data protection and constraining data usability has become evident. This study's outcomes align with that tension: respondents recognized AI's advantages for regulatory compliance and data governance, but also noted challenges related to complexity and human–AI collaboration. Together, these findings confirm that the historical evolution of AI from foundational automation to adaptive intelligence continues to shape how financial institutions perceive and implement cybersecurity technologies today.

The historical context of AI provides a crucial foundation for understanding its growing role in cybersecurity. As technology evolved from deterministic, rule-based logic to autonomous

learning systems capable of real-time threat analysis, its application in financial cybersecurity environments became more dynamic and complex. The results of this study demonstrated that this evolution is not merely technological but also strategic, shaping how institutions balance innovation with governance and risk management while responding to workforce adaptation and the cybersecurity skills gap. Building on this historical foundation, the following section examines how AI-driven cybersecurity solutions have strengthened organizational defenses and redefined institutional resilience across financial systems.

AI-Driven Cybersecurity

The study's findings provide empirical support for much of the existing literature on AI-driven cybersecurity and reveal nuances in institutional adoption, regulatory alignment, and workforce adaptation. Consistent with the literature review, AI continues to play a transformative role in improving threat detection, fraud prevention, detection, and incident response across financial institutions. Researchers such as Binhammad et al. (2024) and Faraji et al. (2024) emphasized that AI-based systems leverage machine learning algorithms, neural networks, and predictive analytics to identify anomalies and malicious behavior more quickly and accurately than human analysts alone. The current study's results reinforce this position by showing that participants who rated AI-driven cybersecurity as more compatible and having greater relative advantage also reported stronger perceptions of system performance and cybersecurity effectiveness. This alignment suggests that institutions recognizing the operational and technological value of AI tools and risk-based AI cybersecurity strategies tend to achieve greater cybersecurity efficiency and responsiveness.

However, the study also extends prior literature by demonstrating that the success of AI-driven cybersecurity is not solely dependent on technical performance but also on organizational

and regulatory integration. Previous research, such as Mishra (2023) and Udeh et al. (2024), has noted that while AI significantly enhances detection and response capabilities, its adoption in financial institutions can be hindered by challenges in aligning with regulatory frameworks and ensuring the ethical use of data. The results from this study corroborate these insights, revealing that while AI technologies have improved institutional adaptability and resilience, issues related to compliance and governance stability have been perceived more variably. These findings suggest that even when AI systems are technologically advanced, the absence of transparent cybersecurity governance and risk management or alignment with compliance standards may constrain their institutional impact, confirming Vial et al.'s (2024) observation that privacy and data-use limitations often limit the full potential of AI in financial cybersecurity.

Moreover, this study contributes to the literature by empirically validating the impact of human–AI collaboration on the overall success of AI-driven cybersecurity systems. Earlier studies broadly discussed this topic conceptually, highlighting workforce augmentation as a secondary benefit of automation (Faraji et al., 2024; Udeh et al., 2024). The current research, however, found measurable differences in how participants perceived human–AI collaboration and job satisfaction as a function of the complexity and compatibility of AI technologies, reflecting ongoing workforce adaptation and cybersecurity skills gap. This supports the theoretical premise within the DOI framework that user engagement and system complexity directly affect technology acceptance and utilization. Participants who viewed AI tools as more intuitive and better integrated with existing workflows reported higher satisfaction and collaboration scores, emphasizing that successful cybersecurity outcomes depend on both technological sophistication and human adaptability.

Finally, while prior literature has primarily framed AI-driven cybersecurity as a linear progression toward enhanced protection, the current findings reveal a more complex, conditional relationship, moderated by organizational readiness and data governance maturity. This distinction extends prior studies by demonstrating that institutional context determines whether AI adoption translates into measurable cybersecurity gains. In effect, the study confirms that the benefits of AI-driven cybersecurity, such as faster incident response and improved threat prediction, are contingent on alignment among technology, people, and governance structures. This reinforces the socio-technical perspective underlying much of the modern cybersecurity discourse, supporting the notion that sustainable AI integration in finance requires balanced emphasis on technical innovation, human oversight, and regulatory compliance.

Overall, the findings underscore that the efficacy of AI-driven cybersecurity solutions extends beyond algorithmic precision to include the broader institutional environment in which they operate. Financial institutions that effectively integrate AI into existing systems achieve improved detection, response, and resilience; however, these advancements are sustainable only when regulatory and policy frameworks evolve in tandem. Therefore, the next section examines how the compatibility of AI-driven cybersecurity technologies with existing cybersecurity policies and regulatory structures influences their adoption and long-term effectiveness within financial institutions.

Compatibility of AI with Existing Cybersecurity Policies & Regulations

The results of this study indicated that the compatibility of AI-driven cybersecurity technologies had a statistically significant effect on institutional outcomes, including system performance, cybersecurity effectiveness, adaptability, resilience, and the composite construct of data privacy and regulatory compliance. These findings demonstrate that when AI technologies

align with existing cybersecurity frameworks, cybersecurity governance and risk management structures, and compliance mandates, financial institutions experience enhanced performance, more adaptive operations, and stronger privacy protections. The results align closely with the themes identified in the literature review, which emphasize the need to integrate AI solutions into established policy and regulatory frameworks to achieve operational and compliance success (Binhammad et al., 2024; Mishra, 2023; Udeh et al., 2024; Vial et al., 2024).

In prior literature, compatibility has frequently been identified as a central determinant of technology adoption and performance outcomes within the DOI and TAM frameworks. Mishra (2023) found that compatibility significantly predicted adoption success for AI-based cybersecurity systems in the financial sector, underscoring the challenge of integrating AI tools with legacy infrastructure and existing security policies. Similarly, Faraji et al. (2024) highlighted that alignment between AI technologies and institutional compliance requirements, such as the GLBA Safeguards Rule, SEC Regulation S-P, and PCI DSS, was a critical enabler of smooth implementation and sustained regulatory compliance. The current study's findings extend these conclusions by providing quantitative evidence that compatibility not only influences adoption but also correlates with tangible improvements in system performance and regulatory outcomes, confirming theoretical expectations from DOI that greater compatibility accelerates innovation diffusion and operational effectiveness.

The study also reinforces insights from Udeh et al. (2024), who argued that adaptive governance structures must guide AI integration to maintain sustainable compliance in financial platforms. Their analysis underscored that compatibility extends beyond technical interoperability to encompass strategic and regulatory alignment, a perspective mirrored in this study's results, which found that compatibility predicted improved regulatory compliance.

Likewise, Vial et al. (2024) observed that institutions that balance AI innovation with privacy obligations through cooperative frameworks among data scientists, compliance officers, and IT teams achieve an optimal equilibrium between analytical capability and data protection. The current study's results support this socio-technical view: institutions reporting higher compatibility levels demonstrated better alignment between AI-enabled analytics and privacy governance mechanisms, reducing the risk of non-compliance or data misuse.

By contrast, Binhammad et al. (2024) emphasized that digital identity protection frameworks must evolve to remain compatible with emerging AI technologies for authentication and anomaly detection. Their findings suggested that organizations achieving interoperability between AI systems and regulatory identity management standards were better equipped to manage cyber risk. This aligns with the present study's outcome that compatibility significantly affects cybersecurity effectiveness, data privacy, and regulatory compliance, indicating that AI tools aligned with established identity protection and data governance standards enhance institutional resilience.

However, this study advances the literature by quantifying the multivariate influence of compatibility on institutional outcomes across multiple dependent variables rather than assessing adoption alone. While prior work has qualitatively discussed policy alignment or case-specific compliance integration, the present study provides empirical evidence that compatibility is statistically predictive of improved performance, adaptability, and compliance, highlighting its role as both a technological and a governance determinant of AI-driven cybersecurity success. Moreover, the inclusion of the composite construct for data privacy and regulatory compliance further substantiates that compatibility serves as a unifying factor, bridging technical innovation and compliance stability.

The findings corroborate existing research while extending it through quantitative validation. The alignment between AI systems and cybersecurity regulations not only facilitates adoption but also enhances institutional performance and governance outcomes. These results affirm that compatibility functions as a linchpin construct within AI-driven cybersecurity strategy, supporting the DOI framework's assertion that innovations perceived as congruent with existing practices and policies are more likely to achieve successful, sustainable diffusion. Consequently, maintaining continuous compatibility through adaptive policy evolution and cross-departmental governance remains critical for financial institutions navigating the intersection of AI innovation, data privacy, regulatory compliance, and risk-based AI cybersecurity strategies.

Complexity of AI-Driven Cybersecurity and Its Impact on Adoption

The findings of this study revealed that the perceived complexity of AI-driven cybersecurity technologies did not have a statistically significant multivariate effect on the combined dependent variables representing institutional outcomes. This result contrasts with the consistent evidence in prior literature suggesting that the technical sophistication and operational intricacy of AI systems often hinder adoption in regulated environments such as finance. Earlier studies, such as Mishra (2023) and Faraji et al. (2024), argued that implementation challenges stem from the steep learning curve, resource-intensive nature, workforce adaptation and cybersecurity skills gap associated with integrating AI-based cybersecurity systems. Mishra (2023) emphasized that organizations with lower technological maturity frequently struggle to deploy machine-learning algorithms effectively due to limited staff expertise and constrained IT infrastructure, while Faraji et al. (2024) noted that excessive algorithmic opacity increases the difficulty of compliance reporting and human oversight.

By contrast, the current study's nonsignificant finding suggests that within the sampled financial institutions, respondents may have achieved greater organizational readiness and familiarity with AI tools, effectively mitigating the adverse effects of perceived complexity. This outcome may also reflect the relatively high cybersecurity maturity levels typical of financial institutions, where established security operations centers, standardized governance frameworks, and advanced risk management practices help organizations integrate complex technologies more effectively. This aligns partially with Udeh et al. (2024), who found that continuous workforce training and cross-departmental collaboration can offset technical complexity by fostering greater understanding of AI operations among cybersecurity and compliance professionals. The absence of a significant relationship in the present study could therefore reflect an evolution in institutional capabilities, in which complexity no longer serves as a decisive barrier but rather as a manageable characteristic of advanced cybersecurity ecosystems. Moreover, financial institutions increasingly employ vendor-supported AI platforms with user-friendly interfaces and pre-trained models, reducing the operational burden historically associated with high complexity.

However, the finding also diverges from the theoretical expectations derived from the DOI framework, which posits that greater perceived complexity generally slows adoption. In traditional DOI applications, complexity represents a key inhibitor of innovation diffusion because it increases uncertainty and learning requirements. However, the present findings suggest that in highly regulated and technologically mature sectors such as financial services, institutional capabilities, workforce expertise, and vendor-supported AI infrastructures may substantially reduce the perceived barriers associated with technological complexity. The current results may indicate that within the financial cybersecurity domain, institutional pressures for

compliance and resilience override the inhibitory effects of complexity. Regulatory mandates, cybersecurity insurance requirements, and executive-level emphasis on AI-enabled risk detection may have normalized complex technologies as necessary operational investments within cybersecurity governance and risk management rather than optional innovations. This interpretation aligns with Vial et al. (2024), who observed that data-governance-driven organizations are increasingly prioritizing integration and compliance over technical simplicity.

Overall, while the literature widely portrays complexity as a hindrance to AI adoption, this study's empirical findings suggest a shift in context. Financial institutions appeared to be entering a phase in which the operational and regulatory imperatives for AI-enhanced cybersecurity and risk-based AI cybersecurity strategies outweigh concerns about technological complexity. Consequently, complexity may no longer be a primary determinant of adoption outcomes but instead a neutral or even expected attribute of sophisticated, compliance-aligned cybersecurity infrastructures.

AI and Data Privacy Protection

The study's results demonstrated that data privacy and regulatory compliance, combined into a composite construct, were significantly influenced by the compatibility and relative advantage of AI-driven cybersecurity technologies. This finding aligned with the literature, which emphasizes that successful AI integration in cybersecurity depends on ensuring that AI tools adhere to privacy-preserving mechanisms, regulatory frameworks, and cybersecurity governance and risk management. Compatibility with existing data protection laws, such as the GLBA, GDPR, and CCPA, was shown to directly affect institutional confidence and adoption success. Similarly, the relative advantage of AI tools, particularly in improving data exfiltration

detection, fraud prevention detection, and enhancing encryption and anonymization techniques, strengthened compliance performance across financial institutions.

These results are consistent with those of Vial et al. (2024), who highlighted the importance of collaboration among data scientists, data owners, and compliance officers in balancing privacy preservation and analytical performance. Financial institutions that effectively integrate AI technologies into privacy-by-design frameworks exhibit higher trust and improved compliance outcomes. The study's findings also resonate with Faraji et al. (2024), who concluded that AI can both enhance and challenge privacy protection depending on governance and transparency mechanisms. The strong relationship found between compatibility and the composite construct in this study supports their argument that alignment with institutional policies and data governance practices determines whether AI improves or undermines privacy assurance.

However, this study's results diverged somewhat from Mishra (2023), who suggested that AI adoption in the financial sector often introduces privacy trade-offs, as increased automation can reduce human oversight in data management. In contrast, the findings here indicate that well-integrated AI systems improve both privacy protection and regulatory compliance, suggesting that the trade-offs Mishra noted may be mitigated when robust governance and compatibility frameworks are in place. Likewise, Binhammad et al. (2024) asserted that AI-driven identity protection tools enhance security at the expense of user control. In contrast, this study observed that when compatibility and policy alignment are achieved, AI implementations can strengthen user data autonomy rather than diminish it.

Overall, the results of this study provide empirical evidence to the ongoing debate about whether AI enhances or compromises data privacy in regulated environments. The demonstrated

significance of both compatibility and relative advantage variables underscores that privacy protection depends not only on technological sophistication but also on institutional readiness, governance maturity, and the harmonization of AI solutions with existing compliance frameworks. These findings extend prior research by demonstrating that privacy risks can be mitigated through the strategic alignment of AI tools and risk-based AI cybersecurity strategies with established cybersecurity and regulatory frameworks. Thereby confirming that AI-driven privacy protection can coexist with innovation when implemented within a governance-focused model.

Human-AI Collaboration

The results of this study revealed that Human–AI Collaboration and Job Satisfaction demonstrated a moderate but non-significant relationship with the independent constructs of compatibility, complexity, and relative advantage. While participants generally recognized AI as an enabler of cybersecurity efficiency and decision support, the statistical outcomes indicated that the perceived benefits of AI integration were not yet translating into consistent improvements in workforce satisfaction or collaboration. These findings suggest that although financial institutions are increasingly adopting AI tools, the cultural and operational alignment between human professionals and AI systems, including workforce adaptation, remained under development. This aligns with observed patterns in the MANOVA results, in which other dependent variables, such as system performance and data privacy compliance, showed stronger associations, underscoring that human–AI collaboration may be a secondary effect that emerged after technical maturity and regulatory alignment, and cybersecurity governance is achieved.

Compared with the literature, the literature presented a more optimistic perspective on the human–AI dynamic in cybersecurity operations. Mishra (2023) emphasized that AI-enhanced

tools, such as predictive analytics and automated detection systems, could alleviate human workload and improve job satisfaction by reducing repetitive tasks and enhancing accuracy in threat response. Similarly, Udeh et al. (2024) highlighted that sustainable finance platforms that integrate AI exhibited greater collaboration between cybersecurity teams and automated systems, fostering a synergistic environment for proactive defense and continuous learning. However, this study's findings partially diverge from those conclusions, suggesting that the human adaptation curve may be slower in traditional financial institutions, where regulatory compliance and legacy systems impose structural constraints on operational change.

Moreover, Vial et al. (2024) argued that while AI supports analytical depth, it can inadvertently create barriers to human collaboration when transparency is limited, particularly when models operate as "black boxes." This observation resonates with the non-significant statistical relationship identified in this study, indicating that a lack of interpretability and trust in AI recommendations may reduce collaborative engagement. Faraji et al. (2024) similarly cautioned that workforce adaptation requires structured training and clear governance mechanisms to ensure human operators understand and effectively utilize AI systems. These theoretical insights help contextualize why human–AI collaboration, though promising in concept, remains under-realized in empirical practice within U.S. financial cybersecurity environments.

The results reinforce the notion that successful human–AI collaboration depends not only on technical integration but also on organizational readiness, training, transparent governance, and continued workforce adaptation. The divergence between the optimistic projections in prior studies and the more tempered empirical outcomes here reflects the transitional stage of AI adoption in financial institutions. Continued emphasis on interpretability, workforce

empowerment, and ethical design may strengthen collaboration outcomes as AI technologies and human expertise evolve toward greater complementarity.

Overall, the comparative analysis revealed both convergence and divergence between the study's empirical results and prior scholarly findings. Consistent with the existing literature, the data confirmed that AI-driven cybersecurity technologies improve system performance and regulatory compliance when adequately aligned with institutional policies and governance frameworks. However, the findings also revealed notable disparities in areas such as complexity and human–AI collaboration, in which anticipated benefits were less statistically significant than those reported in prior studies. These differences suggest that while financial institutions are advancing in AI adoption, challenges persist in operational integration, transparency, and workforce adaptation. The literature tended to emphasize theoretical and technological potential, whereas this study's empirical results reflected a more pragmatic reality shaped by organizational readiness, regulatory constraints, and the evolving nature of AI governance. Collectively, these insights underscore the need to continue refining AI adoption strategies, balancing innovation with compliance, efficiency with human oversight, and automation with ethical accountability.

Summary

This chapter presented the statistical results examining the influence of the compatibility, complexity, and relative advantage of AI-driven cybersecurity technologies on institutional outcomes in U.S. financial institutions. The analyses evaluated four dependent variables: system performance and cybersecurity effectiveness, adaptability and resilience, human–AI collaboration and job satisfaction, and data privacy and regulatory compliance within

institutional cybersecurity governance, which were combined into a single composite construct to strengthen model robustness.

The dataset consisted of ninety valid responses collected from cybersecurity professionals, IT managers, and compliance officers. Reliability and validity testing confirmed strong internal consistency among the survey constructs (Cronbach's $\alpha > .90$) and alignment with the TAM and DOI theory. Assumption testing verified normality, linearity, and acceptable homogeneity, supporting the use of MANOVA.

Findings indicated that compatibility and relative advantage demonstrated statistically significant multivariate effects on the combined dependent variables, whereas complexity did not. Follow-up univariate analyses revealed that compatibility most strongly influenced system performance, data privacy, and regulatory compliance, while relative advantage was associated with system performance, adaptability, and human–AI collaboration. These results suggest that when AI-driven cybersecurity systems align with existing policies and demonstrate clear operational benefits, adoption and integration are enhanced.

Overall, the results align with prior research emphasizing the importance of organizational readiness, regulatory alignment, and workforce adaptation for successful AI implementation. Chapter 4 provided empirical evidence supporting the theoretical relationships proposed by TAM and DOI and established the foundation for interpreting these findings. Chapter 5 will further analyze these results, discuss implications for theory and practice, and offer recommendations for advancing AI-driven cybersecurity strategies, governance structures, and workforce adaptation in financial institutions.

Chapter 5: Discussion, Recommendations, and Study Summary

The problem addressed in this study was the increasing complexity of integrating AI into financial cybersecurity while ensuring regulatory compliance, data privacy protection, and effective human-AI collaboration (Faraji et al., 2024). The purpose of this quantitative, correlational study was to examine the relationship between the compatibility, complexity, and relative advantage of AI-driven cybersecurity technologies and their adoption and success in financial institutions. To investigate these relationships, the study employed a cross-sectional survey design using a 40-item Likert-scale instrument administered via Qualtrics, yielding 90 valid responses from cybersecurity professionals, IT managers, and compliance officers across U.S. financial institutions. Data analysis procedures included assumption testing, EFA to assess construct validity, and MANOVA to assess multivariate effects across institutional outcome variables. Significant multivariate effects were observed for Compatibility and Relative Advantage, whereas Complexity did not demonstrate a statistically significant effect on institutional outcomes. These results indicated that institutions benefiting most from AI adoption were those that aligned AI capabilities with existing systems and prioritized high value security and compliance needs, consistent with the study's research questions. Additionally, the highly correlated variables Data Privacy and Regulatory Compliance were merged into a composite construct to strengthen multivariate stability and reduce redundancy.

Limitations of the study included the use of self-reported data, the cross-sectional design, which limited causal interpretation, the modest sample size (N = 90), and the potential for response bias given the professional demographics represented. Several statistical assumptions were also violated, including a significant Box's M test and multiple Levene's test violations, which necessitated the use of Pillai's Trace as the primary MANOVA statistic. These

methodological considerations underscore the importance of interpreting the findings within the broader context of institutional cybersecurity governance and risk management, where structural controls and regulatory pressures shape both implementation and outcomes. Although these limitations do not compromise the overall integrity of the findings, they do require careful interpretation regarding generalizability and the magnitude of multivariate relationships.

This chapter is organized into four sections. The discussion interprets the findings in relation to the research questions, theoretical frameworks, and the existing literature. The practice recommendations provide actionable guidance for financial institutions implementing or enhancing AI-driven cybersecurity strategies. The recommendations for future research identify areas for further investigation to expand and refine the study's contributions. The chapter concludes with a Study Summary, which synthesizes the study's purpose, findings, and broader significance. Collectively, the findings also highlight ongoing challenges related to workforce adaptation and the cybersecurity skills gap, particularly as financial institutions integrate AI-driven tools that reshape analyst roles, oversight responsibilities, and decision-making processes.

Discussion

The purpose of this quantitative, correlational study was to examine how the compatibility, complexity, and relative advantage of AI-driven cybersecurity technologies influence their adoption and associated institutional outcomes in U.S. financial institutions. The discussion of findings is organized around the study's significant results and addresses each research question, including the combined influence of compatibility, complexity, and relative advantage examined in Research Question 4. These findings contribute to the understanding of the broader research problem: the challenge of integrating AI tools to enhance cybersecurity performance, support regulatory compliance, improve human–AI collaboration, and strengthen

institutional fraud prevention detection capabilities. In this study, improvements in fraud prevention detection were primarily associated with AI systems that demonstrated strong alignment with existing workflows and delivered measurable operational benefits at the institutional level. This section also evaluates how these results align with, extend, or diverge from existing research and theoretical expectations based on the TAM and DOI frameworks.

Compatibility

Research Question 1 examined the extent to which the compatibility of AI-driven cybersecurity technologies with existing financial cybersecurity policies influenced implementation success, regulatory compliance, and data privacy protection. The results of the MANOVA analysis indicated a statistically significant multivariate effect for compatibility; therefore, the null hypothesis for Research Question 1 was rejected.

Compatibility produced a statistically significant multivariate effect on Research Question 1, as demonstrated by the one-way MANOVA results, confirming that alignment between AI-driven cybersecurity tools and existing organizational processes was a critical determinant of successful adoption. Institutions that perceived AI technologies as fitting well with established workflows, security policies, and regulatory expectations reported stronger system performance, improved data privacy and compliance outcomes, and greater adaptability to emerging threats, based on the statistically significant multivariate effects observed across the combined dependent variables examined for Research Question 1. These findings reinforced core TAM and DOI principles, which assert that technologies perceived as congruent with a user's existing environment are more readily accepted and integrated (Jahangir et al., 2023). From an institutional perspective, this alignment reflected the central role of cybersecurity governance

and risk management in shaping how AI tools were evaluated, authorized, and operationalized within regulated financial environments.

Building on the statistically significant multivariate findings for Compatibility in Research Question 1, in the context of financial institutions where consistency with regulatory frameworks such as GLBA, SEC Regulation S-P, and OCC guidance was essential, compatibility became even more influential. AI tools that supported auditability, automated reporting, and standardized security controls directly strengthened institutional risk posture (Vial et al., 2024). These capabilities were consistent with the implementation of risk-based AI cybersecurity strategies, in which AI adoption was prioritized according to regulatory exposure, threat criticality, and organizational risk tolerance. The strong predictive value of compatibility aligned with research indicating that regulatory alignment, workflow integration, and policy reinforcement directly influence the acceptance of cybersecurity tools in highly regulated environments (Faraji et al., 2024; Mishra, 2023). These results meaningfully advanced the literature by demonstrating that in financial cybersecurity ecosystems, compatibility was not merely a facilitator of ease of use; it functioned as a foundational requirement for institutional adoption and successful outcomes (Binhammad et al., 2024; Udeh et al., 2024).

Complexity

Research Question 2 examined the extent to which the complexity of AI-driven cybersecurity technologies influenced adoption outcomes in financial institutions, particularly in relation to regulatory compliance, cybersecurity workforce adaptation, and data privacy management. The MANOVA results indicated that complexity did not produce a statistically significant multivariate effect; therefore, the null hypothesis for Research Question 2 was retained.

In contrast to the findings for compatibility and relative advantage, complexity did not demonstrate a statistically significant multivariate effect on institutional outcomes for Research Question 2, as indicated by the one-way MANOVA results. Although complexity has often been cited in the literature as a barrier to the adoption of advanced technologies, the results suggest that the perceived difficulty or effort associated with AI tools may no longer be a primary concern for cybersecurity and IT professionals in financial institutions (Faraji et al., 2024). This divergence from some DOI expectations could be partially explained by the sample's professional composition, which included highly trained cybersecurity specialists, IT managers, and compliance professionals accustomed to working with sophisticated systems (Mishra, 2023). For this population, complexity was perceived as a routine component of cybersecurity work rather than an inhibiting factor. This perception suggested that workforce adaptation challenges and the cybersecurity skills gap were less pronounced within the sampled institutions.

Additionally, many financial institutions had invested heavily in digital transformation, workforce upskilling, and automated security operations, which might reduce the perceived burden of using AI tools. Such investments likely mitigated traditional workforce adaptation challenges, enabling organizations to absorb AI-driven complexity without exacerbating existing cybersecurity skills gaps. These interpretations are grounded in the absence of statistically significant multivariate effects of Complexity on the institutional outcome variables examined in Research Question 2, which helps explain why complexity did not significantly influence adoption or institutional outcomes in this study (Binhammad et al., 2024). Although this finding diverged from some prior research, it highlighted a significant shift in technologically mature organizations (Vial et al., 2024). Thus, the study reveals that complexity might not impede AI

adoption in environments where institutional readiness, workforce expertise, and digital infrastructure were already well developed.

Relative Advantage

Research Question 3 examined the extent to which the relative advantages of AI-driven cybersecurity technologies influenced adoption success in financial institutions, particularly in improving threat detection, fraud prevention, and cybersecurity workforce decision-making capabilities. The MANOVA results demonstrated a statistically significant multivariate effect for relative advantage; therefore, the null hypothesis for Research Question 3 was rejected.

Relative advantage demonstrated a statistically significant multivariate effect on Research Question 3, as evidenced by the one-way MANOVA results, indicating that the perceived benefits of AI tools played a decisive role in shaping adoption and institutional outcomes. Respondents who recognized improvements in threat detection, fraud prevention, incident response efficiency, and overall decision-making reported more favorable institutional performance across the dependent variables, as reflected in the significant multivariate pattern observed for Relative Advantage (Mishra, 2023). This aligned with the DOI theory assertion that innovations offering clear, measurable advantages were more likely to be adopted and assimilated (Jahangir et al., 2023). The study's results reinforced existing scholarly findings that highlighted AI's potential to strengthen cybersecurity resilience, improve anomaly detection, reduce false positives, and support proactive risk management (Binhammad et al., 2024; Faraji et al., 2024).

Moreover, consistent with the statistically significant multivariate findings for Relative Advantage, these findings extended TAM by demonstrating that perceived usefulness, operationalized as relative advantage, remained a potent predictor even when the technology was

complex or sophisticated, or when it was deployed in highly regulated environments. Financial institutions appeared motivated to adopt AI technologies when the tools demonstrated superior capabilities relative to traditional systems, a conclusion supported by the observed relationships between Relative Advantage and institutional outcome measures examined in Research Question 3. These results meaningfully contributed to the literature by quantifying how AI benefits translated into institutional-level outcomes, providing empirical support for theoretical expectations in modern cybersecurity contexts.

Taken together, the findings reinforce the complementary value of TAM and DOI frameworks in explaining AI-driven cybersecurity adoption within financial institutions. Compatibility and relative advantage demonstrated meaningful influence on institutional outcomes, highlighting the importance of technological alignment and perceived operational value in shaping adoption decisions within highly regulated cybersecurity environments. In contrast, the absence of a significant effect for complexity suggests that in technologically mature organizations with skilled cybersecurity professionals, perceived difficulty may be less influential than strategic fit and measurable security benefits.

Recommendations for Practice

The results of this study provided several actionable insights for financial institutions seeking to enhance cybersecurity effectiveness through the adoption of AI-driven technologies. Because compatibility and relative advantage had emerged as significant predictors of institutional outcomes, and complexity did not demonstrate a significant multivariate effect, the recommendations below emphasized strategies that strengthened policy alignment, maximized organizational benefits, and supported effective human–AI integration. These recommendations were designed to guide cybersecurity leaders, compliance officers, and IT managers in

translating empirical findings into operational improvements that enhance security posture, regulatory readiness, fraud-prevention capabilities, and workforce support.

Practice Recommendation 1

Financial institutions should strengthen the alignment between AI-driven cybersecurity tools and existing cybersecurity policies and regulatory frameworks to improve implementation success, ensure regulatory compliance, and enhance data protection outcomes. This recommendation was directly supported by the statistically significant MANOVA results for Compatibility reported in Chapter 4 (see Table 4.12a), which showed that higher perceived compatibility was associated with significantly stronger institutional outcomes across system performance, regulatory compliance, and data privacy protection. Given the significant influence of compatibility on institutional outcomes, organizations should prioritize selecting and implementing AI technologies that align with established cybersecurity policies, regulatory expectations, and internal governance structures. Ensuring consistency with requirements such as the GLBA, SEC Regulation S-P, and other sector-specific regulatory standards could reduce operational friction, facilitate smoother adoption, and strengthen compliance and data protection practices (Vial et al., 2024). From a governance and risk management perspective, institutions should conduct structured compatibility assessments during procurement and implementation phases, focusing on interoperability with legacy systems, integration with existing monitoring tools, audit and reporting requirements, and support for policy-based access controls. This approach reinforced cybersecurity governance and risk management by embedding AI adoption decisions within formal risk assessment, compliance validation, and oversight processes rather than treating AI deployment as a purely technical initiative. The emphasis on policy-aligned implementation was consistent with prior findings that effective AI governance frameworks were

essential for maintaining regulatory compliance, organizational stability, and operational trust in cybersecurity environments (Udeh et al., 2024).

Practice Recommendation 2

Organizations in the financial sector are encouraged to focus on AI-enabled cybersecurity technologies that deliver demonstrable improvements in threat identification, fraud mitigation, and analytical decision-making, thereby strengthening overall security outcomes. This recommendation is directly supported by the statistically significant MANOVA results for Relative Advantage reported in Chapter 4 (see Table 23), which showed that higher perceived relative advantage was associated with significantly stronger institutional outcomes across system performance, fraud prevention, workforce augmentation, and decision-making effectiveness. Relative advantage was a significant predictor of positive institutional outcomes, underscoring that financial institutions benefited most when AI tools provided measurable improvements in security performance. Leaders should therefore prioritize AI technologies with demonstrated capabilities in advanced threat detection, behavioral analytics, anomaly identification, and automated fraud prevention (Binhammad et al., 2024; Faraji et al., 2024). Prioritizing these capabilities supported the use of risk-based AI cybersecurity strategies, in which AI investments were aligned with institutional threat exposure, regulatory risk, and the potential impact of security failures. Emphasizing solutions that enhance accuracy, reduce false positives, and accelerate response times could produce substantial operational and compliance benefits. Organizations should also integrate performance metrics, such as incident-detection accuracy, fraud-reduction rates, or time-to-response benchmarks into technology evaluation and continuous monitoring processes. Tracking these metrics enabled institutions to evaluate the effectiveness of AI-driven fraud prevention and detection efforts directly and to justify continued

investment based on measurable security outcomes. This practice ensures that AI-enabled tools consistently contribute to institutional resilience while supporting strategic objectives related to risk reduction and governance stability (Udeh et al., 2024).

Practice Recommendation 3

To fully realize the benefits of AI-driven cybersecurity initiatives, financial institutions need to invest in workforce development and foster collaborative practices that enable effective integration of human expertise with intelligent systems. This recommendation was informed by the non-significant multivariate MANOVA results for Complexity reported in Chapter 4 (see Table 22), which indicated that perceived complexity did not have a statistically significant multivariate effect on institutional outcomes. Although complexity did not statistically influence institutional outcomes, the literature emphasized that effective human–AI collaboration remained essential for realizing the benefits of cybersecurity automation (Binhammad et al., 2024; Mishra, 2023). Financial institutions should therefore invest in targeted workforce training programs that enhance employee proficiency with AI tools, clarify decision-support roles, and reinforce proper handling of sensitive data within AI-enabled workflows. Such investments addressed workforce adaptation challenges and helped mitigate the cybersecurity skills gap that can emerge as organizations adopt increasingly sophisticated AI-driven security technologies. Organizations should also establish governance structures that support collaboration among cybersecurity teams, compliance staff, and data scientists, ensuring that AI insights are interpreted accurately and used to inform risk decisions. By fostering a workforce culture that embraces AI as a collaborative partner rather than a replacement, institutions can reduce resistance to adoption, improve job satisfaction, and enhance overall cybersecurity performance.

Recommendations for Future Research

This study examined the influence of the compatibility, complexity, and relative advantage of AI-driven cybersecurity technologies on institutional outcomes in U.S. financial institutions. The current research used a quantitative, correlational design grounded in the TAM and DOI. The findings offered meaningful theoretical and practical contributions and revealed new opportunities for future research. Researchers could build upon the framework, address methodological limitations, and advance understanding of AI adoption in cybersecurity contexts. Identifying these opportunities was essential to advancing empirical understanding of AI-driven cybersecurity adoption. Future research could also examine how organizations operationalize risk-based AI cybersecurity strategies, particularly how AI adoption decisions are prioritized based on threat severity, regulatory exposure, and institutional risk tolerance. This dissertation helped guide investigations aimed at refining theoretical models, improving methodological rigor, and responding to the evolving technological and regulatory landscape shaping financial cybersecurity.

Future Recommendation 1

Future researchers should consider extending this line of inquiry by using a longitudinal or mixed-methods design to capture how perceptions of AI-driven cybersecurity technologies evolve. This recommendation is informed by the cross-sectional survey design used to address Research Questions 1 through 4 in the present study, which limited causal inference and captured organizational perceptions at a single point in time. As a result, the findings could not fully account for changes related to system maturation, workforce adaptation, or new regulatory requirements. Longitudinal approaches would be especially valuable for examining workforce adaptation over time and assessing how compatibility and relative advantage influence

institutional outcomes as AI tools progress from introduction to routine use. Additionally, incorporating qualitative methods, such as interviews or focus groups, with cybersecurity professionals, compliance officers, and leadership could provide deeper insight into governance challenges, decision-making, and human–AI collaboration that surveys may miss.

Future Recommendation 2

Future research should examine organizations beyond U.S. financial institutions. This recommendation is informed by the scope of the present study, which focused exclusively on cybersecurity professionals working within U.S. financial institutions to address Research Questions 1 through 4. The highly regulated financial sector may uniquely shape perceptions of AI compatibility, complexity, and relative advantage, particularly with respect to data privacy and compliance. Studying sectors such as healthcare, defense, energy, or critical infrastructure could allow researchers to examine whether similar relationships hold under different conditions. Comparative or cross-national studies could also explore how differences in legal frameworks, organizational culture, and threat landscapes influence AI adoption and institutional outcomes. Expanding the focus in this way could improve the generalizability of findings and contribute to a broader understanding of AI-driven cybersecurity adoption across diverse organizational and regulatory contexts.

Future Recommendation 3

The logical extension of this research stream was to extend the TAM and DOI framework informed by the findings of the present study, which examined only the technological perception constructs of compatibility, complexity, and relative advantage across Research Questions 1 through 4. Factors such as organizational cybersecurity maturity, leadership support, ethical AI governance, trust in automated decision-making, and workforce reskilling initiatives might play

a critical role in shaping institutional outcomes beyond technological perceptions alone. Incorporating these factors would allow future studies to more explicitly model cybersecurity governance and risk management as integral mechanisms through which AI adoption influences institutional stability and compliance outcomes. Future researchers could examine these factors as moderating and mediating variables, using advanced analytical approaches, such as structural equation modeling (SEM). This expanded modeling could enable a more holistic understanding of how the technological, human, and organizational dimensions interact to influence cybersecurity effectiveness, regulatory stability, and sustained human–AI collaboration.

Together, these recommendations provide a clear path to advance research on AI-driven cybersecurity adoption. They build established theoretical frameworks while directly addressing the methodological, contextual, and scope-related limitations identified in this study. By expanding research designs, broadening organizational contexts, and including more human and governance-related elements, future studies could deepen insight into how AI technologies affect cybersecurity, regulatory stability, and workforce trends. These research directions lay the groundwork for continued academic inquiry and set the stage for the study's final summary of contributions, implications, and significance.

Study Summary

This quantitative, correlational study examined how the compatibility, complexity, and relative advantage of AI-driven cybersecurity technologies affected institutional outcomes in U.S. financial institutions. The research focused on integrating AI-based cybersecurity while ensuring regulatory compliance, data protection, and effective human–AI collaboration. Data were collected from 90 cybersecurity professionals, IT managers, and compliance officers through a cross-sectional survey. The design was based on the Technology Acceptance Model

and the Diffusion of Innovations theory. Analyses included exploratory factor analysis and multivariate analysis of variance.

The findings demonstrated that perceived compatibility and relative advantage of AI-driven cybersecurity technologies had statistically significant multivariate effects on key institutional outcomes, including system performance and cybersecurity effectiveness; adaptability and resilience; human–AI collaboration and job satisfaction; and data privacy and regulatory compliance. These outcomes also reflected improvements in AI-supported fraud prevention detection, particularly where AI tools enhanced anomaly identification and decision support within regulated financial environments. In contrast, perceived complexity did not exhibit a significant multivariate effect, suggesting that technical difficulty might be less influential in organizations with higher cybersecurity maturity and a skilled workforce. Additionally, the decision to merge the highly correlated constructs of data privacy and regulatory compliance strengthened the stability and interpretability of the multivariate model, reinforcing the interconnected nature of governance and data protection within regulated financial environments.

This study showed that successful AI-driven cybersecurity adoption in financial institutions relied primarily on strategic alignment, organizational value, and regulatory fit, rather than on technical complexity. When AI solutions aligned with current policies and delivered clear operational and security benefits, institutions achieved better performance, compliance, and workforce outcomes. These findings further suggested that addressing workforce adaptation and the cybersecurity skills gap was essential for sustaining long-term benefits from AI-driven cybersecurity adoption. These empirical findings validated key theoretical constructs and provided actionable guidance to support sustainable, governance-aligned AI adoption in

regulated environments. In doing so, this study contributes to the growing body of cybersecurity research examining how AI technologies can be responsibly integrated into critical financial infrastructures while maintaining regulatory stability, workforce collaboration, and organizational resilience.

References

Abikoye, B. E., Adelusi, W., Umeorah, S. C., & Adelaja, A. O. (2024). Integrating risk management in fintech and traditional financial institutions through AI and machine learning. *Journal of Economics, Management and Trade*, *30*(8), 90-102. https://doi.org/10.20944/preprints202407.1609.v1.

Adegbite, A. O., Akinwolemiwa, D. I., Uwaoma, P. U., Kaggwa, S., Akindote, O. J., & Dawodu, S. O. (2023). Review of cybersecurity strategies in protecting national infrastructure: Perspectives from the USA. *Computer Science & IT Research Journal*, *4*(3), 200–219. https://doi.org/10.51594/csitrj.v4i3.658.

Adejumo, A., & Ogburie, C. (2025a). Strengthening finance with cybersecurity: Ensuring safer digital transactions. *World Journal of Advanced Research and Reviews*, *25*(3), 1527–1541. https://doi.org/10.30574/wjarr.2025.25.3.0908.

Adejumo, A., & Ogburie, C. (2025b). The role of cybersecurity in safeguarding finance in a digital era. *World Journal of Advanced Research and Reviews*, *25*(3), 1542–1556. https://doi.org/10.30574/wjarr.2025.25.3.0909.

Ahmed, S., Alshater, M. M., Ammari, A. E., & Hammami, H. (2022). Artificial intelligence and machine learning in finance: A bibliometric review. *Research in International Business and Finance*, *61*, 101646. https://doi.org/10.1016/j.ribaf.2022.101646.

Ajakaye, O. O., Olanrewaju, A. G., Fawehinmi, D., Afolabi, R., & Pius-Kiate, G. M. (2025). Integrating Artificial Intelligence in organizational cybersecurity: Enhancing consumer data protection in the US Fintech Sector. *World Journal of Advanced Research and Reviews*, *26*(1), 2802-2821. https://doi.org/10.30574/wjarr.2025.26.1.1421.

Ajayi, A. J., Joseph, S. A., Metibemu, O. C., Olutimehin, A. T., Balogun, A. Y., & Olaniyi, O. O. (2025). The Impact of Artificial Intelligence on cyber security in digital currency transactions. *Archives of Current Research International*, *25*(2), 329–351. https://doi.org/10.9734/acri/2025/v25i21090.

Ajzen, I. (1991). The theory of planned behavior. The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T.

Ali, A., & Shah, M. (2024). What hinders adoption of artificial intelligence for cybersecurity in the banking sector. *Information*, *15*(12), 760. https://doi.org/10.3390/info15120760

Ali, G., Mijwil, M. M., Buruga, B. A., & Abotaleb, M. (2024). A comprehensive review on cybersecurity issues and their mitigation measures in fintech. *Iraqi Journal for Computer Science and Mathematics*, *5*(3). https://doi.org/10.52866/ijcsm.2024.05.03.004.

Almansoori, A., Al-Emran, M., & Shaalan, K. (2023). Exploring the frontiers of cybersecurity behavior: A systematic review of studies and theories. *Applied Sciences*, *13*(9), 5700. https://doi.org/10.3390/app13095700.

Alneyadi, M. & Normalini, K. (2023). Factors influencing user's intention to adopt AI-Based cybersecurity systems in the UAE. *Interdisciplinary Journal of Information, Knowledge, and Management*, *18*, 459–486. https://doi.org/10.28945/5166.

Ashraf, M., Hafeez, R., & Sajid, A. N. (2022). Factors affecting the adoption of fin-tech in Pakistan based on the unified theory of acceptance and use of technology model: An empirical study on financial inclusion in Pakistan. *Journal of Financial Technologies (Fintech), Inclusion and Sustainability*, *1*(1), 9-26. https://journals.iub.edu.pk/index.php/jftis/article/view/1793.

Awosika, T., Shukla, R. M., & Pranggono, B. (2024). Transparency and privacy: The role of explainable AI and federated learning in financial fraud detection. *IEEE Access*, *12*, 64551–64560. https://doi.org/10.1109/ACCESS.2024.3394528.

Bajunaied, K., Hussin, N., & Kamarudin, S. (2023). Behavioral intention to adopt fintech services: An extension of unified theory of acceptance and use of technology. *Journal of Open Innovation: Technology, Market, and Complexity*, *9*(1), 100010. https://doi.org/10.1016/j.joitmc.2023.100010.

Banerjee, R., Nath, S., Mitra, S. P., Sengupta, P., Islam, M. M., Mukherjee, D., & Biswas, M. (2025). Human-AI partnership: Exploring the potential for coevolutionary progress. *Cuestiones de Fisioterapia*, *54*(3), 4803-4808. https://cuestionesdefisioterapia.com/index.php/es/article/view/2249.

Baruwal Chhetri, M., Tariq, S., Singh, R., Jalalvand, F., Paris, C., & Nepal, S. (2024). Towards human-AI teaming to mitigate alert fatigue in security operations centres. *ACM Transactions on Internet Technology*, *24*(3), 1–22. https://doi.org/10.1145/3670009.

Baxter, G., & Sommerville, I. (2011). Socio-technical systems: From design methods to systems engineering. *Interacting with computers*, *23*(1), 4–17. https://doi.org/10.1016/j.intcom.2010.07.003.

Binhammad, M., Alqaydi, S., Othman, A., & Abuljadayel, L. H. (2024). The role of AI in cyber security: Safeguarding digital identity. *Journal of Information Security*, *15*(02), 245-278. https://doi.org/10.4236/jis.2024.152015.

Boletsis, C., Halvorsrud, R., Pickering, J., Phillips, S., & Surridge, M. (2021). Cybersecurity for SMEs: Introducing the human element into socio-technical cybersecurity risk assessment: *Proceedings of the 16th International Joint Conference on Computer Vision, Imaging*

and Computer Graphics Theory and Applications, 266–274. https://doi.org/10.5220/0010332902660274.

Boorugupalli, K. K., Kulkarni, A. K., Suzana, A., M, D., Ponnusamy, S., & Kumar S, S. (2025). Cybersecurity Measures in Financial Institutions Protecting Sensitive Data from Emerging Threats and Vulnerabilities. *ITM Web of Conferences*, *76*, 02002. https://doi.org/10.1051/itmconf/20257602002.

Cai, W., Pasquale, L., Ramkumar, K., McCarthy, J., Nuseibeh, B., & Doherty, G. (2023). Human-AI collaboration for sustainable security: Opportunities and challenges. In *USENIX Symposium on Usable Privacy and Security (SOUPS)*. https://www.usenix.org/system/files/soups2023-poster98_cai_abstract_final.pdf

Chakkappan, G., Morshed, A., & Rashid, M. M. (2024). Explainable AI and big data analytics for data security risk and privacy issues in the financial industry. *2024 IEEE Conference on Engineering Informatics (ICEI)*, 1–9. https://doi.org/10.1109/ICEI64305.2024.10912422.

Choithani, T., Chowdhury, A., Patel, S., Patel, P., Patel, D., & Shah, M. (2024). A comprehensive study of artificial intelligence and cybersecurity on bitcoin, crypto currency and banking system. *Ann. Data. Sci. 11*(1), 103-135. https://doi.org/10.1007/s40745-022-00433-5.

Chung, M.-H., Chignell, M., Wang, L., Jovicic, A., & Raman, A. (2020). Interactive Machine Learning for Data Exfiltration Detection: Active Learning with Human Expertise. *2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 280–287. https://doi.org/10.1109/SMC42975.2020.9282831.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319–340. https://doi.org/10.2307/249008

Dawodu, S. O., Omotosho, A., Akindote, O. J., Adegbite, A. O, & Ewuga, S. K. (2023). Cybersecurity risk assessment in banking: Methodologies and best practices. *Computer Science & IT Research Journal*, *4*(3), 220–243. https://doi.org/10.51594/csitrj.v4i3.659.

Deshpande, A. (2024). Cybersecurity in financial services: Addressing AI-related threats and vulnerabilities. *2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS)*, 1–6. https://doi.org/10.1109/ICKECS61492.2024.10616498.

Dhanawat, V., Shinde, V., Karande, V., & Singhal, K. (2024). Enhancing financial risk management with federated AI. *2024 8th SLAAI International Conference on Artificial Intelligence (SLAAI-ICAI)*, 1–6. https://doi.org/10.1109/SLAAI-ICAI63667.2024.10844982.

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review, 48*(2), 147–160. https://doi.org/10.2307/2095101.

Djenna, A., Barka, E., Benchikh, A., & Khadir, K. (2023). Unmasking cybercrime with artificial-intelligence-driven cybersecurity analytics. *Sensors*, *23*(14), 6302. https://doi.org/10.3390/s23146302.

Dopamu, O., Adesiyan, J., & Oke, F. (2024). Artificial intelligence and US financial institutions: Review of AI-assisted regulatory compliance for cybersecurity. *World Journal of Advanced Research and Reviews, 21*(3), 964–979. https://doi.org/10.30574/wjarr.2024.21.3.0791.

Duggal, M., Moholkar, N., Bhope, A., Rane, D. P., Ubarhande, K., & Raje, H. (2024). Impact of Emerging Technologies on Financial Management Systems: AI, ML, and Cybersecurity Perspectives. *2024 Second International Conference Computational and Characterization Techniques in Engineering & Sciences (IC3TES)*, 1–5. https://doi.org/10.1109/IC3TES62412.2024.10877441.

Ebert, C., & Beck, M. (2023). Artificial intelligence for cybersecurity. *IEEE Software*, *40*(6), 27–34. https://doi.org/10.1109/MS.2023.3305726.

Faraji, M. R., Shikder, F., Hasan, M. H., Islam, M. M., & Akter, U. K. (2024). Examining the role of artificial intelligence in cyber security (CS): A systematic review for preventing prospective solutions in financial transactions. *International Journal*, *5*(10), 4766-4782. DOI: https://doi.org/10.61707/7rfyma13.

Folorunso, A., Adewumi, T., Adewa, A., Okonkwo, R., & Olawumi, T. N. (2024). Impact of AI on cybersecurity and security compliance. *Global Journal of Engineering and Technology Advances*, *21*(1), 167–184. https://doi.org/10.30574/gjeta.2024.21.1.0193.

Gale, M., Bongiovanni, I., & Slapnicar, S. (2022). Governing cybersecurity from the boardroom: Challenges, drivers, and ways ahead. *Computers & Security*, *121*, 102840. https://doi.org/10.1016/j.cose.2022.102840.

George, A. S. (2023). Securing the future of finance: How AI, blockchain, and machine learning safeguard emerging Neobank technology against evolving cyber threats. *Partners Universal Innovative Research Publication, 1*(1), 54-66. https://doi.org/10.5281/ZENODO.10001735.

Ghandour, A. (2021). Opportunities and challenges of artificial intelligence in banking: Systematic literature review. *TEM Journal*, 1581–1587. https://doi.org/10.18421/TEM104-12.

Gopal, S., Gupta, P., & Minocha, A. (2023). Advancements in Fin-Tech and Security Challenges of Banking Industry. *2023 4th International Conference on Intelligent Engineering and Management (ICIEM)*, 1–6. https://doi.org/10.1109/ICIEM59379.2023.10165876.

Goswami, S. S., Mondal, S., Halder, R., Nayak, J., & Sil, A. (2024). Exploring the impact of artificial intelligence integration on cybersecurity: A comprehensive analysis. *Journal of Industrial Intelligence*, *2*(2), 73–93. https://doi.org/10.56578/jii020202.

Gupta, A., & Owusu, A. (2025). Regulating risk culture in the insurance industry using machine learning. *Journal of Risk & Insurance*, *92*(2), 536–574. https://doi.org/10.1111/jori.70009.

Han, Y., Chen, J., Dou, M., Wang, J., & Feng, K. (2023). The impact of artificial intelligence on the financial services industry. *Academic Journal of Management and Social Sciences*, *2*(3), 83–85. https://doi.org/10.54097/ajmss.v2i3.8741.

Hassan, M., Aziz, L. A.-R., & Andriansyah, Y. (2023). The role Artificial Intelligence in modern banking: an exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance. *Reviews of Contemporary Business Analytics, 6*(1), 110–132. Retrieved from https://researchberg.com/index.php/rcba/article/view/153.

Hentzen, J. K., Hoffmann, A., Dolan, R., & Pala, E. (2022). Artificial intelligence in customer-facing financial services: A systematic literature review and agenda for future research. *International Journal of Bank Marketing*, *40*(6), 1299–1336. https://doi.org/10.1108/IJBM-09-2021-0417.

Jahangir, W. & Zia-ul-Haq. (2023). Integrating technology acceptance model, theory of diffusion of innovations and theory of planned behaviour to study the adoption of Facebook marketplace. *NMIMS Management Review*, *31*(3), 214–222. https://doi.org/10.1177/09711023231205500.

Jain, V., Balakrishnan, A., Beeram, D., Najana, M., & Chintale, P. (2024). Leveraging Artificial Intelligence for Enhancing Regulatory Compliance in the Financial Sector. International Journal of Computer Trends and Technology, 72(5), 124–140. https://doi.org/10.14445/22312803/IJCTT-V72I5P116.

Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P., & Hur, J. (2024). Cybersecurity threats in FinTech: A systematic review. *Expert Systems with Applications*, *241*, 122697. https://doi.org/10.1016/j.eswa.2023.122697.

Jony, M. A. M., Arafat, M. S., Islam, R., Rafi, S. S., Jalil, M. S., & Hossen, F. (2024). AI-powered cybersecurity in financial institutions: Enhancing resilience against emerging digital threats. *Advanced International Journal of Multidisciplinary Research*, *2*(6), 1113. https://doi.org/10.62127/aijmr.2024.v02i06.1113.

Kang, W., Shao, B., Du, S., Chen, H., & Zhang, Y. (2024). How to improve voice assistant evaluations: Understanding the role of attachment with a socio-technical systems perspective. *Technological Forecasting and Social Change*, *200*, 123171. https://doi.org/10.1016/j.techfore.2023.123171.

Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, *97*, 101804. https://doi.org/10.1016/j.inffus.2023.101804.

Kumari, B., Kaur, J., & Swami, S. (2024). Adoption of artificial intelligence in financial services: A policy framework. *Journal of Science and Technology Policy Management*, *15*(2), 396–417. https://doi.org/10.1108/JSTPM-03-2022-0062.

López González, A., Moreno, M., Moreno Román, A. C., Hadfeg Fernández, Y., & Cepero Pérez, N. (2024). Ethics in artificial intelligence: An approach to cybersecurity. *Inteligencia Artificial*, *27*(73), 38–54. https://doi.org/10.4114/intartif.vol27iss73pp38-54

Martin, T. (2022). On the need for collaborative intelligence in cybersecurity. *Electronics*, *11*(13), 2067. https://doi.org/10.3390/electronics11132067.

Malatji, M., & Tolah, A. (2024). Artificial intelligence (AI) cybersecurity dimensions: A comprehensive framework for understanding adversarial and offensive AI. *AI and Ethics*. https://doi.org/10.1007/s43681-024-00427-4.

Mishra, S. (2023). Exploring the impact of AI-based cyber security financial sector management. *Applied Sciences (2076-3417)*, *13*(10), 5875. https://doi.org/10.3390/app13105875.

Mullin, J. (2023). Artificial Intelligence and bank supervision. Econ Focus, Federal Reserve Bank of Richmond, 23, 8-11. https://www.richmondfed.org/publications/research/econ_focus/2023/q2_federal_reserve.

Norzelan, N. A., Mohamed, I. S., & Mohamad, M. (2024). Technology acceptance of artificial intelligence (AI) among heads of finance and accounting units in the shared service industry. *Technological Forecasting and Social Change*, *198*, 123022. https://doi.org/10.1016/j.techfore.2023.123022.

Nwafor, K. C., Ikudabo, A. O., & Onyeje, C. C. (2024). Mitigating cybersecurity risks in financial institutions: The role of AI and data analytics. *International Journal of Science and Research Archive*, *13*(1), 2895–2910. https://doi.org/10.30574/ijsra.2024.13.1.2014.

Ogbanufe, O., Kim, D. J., & Jones, M. C. (2021). Informing cybersecurity strategic commitment through top management perceptions: The role of institutional pressures. *Information & management*, *58*(7), 103507. https://doi.org/10.1016/j.im.2021.103507

Oriji, O., Shonibare, M. A., Daraojimba, R. E., Abitoye, O., & Daraojimba, C. (2023). Financial technology evolution in Africa: A comprehensive review of legal frameworks and implications for AI-driven financial services. *International Journal of Management & Entrepreneurship Research*, *5*(12), 929–951. https://doi.org/10.51594/ijmer.v5i12.627.

Paul, E. O., Callistus, O., Somtobe, O., Esther, T., Somto, K.-A., Clement, O., & Ejimofor, I. (2023). Cybersecurity strategies for safeguarding customer's data and preventing financial fraud in the United States financial sectors. *International Journal on Soft Computing*, *14*(3), 01–16. https://doi.org/10.5121/ijsc.2023.14301.

Phillips, T., & Conner, A. Financial regulatory agencies. https://https://www.americanprogress.org/wp-content/uploads/sites/2/2024/06/AI-5-FinancialRegAgencies.pdf

Rana, S., & Chicone, R. (2024). Navigating the paradox of AI in cybersecurity: Unpacking societal optimism and ethical skepticism. *Issues in Information Systems*, *25*(1), 175–187. https://doi.org/10.48009/1_iis_2024_115.

Rizvi, M. (2023). Enhancing cybersecurity: The power of artificial intelligence in threat detection and prevention. *International Journal of Advanced Engineering Research and Science*, *10*(5), 055–060. https://doi.org/10.22161/ijaers.105.8.

R, S., & Bagrecha, C. (2023). A study on generative AI and its impact on banking and financial services sector: Data privacy & sustainable perspective. *2023 IEEE Technology & Engineering Management Conference - Asia Pacific (TEMSCON-ASPAC), Technology & Engineering Management Conference - Asia Pacific (TEMSCON-ASPAC), 2023 IEEE*, 1–5. https://doi.org/10.1109/TEMSCON-ASPAC59527.2023.10531592.

Robles, P., & Mallinson, D. J. (2023). Catching up with AI: Pushing toward a cohesive governance framework. Politics & Policy, 51(3), 355–372. https://doi.org/10.1111/polp.12529.

Rogers, E. M. (2003b). *Diffusion of Innovations, 5th Edition*. Simon and Schuster

Salem, A. H., Azzam, S. M., Emam, O. E., & Abohany, A. A. (2024). Advancing cybersecurity: A comprehensive review of AI-driven detection techniques. *Journal of Big Data*, *11*(1), 105. https://doi.org/10.1186/s40537-024-00957-y.

Sai Meghana, G. V., Saqlain Afroz, S., Gurindapalli, R., Katari, S., & Swetha, K. (2024). A Survey paper on Understanding the Rise of AI-driven Cyber Crime and Strategies for Proactive Digital Defenders. *2024 4th International Conference on Pervasive Computing and Social Networking (ICPCSN)*, 25–30. https://doi.org/10.1109/ICPCSN62568.2024.00012.

Sontan, A. D. & Samuel, S. V. (2024). The intersection of artificial intelligence and cybersecurity: Challenges and opportunities. *World Journal of Advanced Research and Reviews*, *21*(2), 1720–1736. https://doi.org/10.30574/wjarr.2024.21.2.0607.

Temelkov, Z. (2023). Overview of artificial intelligence (AI) application in the banking industry. *International Journal of Economics, Management and Tourism*, *3*(2), 43–51. https://doi.org/10.46763/IJEMT2332043t.

Thapaliya, S. (2024). Examining the influence of AI-driven cybersecurity in financial sector management. *The Batuk*, *10*(2), 129-144. https://doi.org/10.3126/batuk.v10i2.68147.

Todupunuri, A. (2023). The role of artificial intelligence in enhancing cybersecurity measures in online banking using AI. *International Journal of Enhanced Research in Management & Computer Applications*, *12*(01), 10-55948. https://scholar9.com/publication/e26be2ba1c2420f1326becc52794d6db.pdf

Udeh, E. O., Amajuoyi, P., Adeusi, K. B., & Scott, A. O. (2024). The integration of artificial intelligence in cybersecurity measures for sustainable finance platforms: An analysis. *Computer Science & IT Research Journal*, *5*(6), 1221-1246. https://doi.org/10.51594/csitrj.v5i6.1195.

Vafaei-Zadeh, A., Nikbin, D., Teoh, K. Y., & Hanifah, H. (2025). Cybersecurity awareness and fear of cyberattacks among online banking users in Malaysia. *International Journal of Bank Marketing*, *43*(3), 476–505. https://doi.org/10.1108/IJBM-03-2024-0138

Van Bekkum, M., & Zuiderveen Borgesius, F. (2023). Using sensitive data to prevent discrimination by artificial intelligence: Does the GDPR need a new exception? *Computer Law & Security Review*, *48*, 105770. https://doi.org/10.1016/j.clsr.2022.105770.

Van Hoang, N. (2023). Human Expertise and Machine Learning in Collaborative Intelligence Frameworks for Robust Cybersecurity Solutions. *Journal of Applied Cybersecurity Analytics, Intelligence, and Decision-Making Systems*, *13*(12), 1-12. http://sciencespress.com/index.php/JACAIDMS/article/view/2023-12-04.

Varmaz, N. (2020). GDPR vs. Big data & AI in fintechs. *Vierteljahrshefte Zur Wirtschaftsforschung*, *89*(4), 55–72. https://doi.org/10.3790/vjh.89.4.55.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User Acceptance of Information Technology: Toward a unified view. *MIS Quarterly*, *27*(3), 425. https://doi.org/10.2307/30036540.

Vial, G., Crowe, J., & Mesana, P. (2024). Managing data privacy risk in advanced analytics: Cybersecurity techniques that keep personal data safe can limit its use for analytics -- but data scientists, data owners, and IT can partner more closely to find middle ground. *MIT Sloan Management Review*, *65*(4), 47–51.

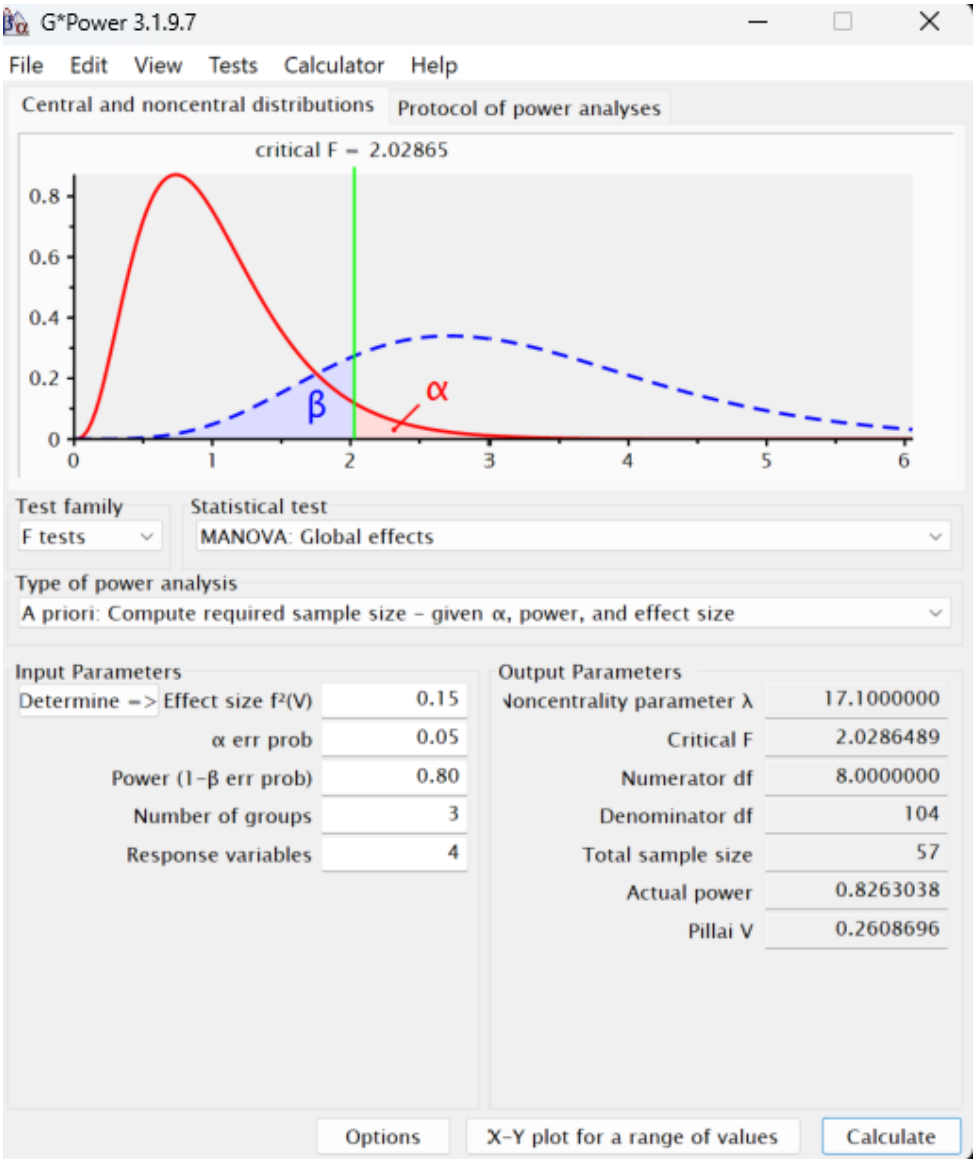
Yu, X., Xu, S., & Ashton, M. (2023). Antecedents and outcomes of artificial intelligence adoption and application in the workplace: The socio-technical system theory perspective. *Information Technology & People*, *36*(1), 454–474. https://doi.org/10.1108/ITP-04-2021-0254.

Zhong, J., Wang, X., & Zhang, T. (2024). Network Security Governance Policy and Risk Management: Research on Challenges and Coping Strategies. *Journal of Machine and Computing*, 153–169. https://doi.org/10.53759/7669/jmc202404015.

Zhou, X. (2023). Challenges and countermeasures of artificial intelligence technology in the application of financial industry. *Advances in Economics, Management and Political Sciences*, *63*(1), 77–82. https://doi.org/10.54254/2754-1169/63/20231382.

Appendix A

G*Power Calculations



Note. This G*Power analysis illustrates the a priori sample size calculation for a MANOVA global effects test, indicating that a minimum of 57 participants is required to achieve 80% power with a medium effect size ($f^2 = 0.15$), $\alpha = 0.05$, across three groups and four response variables.

Appendix B

Research Instrument

Scale: 1 = Very Dissatisfied, 2 = Dissatisfied, 3 = Slightly Dissatisfied, 4 = Neither Satisfied nor Dissatisfied, 5 = Slightly Satisfied, 6 = Satisfied, 7 = Very Satisfied

Research Question	Variable	Question	1	2	3	4	5	6	7
RQ1	Compatibility (IV)	The AI cybersecurity tools align well with our organization's security policies and frameworks.	[]	[]	[]	[]	[]	[]	[]
		Implementing AI-based cybersecurity tools does not require significant changes to our existing infrastructure.	[]	[]	[]	[]	[]	[]	[]
		The AI systems are compatible with our current data governance and privacy policies.	[]	[]	[]	[]	[]	[]	[]
		The AI tools support the regulatory compliance processes we already have in place.	[]	[]	[]	[]	[]	[]	[]
		Our IT systems easily integrate with the selected AI-driven cybersecurity platforms.	[]	[]	[]	[]	[]	[]	[]
	Implementation Success (DV)	Implementing AI-based cybersecurity tools in our institution was efficient and timely.	[]	[]	[]	[]	[]	[]	[]
		AI-driven systems have been successfully adopted across all relevant departments.	[]	[]	[]	[]	[]	[]	[]
		The implementation process of AI tools aligned with our strategic IT goals.	[]	[]	[]	[]	[]	[]	[]
	Regulatory Compliance and Data Privacy Protection (DV)	The AI cybersecurity tools help us meet regulatory requirements such as OCC, the Federal Reserve, NCUA, SEC, FIO, GDPR, CCPA, and PCI-DSS.	[]	[]	[]	[]	[]	[]	[]

		AI has enhanced our ability to protect sensitive financial and customer data.	[]	[]	[]	[]	[]	[]	[]
RQ2	Complexity (IV)	Our organization finds AI-driven cybersecurity tools difficult to configure and deploy.	[]	[]	[]	[]	[]	[]	[]
		The technical requirements of AI-based cybersecurity systems are overly complex.	[]	[]	[]	[]	[]	[]	[]
		Understanding how AI security tools function requires specialized expertise.	[]	[]	[]	[]	[]	[]	[]
		The learning curve associated with AI cybersecurity technologies is steep.	[]	[]	[]	[]	[]	[]	[]
		We often rely on external consultants or vendors to manage our AI-based security systems.	[]	[]	[]	[]	[]	[]	[]
	Adoption Challenges (DV)	The complexity of AI cybersecurity tools has delayed their full implementation in our organization.	[]	[]	[]	[]	[]	[]	[]
		Complexity has negatively impacted the overall success of AI tool adoption efforts.	[]	[]	[]	[]	[]	[]	[]
	Workforce Adaptation and Data Privacy Management (DVs)	Our cybersecurity staff finds it challenging to adapt to AI-enhanced tools	[]	[]	[]	[]	[]	[]	[]
		Training our staff to manage AI-driven cybersecurity technologies requires a significant amount of time and effort.	[]	[]	[]	[]	[]	[]	[]
		The complexity of AI systems makes it harder to ensure consistent data privacy practices.	[]	[]	[]	[]	[]	[]	[]
RQ3	Relative Advantage (IV)	AI-based cybersecurity tools offer clear benefits over traditional security methods.	[]	[]	[]	[]	[]	[]	[]

		Using AI-driven technologies significantly improves the speed of incident response.	[]	[]	[]	[]	[]	[]	[]
		AI tools provide enhanced accuracy in detecting sophisticated cyber threats.	[]	[]	[]	[]	[]	[]	[]
		Our organization experiences greater efficiency in cybersecurity operations due to AI.	[]	[]	[]	[]	[]	[]	[]
		The advantages of AI security systems justify their adoption despite associated costs or risks.	[]	[]	[]	[]	[]	[]	[]
	Threat Detection and Fraud Prevention (DVs)	The use of AI has enhanced the effectiveness of our fraud detection processes.	[]	[]	[]	[]	[]	[]	[]
		Real-time threat alerts generated by AI systems improve our incident response time.	[]	[]	[]	[]	[]	[]	[]
		AI-driven analytics help our institution identify malicious patterns that human analysts might miss.	[]	[]	[]	[]	[]	[]	[]
	Workforce Decision-Making Support (DV)	AI systems provide valuable insights that help analysts make informed security decisions.	[]	[]	[]	[]	[]	[]	[]
		AI helps prioritize threats, allowing cybersecurity staff to focus on critical issues.	[]	[]	[]	[]	[]	[]	[]
RQ4	Combined Impact on Regulatory Compliance	The collective influence of compatibility, complexity, and relative advantage affects our ability to meet cybersecurity regulatory standards.	[]	[]	[]	[]	[]	[]	[]
		Even with high complexity, the perceived benefits of AI justify its use in compliance-related functions.	[]	[]	[]	[]	[]	[]	[]
		Our organization's compliance posture has strengthened due to the	[]	[]	[]	[]	[]	[]	[]

		combined effects of well-matched, advantageous, and manageable AI systems.							
	Combined Impact on Fraud Prevention	AI tools that are compatible, easy to manage, and offer clear benefits have significantly improved fraud prevention.	[]	[]	[]	[]	[]	[]	[]
		Fraud prevention outcomes depend on balancing AI system complexity with ease of use.	[]	[]	[]	[]	[]	[]	[]
		When AI systems are beneficial and align with existing processes, fraud detection improves.	[]	[]	[]	[]	[]	[]	[]
		Our ability to prevent fraud improves when AI tools are not overly complex and integrate seamlessly.	[]	[]	[]	[]	[]	[]	[]
	Combined Impact on Workforce Augmentation / Human-AI Collaboration	When AI systems are too complex, it limits their usefulness to cybersecurity teams.	[]	[]	[]	[]	[]	[]	[]
		The perceived advantages of AI must be balanced with usability to support analyst decision-making.	[]	[]	[]	[]	[]	[]	[]
		Human-AI collaboration is most effective when AI tools are well-integrated, intuitive, and demonstrably beneficial.	[]	[]	[]	[]	[]	[]	[]

Appendix C Informed Consent

Hello,

My name is Tanya Stewart, and I am a doctoral student at National University. I am conducting an online survey to gain a deeper understanding of how financial institutions utilize AI-driven cybersecurity tools and how these tools impact areas such as compliance, fraud prevention, teamwork, and adaptability.

To participate, you must:

- Be age 18 or older.
- Be currently employed in the financial services sector within the United States
- Hold a professional role related to cybersecurity, information security, IT risk management, or related functions.
- Have experience or familiarity with AI-driven cybersecurity tools (e.g., machine learning-based threat detection, automated incident response, behavioral analytics).
- Have access to a computer or mobile device with an internet connection to complete the online survey.

The survey includes 40 Likert scale questions and will take about 30–40 minutes to complete. The survey will ask about:

- Demographic information (such as your role, years of experience, and sector).
- Your experiences and perceptions of AI-driven cybersecurity tools.
- Perceived compatibility, complexity, and relative advantage of these technologies.
- Organizational outcomes such as compliance, fraud prevention, teamwork with AI, and adaptability.

Your participation in this study is voluntary. If you decide to participate, your responses will be anonymous and recorded without any identifying information linked to you. No names, email addresses, or IP addresses will be collected.

If you have any questions about this study, please contact me at T.Stewart3770@o365.ncu.edu.

If you have any questions about your rights as a research participant, or if you wish to report a research-related problem, you may contact the National University IRB at irb@nu.edu.

By clicking the Next button and completing the survey, you indicate that you consent to participate in this research. If you do not want to participate, please close your browser.

[ ] I Agree (Continue to Survey)
[ ] I Do Not Agree (Exit Survey)