

1-22-2026

Strategies Financial Institutions Use to Mitigate Security Breaches for Mobile Customers

STEVEN F. KNESE
Walden University

Follow this and additional works at: <https://scholarworks.waldenu.edu/dissertations>

This Dissertation is brought to you for free and open access by the Walden Dissertations and Doctoral Studies Collection at ScholarWorks. It has been accepted for inclusion in Walden Dissertations and Doctoral Studies by an authorized administrator of ScholarWorks. For more information, please contact ScholarWorks@waldenu.edu.

Walden University

College of Management and Human Potential

This is to certify that the doctoral study by

Steven F. Knese

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee

Dr. Cheryl Waters, Committee Chairperson, Information Technology Faculty

Dr. Geraldine Light, Committee Member, Information Technology Faculty

Chief Academic Officer and Provost

Sue Subocz, Ph.D.

Walden University
2026

Abstract

Strategies Financial Institutions Use to Mitigate Security Breaches for Mobile Customers

by

Steven F. Knese

MSIT, Walden University, 2018

MSIS, Nova Southeastern University, 2015

MBA, Nova Southeastern University, 2009

BS, Florida International University, 2002

BA, Florida International University, 2002

Doctoral Project Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

March 2026

Abstract

Mobile fraud attack rates are increasing rapidly. Financial institutions, cybersecurity managers, and regulators need effective strategies to reduce consumer financial harm and operational risk. Grounded in the cybernetics model, this qualitative, pragmatic inquiry identified the cybersecurity strategies that cybersecurity professionals use at financial institutions to mitigate data breaches for mobile customers accessing financial data. Data were collected from five cybersecurity professionals through semistructured interviews and from publicly available documents and guidance issued by financial institutions and standards bodies. Six significant themes emerged from thematic analysis: implementing multifactor authentication, deploying virtual private networks (VPNs), delivering user education, promoting regular account monitoring, endorsing authentication apps, and enforcing strong password policies. A key recommendation is to integrate cybernetic principles into the design of multifactor authentication to enhance security protocols. The implications for positive social change include the potential for financial institutions and policymakers to implement the identified strategies to protect consumers' livelihoods and reduce operational and transactional risks.

Strategies Financial Institutions Use to Mitigate Security Breaches for Mobile Customers

by

Steven F. Knese

MSIT, Walden University, 2018

MSIS, Nova Southeastern University, 2015

MBA, Nova Southeastern University, 2009

BS, Florida International University, 2002

BA, Florida International University, 2002

Doctoral Project Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

March 2026

Dedication

I dedicate this doctoral project to the Father, Son, and Holy Spirit.

Acknowledgments

A very special thanks to my Chair, Dr. Cheryl Waters, who, without her help, my DIT completion would not have been possible. Finding participants was challenging, and Associate Deans from Broward College, Mitch McBee and Brian Faris, assisted in locating the interviewees. Special thanks to my teammates with whom I have developed a peer friendship, and for being here, I owe you both Dr. James Clapp and Dr. Vivian Lyon; without your encouragement, I could not have done this. I owe you both.

Table of Contents

List of Tables	v
List of Figures	vi
Section 1: Foundation of the Project.....	1
Background of the Problem	1
Problem Statement.....	2
Purpose Statement.....	2
Nature of the Project	3
Research Question	4
Conceptual Framework.....	4
Definition of Terms.....	6
Assumptions, Limitations, and Delimitations.....	7
Assumptions.....	7
Delimitations.....	8
Significance of the Project	9
Contribution to Information Technology Practice.....	9
Implications for Social Change.....	9
A Review of the Professional and Academic Literature.....	10
Overview of Academic Literature	10
Strategies Found in the Literature.....	12
Conceptual Design.....	17
Financial Transactions by Mobile Platforms Defined	27

Artificial Intelligence and Machine Learning Security	31
TPM, HSM, and Hardware Security.....	32
Blockchain	33
Completely Automated Public Turing Test to Tell Computers and Humans Apart	34
Consumer Awareness.....	37
Data Encryption	40
Dynamic Card Verification.....	42
Hypertext Transfer Protocol Secure, Transport Layer Security, and Domain Name System	43
Mobile Application Management, Enterprise Mobility Management, and Mobile Device Management.....	45
Multi-Factor Authentication and Two-Factor Authentication.....	46
Virtual Private Networks	48
App Development.....	50
Transition and Summary.....	51
Section 2: The Project.....	53
Purpose Statement.....	53
Role of the Researcher	53
Research Method and Design	56
Method	56
Research Design.....	58

Population and Sampling	60
Ethical Research.....	62
Data Collection	63
Instruments.....	63
Data Collection Technique	64
Data Organization Techniques.....	65
Data Analysis Technique	66
Reliability and Validity.....	68
Dependability	68
Credibility	69
Transferability.....	69
Confirmability.....	69
Transition and Summary.....	69
Section 3: Application to Professional Practice and Implications for Change	71
Overview of Project	71
Presentation of the Findings.....	72
Theme 1: Using Dual and Multifactor Authentication	75
Theme 1: Connection to Literature	77
Theme 2: Check Accounts Frequently.....	80
Theme 2: Connection to Literature	81
Theme 3: Authentication App.....	82
Theme 3: Connection to Literature	83

Theme 4: User Education.....	85
Theme 4: Connection to Literature.....	85
Theme 5: Applying a VPN.....	86
Theme 5: Connection to Literature.....	87
Theme 6: Strong Passwords.....	88
Theme 6: Connection to Literature.....	89
Applications to Professional Practice.....	90
Implications for Social Change.....	92
Recommendations for Action.....	93
Recommendations for Further Project.....	95
Reflections.....	96
References.....	99
Appendix A: NIH Certificate of Compliance.....	139
Appendix B: Interview Protocol.....	140

List of Tables

Table 1. Matrix of Literature Comparison 12

Table 2. Themes..... 75

List of Figures

Figure 1. Internet Crime Complaint Center Report (IC3)..... 76

Section 1: Foundation of the Project

Background of the Problem

As the adoption of mobile devices for transmitting financial information increases, so do the opportunities that cybercriminals can exploit. With over 90% of Americans owning a smartphone, financial transactions are increasing at an unprecedented rate (Gelles-Watnick, 2024). The growth of financial transactions amplifies the risk, with a global estimated cost of cybercrime in the cybersecurity market projected to surge to \$5.7 trillion by 2028 (Petrosyan, 2023). Identity theft is the fastest-growing type of crime in the United States and globally (Sobers, 2019). Users often blame identity theft on other authorities and do not accept responsibility for their own identity theft, thereby compounding a responsibility problem (Farrar et al., 2020).

Financial institutions identify common barriers to consumer adoption of mobile technology for financial transactions. Over 70% of mobile consumers are concerned about security strategies for mobile financial transactions, as 50% of all financial apps do not have security baked in (Federal Deposit Insurance Corporation, 2011). Financial centers recognize that the adoption of newer mobile cybersecurity technology, skill development, and deployment are essential to safeguard mobile financial transactions. Sixty-five percent of mobile payment users had used three or more payment types in the past month, compared with 45% of traditional payment users (Pew Research Center, 2019). This research examines the methods and tools employed by financial institutions to secure their networks for mobile financial transactions.

Problem Statement

For the fourth quarter of 2020, U.S. consumers predominantly completed their banking transactions through apps on devices more often than any other method (American Bankers Association, 2023). The House Subcommittee on Cybersecurity (2023) has estimated that malicious cyber activity costs the U.S. economy \$100 billion annually. The general information technology (IT) problem addressed in this project is the lack of security awareness for online financial transactions completed through mobile devices. The specific IT problem is that some cybersecurity professionals at financial institutions lack effective strategies for implementing cybersecurity measures to mitigate data breaches for their mobile customers who access financial data.

Purpose Statement

This qualitative, pragmatic inquiry identified the cybersecurity strategies that cybersecurity professionals use at financial institutions to mitigate data breaches for mobile customers accessing financial data. The studied population includes the websites of financial institutions, the U.S. government, and the National Institute of Standards and Technology (NIST), as well as publicly available websites governing mobile financial transactions and cybersecurity professionals' articles and websites. This project may benefit society by enabling the secure and easy transmission of mobile financial data, thereby protecting people's livelihoods and reducing operational and transactional risks. Identifying and implementing effective cybersecurity strategies can enhance the customer experience, promote responsible use, and mitigate the threat of cybercrime. Positive

social change may include customers who adopt mobile technology in greater numbers for financial data transmission, resulting in lower costs and fees.

Nature of the Project

I chose the qualitative pragmatic inquiry approach for this project, which involves a systematic examination of social phenomena in natural settings. Bhandari (2020b) states that qualitative research focuses on the circumstances that occur, answers questions about experience, provides meaning, and creates a perspective that informs the effects of those circumstances from the perspective of those involved. This project aimed to gain a deep understanding of the methods used by cybersecurity professionals to mitigate financial data breaches involving consumers and their use of mobile devices for banking purposes. Hypothesis tests in quantitative studies require statistical data from researchers who employ a quantitative approach to make decisions about observed effects (Mishra et al., 2019). Qualitative research is not designed for hypothesis testing, as that would involve converting qualitative data into categorical data that is measurable statistically (Chigbu, 2019). A mixed-method is suitable for a project that combines qualitative and quantitative approaches, noting that the project will not require numerical testing. I did not choose the mixed-methods approach because it is typically used in the behavioral, health, and social sciences, as well as multidisciplinary settings, for complex situational or societal research (George, 2021).

I used the qualitative pragmatic inquiry for this project. Pragmatic inquiry research studies provide a deep understanding, description, and explanation of the expert's perspective on what worked and how it relates to the phenomenon (Ramanadhan

et al., 2021). I employed a qualitative pragmatic inquiry to examine this real-world phenomenon, aiming to generate an in-depth understanding of the security protocols utilized by cybersecurity professionals within financial institutions. Ethnographic research involves distinct cultures or cultural groups (Singh, 2023). Ethnography was unsuitable for this study, as the research did not focus on a distinct culture or cultural group. Other qualitative research approaches include narrative, phenomenology, and case studies (Hoover, 2021). The narrative method explores an individual's life (Turnbull et al., 2023). The narrative method was considered inappropriate for this study, as the research does not seek to explore an individual's life. Phenomenology aims to understand a phenomenon and is particularly suitable for researching people's experiences (Picton et al., 2017). Phenomenology is not suitable for the project, as it is not concerned with explaining life experiences. Case studies are usually for a single instance.

Research Question

What security strategies do cybersecurity professionals at financial institutions use to mitigate data breaches for mobile customers who access financial data?

Conceptual Framework

Wiener (1961) established that cybernetics examines human-machine interaction by analyzing diverse systems through the principles of feedback, control, and communication. The conceptual model of cybernetics drives this research to observe the strategies employed by cybersecurity professionals in implementing security for financial transactions made by their mobile customers using mobile devices. Wiener (1961) defines cybernetics as an approach to exploring information security and cybersecurity,

as well as their overlap (Kushal & Arun, 2017). Cybernetics examines human-machine interaction through systematically analyzing feedback, control, and communication principles (Wiener, 1961). Cybernetics is a suitable conceptual model for understanding the key factors influencing cybersecurity professionals' mobile device cybersecurity strategies.

Cybernetics is used to understand the strategies of cybersecurity professionals to protect mobile financial transactions. Cybernetics encompasses eight key characteristics: feedback, threshold, energy, intelligent systems, human behavior and psychology, automata theory, game theory, and quantitative analysis (Kushal & Arun, 2017). Feedback, thresholds, and intelligent systems relate to communication between machines that utilize intelligent systems. Energy drives computing devices, information flow, and algorithms (Tataroiu et al., 2019). Threshold limits and mechanistic feedback provide the limitations on any system. Human behavior and psychology depict a training need. Automata theory is the communication between humans and the control of machines. The theory of games is closely related to engaging and interactive training experiences. Quantitative analysis is a quantifiable component.

This research explores strategies of cybersecurity professionals' strategies to mitigate the security risks associated with financial transactions conducted on mobile devices. The research employs the conceptual model of cybernetics to examine the factors affecting cybersecurity professionals' choices of strategies to mitigate security risks associated with emerging mobile technology used for financial services.

Definition of Terms

Completely Automated Public Turing Test To Tell Computers and Humans Apart (CAPTCHA) is an interactive feature added to web forms to differentiate the form used by humans and automated agents by entering the text from a distorted image or taken from an audio recording (NIST, 2020b).

Dynamic Card Verification. Authentication codes are uniquely generated and tailored for every credit card transaction (Secure Technology Alliance, 2020).

Denial of Services Attack (DOS). DOS prevents the availability of stored information (Xu et al., 2020a).

Enterprise Mobility Management. Management of physical controls for mobile devices, ensuring trusted mobile device networks, controlling content, and applications, has been introduced as enterprise mobility management (Franklin, 2019).

Mobile Application Management. Software development is responsible for provisioning and controlling access to mobile apps used in mobile financial transactions as part of mobile application management (Bunyakiati & Sammapun, 2019).

Mobile Device Management. Remote monitoring of mobile devices, permissions management, file management, and application management of mobile devices (Hayes et al., 2020).

Multi-Factor Authentication. The end-user inputs different authentication factors, including users' knowledge, possession of a token device, and inheritance; a biometric is a multi-factor authentication (Sharma, 2019).

Assumptions, Limitations, and Delimitations

Critical limitations often arise when conducting scholarly research. The deficiencies include, but are not limited to, the availability of resources, the interviewer's lack of skills for the reasoning process, and inherent failings. Clarification is necessary for the three categories of phenomena: assumptions, limitations, and delimitations.

Assumptions

Two primary philosophical assumptions exist: ontology and epistemology (Burrell & Morgan, 1979). Ontology refers to our assumptions about how we perceive the world, and epistemology is the study of the correct way to understand the world (Bhattacharjee, 2012). Psychologists believe that social reality is conceptualized from both objective and subjective perspectives. The assumptions underpinning this project have been recognized and explicitly articulated. The first assumption is that the websites of cybersecurity financial institutions, cybersecurity professionals, the U.S. government, and NIST's publicly available websites governing mobile financial transactions reveal that two-factor and multifactor authentication lowers the risk of financial transmission breaches. The second assumption I am operating under is that the cybersecurity personnel of financial institutions are highly trained and well-versed in data breaches. The third assumption is to employ a pragmatic approach in analyzing qualitative data, which will provide the necessary information to answer the research question. The fourth assumption is that individual websites' interpretations might illuminate the research direction. NCapture, a web browser extension compatible with Google Chrome, facilitates the systematic collection of online content for subsequent importation into NVivo 15, a

leading software platform for qualitative data analysis. This project was underpinned by both objective and subjective paradigmatic assumptions, acknowledging the epistemological value of each framework in interpreting social reality. I employed the most recent iteration of NVivo 15 to support a rigorous thematic analysis of the collected data. NVivo 15 offers advanced analytical tools that enable researchers to interrogate qualitative datasets with greater depth and precision. The analytical process remained grounded in thematic analysis, allowing for the identification, analysis, and interpretation of patterns of meaning within the data. I implemented strategies to minimize methodological constraints, restrictions, defects, and shortcomings, reducing study limitations. However, limitations are inevitable in every project (Busse et al., 2016). Using a qualitative approach in this project presents the first primary limitation. A limitation is that the data sources may limit the findings in the research due to issues with credibility, transferability, dependability, and conformability (Nowell et al., 2017).

Delimitations

Delimitations are boundaries or limitations that a researcher establishes to ensure the project's aims and objectives are achievable (Theofanidis & Fountouki, 2019). This research has six delimitations. First, I researched large financial institutions that offer mobile access to financial data. Second, cybersecurity professionals who have the authority to implement mobile security measures. Third, I considered only cybersecurity professionals with at least three years of experience in mobile cybersecurity. Fourth, only cybersecurity professionals who conduct mobile financial security measures were considered. Fifth, only the websites of large financial institutions, the U.S. government,

and NIST's publicly available websites that govern mobile financial transactions were reviewed.

Significance of the Project

Contribution to Information Technology Practice

Similar research on mobile information security using the conceptual cybernetics model also exists. Given the lack of published literature, this additional research on strategies used by cybersecurity professionals to mitigate security breaches on mobile devices using cybernetics may enhance IT security practice. This project may lead to further research on security methodologies for mobile devices, drawing on the principles of cybernetics. This multidisciplinary approach encompasses control, system, and information theories.

Implications for Social Change

Mobile devices are rapidly changing the day-to-day business activities of global business and financial organizations. Mobile devices are poised to replace traditional financial operations and processes (Damen, 2021). Financial institutions enhance consumer value by providing mobile security and threat management solutions. The Pew Research Center (2021) stated 97% of Americans own cell phones. Wi-Fi hotspots in coffee shops, libraries, airports, hotels, universities, and other public places are convenient. However, often, they are not secure (Federal Trade Commission, 2021a). Positive social change may result from the security strategies developed by this project, enabling cybersecurity professionals at financial institutions to implement best practices that protect their mobile customers' financial transactions while on Wi-Fi hotspots in

various public places, such as coffee shops, libraries, airports, hotels, universities, and other public venues, which may decrease fraud.

Information security awareness procedures and policies developed for this project regarding mobile financial transactions may provide an additional layer of security for individuals using public networks. Mobile financial consumers and financial institutions may experience social change through cost savings, as the convenience of mobile financial transactions attracts customers in higher numbers, thereby mitigating mobile security concerns. Financial centers and consumers who utilize mobile technology in financial transactions can save time and transportation costs, reduce the need for employees to complete transactions, and contribute to the “green theme” by minimizing paperwork (Pazarbasioglu et al., 2020).

A Review of the Professional and Academic Literature

Overview of Academic Literature

This literature review provides a framework of financial cybersecurity advancements completed using mobile devices. Recently, cybersecurity research has expanded to include financial transactions facilitated by mobile technology. A literature review identifies peer-reviewed literature that utilizes various cybersecurity methodologies involving mobile devices to transmit financial data. This pragmatic inquiry examines the security strategies employed by cybersecurity professionals at financial institutions to mitigate financial security breaches affecting their mobile customers. The literature review focuses on the cybersecurity measures to protect mobile financial transactions.

This project explores the current strategies employed by cybersecurity professionals within financial institutions, with a particular focus on banking institutions, to provide illustrative examples. Some of the current strategies are CAPTCHA used to differentiate between real users and automated users, data encryption which translates data into another form that requires a key, dynamic card verification, which replaces a card verification value (CVV), hypertext transfer protocol secure (HTTPS) is a continuation of HTTP with a secure communication, Transport layer security (TLS) is a cryptographic protocol designed to provide secure network communication, Mobile application management (MAM) controls end-user use of an enterprise IT application, enterprise mobility management (EMM) secures enterprise and employee own devices, mobile device management (MDM) is mobile device management, multi-factor authentication (MFA) requires two or more authentication methods, and two-factor authentication (2FA) is a two-step verification, and virtual private networks (VPNs) protects private data transmitted over a public network.

This project contains references from 269 informational articles, peer-reviewed journal articles, and conference proceedings. Table 1 provides the matrix for literature comparison. The primary research libraries and databases include the Walden University Library, ACM Digital Library, Pew Research Center, EBSCOhost (Computers, Applied Science & Technology), IEEE Computer Society Digital Library, ScienceDirect, Google Scholar, NIST, and ProQuest Computing. The peer-review status of articles was verified using Ulrich's Global Serials Directory and individual journal websites. I reviewed 282 articles for this project, of which 217 are citations in the literature review. Of the 278

articles, 236 (84%) were peer-reviewed, and 233 (83%) were published within five years of my anticipated 2025 graduation date. I selected keywords to align with the research question and enhance search engine optimization. Keywords include cybercrime, Mobile Financial Technology (MFT), mobile financial transactions, and mobile financial technology. CAPTCHA, data encryption, dynamic card verification, hypertext transfer protocol, secure multi-factor authentication, and VPNs. The search strategy utilized keywords, key phrases, and an organized structure, combined with keywords relevant to my research question.

Table 1

Matrix of Literature Comparison

Reference data	Total number
Total references	282
Total peer-references references	260
Total non-peer-reviewed references	22
Seminal sources	33
Conference papers	6
Total published within five years of publication	233
Total published outside of five years from publication	26
Total percentage of peer-reviewed source material	92%
Total percentage of material published within five years	92%
Total percentage published within five years and peer-reviewed	92%

Strategies Found in the Literature

The literature review is a piece of discursive prose, not a list that describes or summarizes each literature review (Simon Fraser University, 2022). The organizing principle is thematic around a specific topic or issue (University of West Florida, 2021). The issue is an IT problem that some cybersecurity professionals at financial institutions

lack effective strategies to implement cybersecurity measures that mitigate data breaches for their mobile customers who access financial data.

This pragmatic inquiry aims to identify the cybersecurity strategies cybersecurity professionals use at financial institutions to mitigate data breaches for mobile customers who access financial data (Ramanadhan et al., 2021). Some of the themed strategies sought are creating a secure cyber ecosystem, defining an assurance framework, utilizing open standards, enhancing the regulatory framework, developing mechanisms for IT security, leveraging E-governance services, and protecting critical information infrastructure (TutorialsPoint, 2022).

Creating a secure cyber-ecosystem involves multiple devices from various entities (Bederna & Rajnai, 2022). The leading players included governmental agencies, private organizations specializing in cybersecurity, and other private entities (U.S. Department of Homeland Security, 2019). One strategy is maintaining a solid cyber-ecosystem where cyber devices depend on each other for automated security decision-making, mitigating cybersecurity risks, reducing attacks, and quick recovery from a cybersecurity attack (Cybersecurity & Infrastructure Security Agency [CISA], 2022). Other monitoring techniques from software products may supervise the cyber-ecosystem (U.S. Department of Defense, 2022). A symbiotic relationship, which denotes a mutually beneficial one, involves three key structures: automation, interoperability, and authentication (CISA, 2019). Automation will facilitate the installation of advanced security measures, expedite cybersecurity processes, and enable swift, informed cybersecurity decisions (NIST, 2020a). Interoperability galvanizes collaborative actions, increases awareness, and

involves artificial intelligence (AI) learning (Kaspersky, 2020). Authentication procedures enhance the identification and verification technologies that deliver heightened security, increased affordability, ease of implementation, and use for administration, scalability, and interoperability (ISC2, 2023).

The assurance framework objectively reviews the evidence, independently assessing the organization's governance, risk management, and control processes (The University of the Sunshine Coast, 2022). Defining and creating an assurance framework involves outlining global compliance standards, which traditional products, proven processes involving credentialed personnel, and the latest technological standards provide (Utah State University, 2022). The Cybersecurity Assurance Framework provides national security requirements (The White House, 2021). The framework involves critical infrastructure organizations and the requirements governing actions (The White House, 2021).

Open Standards involve interoperability and data exchange among various products and services intended for adoption by a wide range of users (U. S. Department of Defense, 2020). Open standards play a vital role in the information security approach, including diverse geographical regions and managing societal regulations (Winters, 2019). Open standards enhance key processes, integrate multiple systems with controls, provide an environment for users to evaluate new products and services, facilitate the adoption of new technologies or business models, facilitate understanding of complexities, and promote economic growth (U.S. Department of Education, 2017). Open standards enable security network developers to meet requirements while providing

visual details of the testing process and outcomes. The primary objective of cybersecurity open standards is to enhance the security of IT systems, networks, and critical infrastructures for the secure transmission of data (Hill, 2022). Security technology for the financial industry, which relies heavily on online financial transactions, has not kept pace with the rapid development of IT systems and data. It exposes users to online vulnerabilities (Tse, 2022). Open security standards provide an environment for sharing knowledge, best practices, and a common understanding of concepts, terms, and definitions (Richardson, 2024).

Enhancing and strengthening the regulatory framework secures a cyberspace ecosystem and strengthens the regulatory framework (Peters, 2022). Regulatory frameworks encompass local, state, national, and international legal devices (Dinapoli, 2021). They can be mandatory and involve laws and regulations. They may also be voluntary, as evidenced by the issuance of codes of conduct. Securing a regulatory framework promotes research and development, enhances human resources through education and training, encourages organizations to promote a chief information security officer (CISO), and effectively implements partnerships (Raza, 2020). The elements of a regulatory framework are technical standards, economic regulation, quality of service, environmental regulation, contractual agreements, licensing, regulatory processes, and standardization (USAID, 2021). Maintaining compliance by utilizing open sources of information related to the regulatory framework can help an entity mitigate security breaches and data loss risks.

Developing mechanisms for IT security includes technical tools and techniques to implement security services (Wadhwa, 2023). A mechanism may act alone or in conjunction with other symbiotic controls to provide a secure environment for a particular service. IT security mechanisms incorporate symbiotic controls, end-to-end security measures, and data encryption protocols (Zheng et al., 2021). Link-oriented measures deliver security between nodes. End-to-end is a medium that transports protected protocol data units from source to destination. Association-oriented measures modified sets of end-to-end measures. Data encryption may include ciphers and public-key ciphers, which encode information to be decoded by authorized personnel (Simplilearn, 2020).

Securing E-Governance Services is using the web to deliver public information and services (Zakrzewska & Miciuła, 2021). E-governance applications empower citizens and businesses to conduct online transactions that might otherwise require a visit to a physical office. There are four primary types of e-governance: government-to-government, government-to-citizen, government-to-business, and government-to-employee (D'Agostino et al., 2019). E-government services enable businesses and citizens to find the necessary information or service. E-government services are transacted through data encryption in transmission, applying detection mechanisms, and authenticating users.

Critical Information Infrastructure Protection (CIIP) refers to the assets, systems, and functions essential for maintaining business operations. One of the CIIP sectors is

related to banking and finance. The threats to CIIP are massive, involving attacks from ubiquitous sources (The World Bank, 2021).

Conceptual Design

Cybernetics examines human-machine interaction by analyzing systems using feedback, control, and communication principles (Wiener, 1961). The conceptual model of cybernetics drives this research to observe the strategies employed by cybersecurity professionals in implementing security for financial transactions made by their mobile customers using mobile devices. Cybernetics is an approach to exploring information security perspectives (Wiener, 1961; see also Kushal & Arun, 2017). Cybernetics constitutes the systematic study of human-machine interaction, grounded in the premise that researchers analyze varied systems by examining feedback loops, control architectures, and communication protocols (Wiener, 1961). Cybernetics is a suitable conceptual model for understanding the key factors influencing cybersecurity professionals' mobile device cybersecurity strategies.

Cybernetics is used to understand the strategies employed to protect mobile financial transactions. Cybernetics comprises eight characteristics: feedback, threshold, energy, intelligent systems, human behavior and psychology, automata theory, the theory of games, and quant analysis (Kushal & Arun, 2017). Feedback, thresholds, and intelligent systems relate to communication between machines that utilize intelligent systems. Energy drives computing devices, information flow, and algorithms (Tataroiu et al., 2019). Threshold limits and mechanistic feedback provide the limitations on any system. Human behavior and psychology depict a training need. Automata theory is the

communication between humans and the control of machines. The theory of games is closely related to engaging and interactive training experiences. Quant analysis is a technique using mathematical and statistical methods.

This research examines the strategies employed by cybersecurity professionals to mitigate the security risks associated with financial transactions conducted on mobile devices. It examines the strategies these professionals employ to mitigate these risks. The research employs the conceptual cybernetics model to examine the factors that affect the strategies of cybersecurity professionals in mitigating security risks associated with emerging mobile technology used in financial services.

Development and Features of Cybernetics

Anaxagoras of Clazomenae was an influential Presocratic natural philosopher and scientist who lived and taught in Athens, Greece. A form-matter dualism variant in cybernetics emerged from Anaxagoras, who lived from 500 to 428 B.C.E. (Patzia, n.d.). Socrates, Plato, and Aristotle examined the work of Anaxagoras, seeking to uncover an efficient cause rather than a purpose-driven explanation. Norbert Wiener, the founder of cybernetics, employed dualism to demonstrate that information constitutes a distinct reality from matter and energy (Wiener, 1961). Wiener proposed the theoretical foundations for cybernetics, or control and communication, which involves controlling the flow of information in systems with feedback loops.

Some information security subfields are cryptography, information leakage, intrusion detection, information flow security, digital forensic analysis, and information security for networks and mobile devices (Jain, 2021). Users may have prevented failures

in information security and project outcomes by applying cybernetic principles when implementing information security mechanisms or projects. (Kushal & Arun, 2017). Computer networks provide the backbone for financial centers, healthcare, governments, public infrastructure, and other industries; cybersecurity has emerged as a significant research area for academia, industry, and government. Cybernetics originates from the Greek words *kybernetes* and *kybernetikos*, which describe a steering device capable of steering or guiding human governance (Britannica, 2021). Cybernetics encompasses and is not limited to AI, learning, adaptation, cognition, convergence, social control, efficacy, efficiency, connectivity, and communication (Mitra, 2019). Cybernetics, developed by Wiener in 1948, can be considered a relatively recent science of control. Cybernetics is similar to the science of organization. A characteristic of cybernetics is evident in the construction of models. Cybernetic models are hierarchical and adaptive to feedback models (Balleine & Dezfouli, 2019). Cybernetics is involved in the processing and control of information. A key concept in cybernetics is feedback, as complex systems adapt to environmental factors through feedback (Jakubik, 2021). Wiener (1948) explores dynamic systems and how feedback influences behavior. Control theory is a system's output generated by a control stimulus, with the output measured (Peng et al., 2022). The control system comprises two components: the control object and the controller (Peng et al., 2022).

Cybernetics is a control theory that compares the actual state of a system with a prescribed standard. Wiener (1948) defined cybernetics as the project of information and control in animals and machines. Cybernetics deals with how things behave, rather than

with the things themselves, by asking what a thing does and what it can do. We can understand computer systems through the lens of cybernetics. Cybernetics crosses many disciplines. Cybernetics has enabled some disciplinary concepts to emerge and has helped us understand them. “Cyber” is short for cybernetics and relates to computerized systems, security, and IT security through cybersecurity, cyberattacks, and cyber threats (Li & Liu, 2021). With the rise and popularization of online transactions, mobile devices, and intelligent systems, cybersecurity has become a crucial aspect of modern financial institutions' security (McLennan, 2022).

Cybercriminals scan networks, develop exploits, and attack systems. At the same time, cybersecurity professionals detect the attacks, analyze exploits, and continue to patch systems. Defenders may not proactively address some exploits, leaving system vulnerabilities unpatched. Developing cybersecurity may be based on cybernetics using control theory, systems theory, and information theory applied to regulatory security systems to develop online security systems (Yan, 2022). Cybernetics shows how principles and protocols unify systems. Cybernetics regards systems as complex, multidimensional networks of information systems. In the future, cybernetic systems that think will distinguish open systems that exchange information with other intelligent environmental networks. Cybernetics may provide a consistent paradigm for the development of AI.

Cybernetic epistemology is concerned with addressing philosophical issues related to computational knowledge representation (American Psychological Association, 2018). Cybernetic epistemology is entirely observer-dependent (Alicea et al. 2020).

Information Warfare is the context of cybernetics using complexity theory to analyze discovery (Bindas, 2020). Information Warfare is destructive against information assets, systems, computers, and networks that support power grids, communications, financial transactions, and transportation systems (Lewis, n.d.).

Advantages of Cybernetics

Cybernetics may ground corporate governance. Various cybernetics are employed in communication channels, decision-making, and control tools, providing strategies for overcoming human variations and the limitations of complex management (Umpleby et al., 2019). Cybernetics enables us to view a company as a standalone system and analyze how organizational units influence decision-making processes in-depth. Control and regulation are inherent to any successful organization. A cybernetic management approach, known as a “hard systems approach,” can self-regulate, maintain a steady state, and retrieve information (CEOpedia, 2019). Cybernetics aids in stability when disruptions threaten machines, software, organisms, and organizations (Popa, 2022). Cybernetics may be considered a universal language and framework that is understood by scientists and designers from diverse disciplines, facilitating effective communication. Discovering a connection between cybernetics and information security may be used to circumvent the complex research challenges in information security (Kushal & Arun, 2017).

Cybernetics steers, governs, and navigates various disciplines toward their desired goals. Cybernetics has existed for over seventy years, beginning with the development of automation and control in electrical and mechanical systems and extending to biological,

social, and learning systems (Chepin, 2021). This qualitative project employed cybernetics, a framework grounded in constructivist principles. Constructivism involves engaging, exploring, explaining, elaborating, and evaluating. Cybernetics is a transdisciplinary approach to observing regulatory systems. This approach provides feedback with the outcomes used as inputs for further action. Cybernetics for the Doctorate of Information Technology (DIT) interviewing process examined the technological controls of security systems that protect mobile financial data transactions. Cybernetics studies the controls of any system that employs technology (Loshkarev, 2021).

Disadvantages of Cybernetics

Many professionals associate cybernetics with computers and robotics, overlooking the fact that cybernetics may be informed by a general theory of information and regulation that openly challenges the ontology established by modern science (Umpleby et al., 2019). Another disadvantage of not supporting fundamentals in Cybernetic research is that essential ideas evolve, and researchers must address them. Cybernetic science lacks educational programs in universities.

Cybersecurity is more reactive than proactive for the transmission of financial data over mobile devices. A limitation in current cybersecurity research is its reactive and application-based nature (August, 2021). Cybernetics' disadvantages include circumventing bounded rationality in decision-making, obtaining accurate information, and using control to manage complexity (Bardin & Ferrari, 2022). Control mechanisms include a standard of goals obtained through feedback to identify performance variations.

Although in use since the era of Plato's Greece, cybernetics is helpful for IT studies. A disadvantage is that some professionals lack understanding of the recent application of cybernetics in information gathering (Mayer, 2021). Communication between humans and machines, as well as between machines, may not fit all situated cybernetics (Kushal & Arun, 2017). Cybernetics research receives little support from government agencies or the private sector (Umpleby et al., 2019).

Justification for Cybernetics in This Project

A cybernetic session gathers information quickly and effectively, and organizers can easily arrange it for interviewees. Cybernetics' range of uses includes identifying needs for management information, developing policies, and managing financial resources (Bell et al., 2021). Random thoughts generate concepts that may be meaningful. The interviewees felt inclusion, which leads to higher involvement. The Cybernetic Approach is relatively new, providing an environment for mutual understanding. Interviewers may come to the point directly because of cybernetics. Interpersonal social mechanisms are rigid, whereas the Cybernetic Approach allows for sharing more ideas. Security professionals should incorporate the philosophy of cybernetics into efforts to mitigate vulnerabilities in computing systems. Experts define information security as a mechanism that protects information and maintains the relationships between the two. Researchers have found that information security and cybernetics share a strong bond, which can help solve some of the complex research challenges in information security. Deploying the information security mechanism creates a relationship between information security and cybernetics (Kushal & Arun, 2017).

Information security protects information and the order of relations between two entities, requiring security checks to be performed along with the transaction. An order of relationships involves information security that checks the information from the first entity and then allows the flow to the second entity. An end-user demonstrates authentication by entering a username and password, after which the system directs them to a multifactor authenticator to complete the secure transaction. Wiener (1961) proposed the theory of the game in cybernetics. A user entering a password demonstrates game theory and illustrates how users communicate with machines. The machine displays whether the password was correct or incorrect. If the password is correct, the machine displays the contents of what the user wants, demonstrating communication between the machine and another machine. Game theory is widely used in information security (Kushal & Arun, 2017). Security researchers can apply Wiener's (1961) cybernetic philosophy to address research challenges.

Application of Cybernetics in Previous Studies

Peña-Ayala and Cárdenas-Robledo (2019) defined a proactive and reactive mechanism applied in U-Learning settings, a cybernetic method to regulate learning through learning strategies. Research grounded in cybernetics is applied in psychotherapy and family therapy (Umpleby et al., 2019). Reflexivity theory examines the data collection and interpretation process, a component of cybernetics that may be beneficial to government regulators managing economic systems. Scholars and practitioners apply theories of information, regulation, and cybernetic management to understand and operate knowledge-based economies. Social scientists Schweizer and Lazurko (2020)

introduced Cross-Impact Balances which is a quasi-qualitative method of cross-impact balances that allows for a potential bridge between social scientific applications. Kastberg (2020) studied communication. Müller (2018) explores the shift from It-Science to Bit-Science through the framework of second-order science and new cybernetics. The transformation from It-Science to Bit-Science was a dual revolution in complexity and reflexivity, bringing about fundamental changes in scientific production processes, reconfiguring the architecture of science, introducing new research designs, and identifying complex patterns that intersect with societal and natural sciences. Grevtseva et al. (2019) published “The Cybernetic Approach as the Digital Competence of the Future Electronics Engineers.” This work acknowledges that digital competence is an integral component of the professional competence content in cybernetic pedagogy. Tamir (2020) published “Effortful Emotion Regulation as a Unique Form of Cybernetic Control.” The project involved cybernetic and feedback control processes in self-regulating behaviors. Apter (1970) published “Cybernetics: A Case Project Of A Scientific Subject-Complex.” Apter (1970) asserted that cybernetics could also be a contributing source to some other discipline. Apter (1970) also stated that subject specialists naturally use tactics that mirror cybernetics.

Supporting Conceptual Models

Mayr and Thalheim (2021) state that modeling or reasoning with models is a basic human capacity for coping with and understanding complex phenomena. Cybernetics is concerned with modeling. Donevski and Zia (2022) developed the cybernetic model of self-control by postulating that the context of self-control occurs

within a test–operate–test–exit (TOTE) loop. Individuals enter TOTE loops when they establish goals. The first action test evaluates the current state and the future goal state. Individuals need to take action to close the achievement gap. When the individual attains the goal, they exit the TOTE loop. Individuals perceive a positive effect as a movement towards a goal, contrasted with an adverse effect as a movement away from a goal. Rosenkranz and Holten (2007) published “Combining Cybernetics and Conceptual Modeling: The Concept of Variety in Organizational Engineering.” Combining cybernetic theories with conceptual modeling promotes the analysis and design of information systems by employing conceptual models that may contribute to organizational paradigms. Rosenkranz and Holten (2007) published “Combining Cybernetics and Conceptual Modeling: The Concept of Variety in Organizational Engineering.” Rosenkranz and Holten suggest that combining cybernetic theories with conceptual modeling may be necessary to analyze and design information systems, thereby achieving alignment between business and IT. Schwaninger (2003) published “A Cybernetic Model to Enhance Organizational Intelligence,” which focused on modeling organizational cognitive processes. Kovalchuk et al. (2022) published “Three-stage intelligent support of clinical decision making for higher trust, validity, and explainability,” which outlines the building of decision support systems (DSSs) using data-driven (DD) predictive modeling. Management science models have increased in decision support systems (DSS) involving individuals and cybernetics.

Contrasting Conceptual Models

Rezk and Gamal (2020) presented models and theories on effective schooling. Rational control theory, contingency theory, public choice theory, and retroactive planning are key theories that explain educational effectiveness. A fifth theoretical perspective is chaos theory. The following principles are theory-embedded: proactive structuring, fit, market mechanisms, the cybernetic principle, and self-organization. The Cybernetic principle contrasts with the Cybernetic loop's assessment, feedback, and corrective action. Thumbadoo and Taylor (2021) contrast cybernetics, which uses a feedback loop with other forms of reasoning, learning, cognition, adaptation, emergence, communication, and efficiency. Circularity is a systemic entity organized as a discrete set of components whose functional interrelationships are related (American Society for Cybernetics, n.d.). Panagia (2021) stated that cybernetics contrasted circularity by demonstrating that negative feedback loops regulate control systems. Cybernetics contrasts with other methods that deal with complex systems. Cybernetics is relevant in projecting complex systems as constantly evolving loops (Geckeler, 2020). Conventional science is concerned with projecting parts, reductionism, which explains the whole. Cybernetics differs from conventional science in that it focuses on goal-directed behavior.

Financial Transactions by Mobile Platforms Defined

Cybercrime targeting individuals who use mobile devices for financial data transactions has reached unprecedented levels, with anticipated growth primarily driven by escalating cybersecurity threats. Cybercriminals utilize various computational devices

to execute illicit transactions for financial gain. There is disagreement on whether mobile financial transaction data can be adequately protected (Ali, 2019). Cybercrimes include, but are not limited to, identity theft, phishing, vishing, denial-of-service (DOS) attacks, malware, hacking, social engineering, automating online banking fraud, and exploiting mobile phones and other electronic gadgets, as well as social networks and the emergence of electronic media platforms (Ali, 2019). The Security.org Team (2023) found that 65% of credit and credit card holders have been victims of fraud at some point in their lives, up from 58% the previous year. Security.org Team (2023) states that fraud affects about 151 million Americans. A project by Gomes et al. (2020) states that only 50% of respondents can differentiate between a trusted and an untrusted email. Social engineering is one of the most significant challenges to network security for mobile transactions, as it exploits the natural human tendency to trust (Salahdine & Kaabouch, 2019). Mobile users represent a significant risk increase due to the rapid spread of mobile devices.

The rapid spread of mobile devices, including smartphones, tablets, laptops, and other portable devices that offer computing technology, has accelerated mobile financial transactions. A 2020 study by researchers in Australia found that 84% of the population used mobile technology to access the Internet, with 79% accessing the Internet multiple times a day (Kaviani et al., 2020). Mobile platform adoption in 2017 and 2018 encompassed over 2 billion Android mobile devices and 1.3 billion iOS mobile devices, which operate on various smartphones, tablets, and other mobile devices (Soh & Grover, 2020). Android malware poses a significant threat to the information security of mobile

financial transactions, as mobile users are often unaware that they are granting permission for malware infections (Chakravarty & Varma, 2020). Each financial institution governs what features an app performs and what unique services it offers to protect the mobile user. Most mobile financial apps offer features such as checking account balances, processing electronic payments, facilitating remote check deposits, transferring funds, and downloading electronic financial statements (Karjaluo et al., 2019). The system may hack devices that run Android, bypass Samsung's secure boot mechanism, and jeopardize financial transactions (Claudinei Morin et al., 2020).

Mobile banking involves making financial transactions on any mobile electronic device. Mobile banking financial transactions can range from as simple as checking balances to as complex as account administration. Mobile banking refers to the provision of financial services, including conducting bank and stock market transactions, managing accounts, and accessing customized financial information (American Bankers Association, 2023). Convenience, safety, reliability, efficiency, and responsiveness were key factors in the adoption of mobile financial transactions completed through apps (Zhao & Bacao, 2021). Many financial institutions have been offering mobile banking (m-banking) as customer adoption shifts from the traditional pc to smartphones, tablets, and mobile apps (Shevlin, 2021). Consumers have demanded mobile financial services that provide them with control over their finances, access to money, convenience, affordability, security, customer service, and long-term financial management tailored to their specific needs (Ullah et al., 2022). Real-time alerts give consumers control over

their finances, providing awareness of money deposited and withdrawn from their accounts.

Financial providers offer quick access to funds, allowing consumers to pay bills and make purchases. Using mobile financial transactions is convenient, as it saves consumers time and effort (Marginingsih et al., 2019). Mobile financial transactions have reduced costs for consumers and financial institutions, making transactions affordable (Marginingsih et al., 2019). Consumers look for and expect long-term financial management and demand advice on money management, such as spending reports and other tools to help them attain their financial goals (Marginingsih et al., 2019). Financial center customers are demanding protection for their financial transactions using mobile technology. Consumers want security to protect against the electronic theft of monetary funds and professional information (Chuang et al., 2020). With the rapid adoption of mobile devices, financial transactions are becoming increasingly challenging to secure, as strategies to ensure data protection and privacy are being compromised (Zeybek et al., 2019). Mobile phones are the most widely used mobile devices for transacting financial information. At the same time, the security systems vary widely, protecting those financial transactions (Zeybek et al., 2019). Mobile device threats are on the rise and can lead to data loss, security breaches, and regulatory compliance violations (Awan, 2023). Device protection involves physically securing the device in a safe environment to prevent theft. Mobile device infrastructure encompasses the execution of mobile apps on mobile operating systems and the utilization of wireless transmission systems.

More than 87% of the U.S. population now owns a mobile phone, and over half of them have smartphones (FDIC, 2012). Consumers are increasingly relying on mobile devices (FDIC, 2022). Accepting mobile devices is a top priority for many organizations because research shows that increased mobility helps enterprises improve operations and productivity; however, this adoption also increases security threats (Gontovnikas, 2021). Reducing threat areas to protect mobile financial transactions includes AI, trusted platform module (TPM), blockchain, CAPTCHA tests to tell computers and humans apart, consumer awareness through training, data encryption, dynamic card verification, HTTPS, MAM, MFA, physical security, secure socket layer (SSL), security token device, and VPNs.

Artificial Intelligence and Machine Learning Security

A Cybint project revealed that human error is the primary cause of 95% of cybersecurity breaches, and 88% of organizations experience phishing attacks (Drexel University, 2021). AI and data analytics work together and are distinct, with applications in project operations and computer fields. AI's cybersecurity role is to secure company assets and protect user data. AI employs machine learning and deep learning to comprehend network behavior and structure identifiable patterns (Atske, 2023). The advantages of integrating AI with cybersecurity include threat detection, bot blocking, breach prediction, and endpoint protection (Drexel University, 2021). AI's threat detection is paramount to a security countermeasure, providing a security measure against cyberattacks (CISOMAG, 2020). AI can potentially mitigate the escalating number of destructive bot attacks on e-commerce sites through the use of supervised and

unsupervised machine learning algorithms (Columbus, 2020). AI security-based systems can predict how and where enterprises are most likely to be breached, providing a framework for implementing security resources and allocating security tools toward areas of vulnerability (Goodman, 2019). AI security-enabled endpoint solutions can track and continuously monitor all endpoint activities, identifying each electronic transaction as either malicious or approved (Young, 2021).

Zion Market Research (2019) predicts that the global cybersecurity market's AI segment was USD 7.1 billion in 2018 and is expected to reach approximately USD 30.9 billion by 2025, at a compound annual growth rate of slightly above 23.4% between 2019 and 2025. Researchers categorize AI in the cybersecurity market based on its offering, security, technology, security solutions, and end-user. The market encompasses hardware (including processors, memory, and network components), software (such as AI platforms and AI solutions), and services.

TPM, HSM, and Hardware Security

Using hardware-enabled security features can elevate cybersecurity to a new level by enabling centralized control, identifying machine entities, covering all states of information at rest, in transit, and in use, as well as utilizing random access memory, the software development lifecycle, and machine identity deployment in DevOps processes (Bartock et al., 2022). Centralized management of machines reduces the complexity of implementing a policy across devices and workloads. Trusted Platform Module (TPM) provides hardware-based, security-related functions. It is a secure cryptographic processor that performs cryptographic operations. The TPM has physical or embedded

security technology installed on a computer's motherboard or processor, generating and storing parts of PC encryption keys (Intel, 2021). The chip includes embedded physical security, making it tamper-resistant, and malicious software cannot affect the security functions of the TPM (Microsoft, 2022). A TPM is a tamper-resistant integrated circuit built into newer computer motherboards that can perform cryptographic operations to provide sensitive information, such as passwords and cryptographic keys (Trusted Computing Group, 2022).

Hardware security modules (HSMs) are hardware devices that can be integrated into a computer's motherboard. However, manufacturers build more advanced models into the hardware chassis as external devices that users can access via the network. The HSM generates a key and sends data to an HSM for encryption, decryption, or cryptographic signing. If the system detects tampering, it destroys the key (Kontesoy, 2022). Cryptographic key management systems (CKMS) are hardware, software, or firmware that function as approved cryptography (Barker & Barker, 2019).

Blockchain

Blockchains are tamper-evident and tamper-resistant digital ledgers of transactions that are replicated and spread across a network of computer systems. These systems record transactions in a shared ledger within the network, where no transaction can be changed once it has been published. (Rodeck, 2021). Many nodes must verify and confirm the integrity of new data before a new block can be added to the ledger, allowing nodes to solve complex mathematical equations to process decentralized transactions (Rodeck, 2021). Multiple nodes must verify blockchain transactions to ensure integrity,

thereby reducing data storage errors. A malicious actor perpetrating an attack must hack every node that stores the information, which is nearly impossible (Rodeck, 2021).

Blockchain security technology is a leading innovation in security for the finance industry, aiming to reduce fraud, facilitate quick and secure transactions and trades, and support risk management within the interconnected global financial system (Zaid Almahirah, 2021). Blockchain technology encompasses decentralization, high confidence, and tamper resistance, which maintain an advantage through reduced resource consumption, improved scalability, the absence of central authority, and enhanced trust (Hu, 2022).

Completely Automated Public Turing Test to Tell Computers and Humans Apart

CAPTCHA is the first line of defense in preventing unauthorized web bots from accessing web-based services (Hitaj et al., 2021). HTTPS is required as an additional layer of security when transmitting financial data. Websites not optimized for HTTPS will experience difficulties incorporating innovative, web-based platform security measures. If organizations do not use HTTPS, they will struggle to implement security as the internet continues to evolve. Attackers use computer programs to attack websites, while CAPTCHAs provide preventive measures to mitigate the attacks (Wang et al., 2021). The different categories of CAPTCHA are text, audio, video, and image based. The Text CAPTCHA is designed and implemented quickly, requiring users to recognize and submit the correct characters from an array of distorted characters masked in grids and background noise.

In contrast, the audio CAPTCHA portion, which requires users to submit the correct characters as audio CAPTCHA over a noisy background, is typically used in conjunction with other CAPTCHAs for the visually impaired (Arnott, 2023). Developers have recently developed Video CAPTCHA, which requires users to watch and correctly answer questions about the content (Arnott, 2023). Lastly, image-based CAPTCHAs require users to select parts of an image based on the question asked about the image (Arnott, 2023). CAPTCHA utilizes these categories to determine whether the user is a human or a computer. CAPTCHA development requires automated computer programs that generate and grade tests, are made public through an openness disclosure, provide an environment that allows users to solve tests quickly, and offer security by using program-generated tests that are difficult for computers to solve (Arnott, 2023). Malicious actors can defeat any CAPTCHA, including audio, text, video, or image-based formats, by employing low-cost human labor to solve it. CAPTCHA is a program that distinguishes between machine and human input. CAPTCHA is among the most common methods of authentication used by websites and web services (Alqahtani & Alsulaiman, 2020). CAPTCHA maintained an accuracy of 85.32% and solved 56.29% of reCAPTCHA. This advanced risk analysis engine initially presented additional challenges (Alqahtani & Alsulaiman, 2020). CAPTCHA protects search engine databases and prevents attackers from exploiting their sensitive data. OCR uses image-processing algorithms to recognize readable characters from optical data (Bodkhe, 2021). Advances in optical character recognition (OCR), image-processing algorithms, and text-based CAPTCHA cannot guarantee authentication (Alqahtani & Alsulaiman, 2020). Vicarious, a developing AI,

solved modern CAPTCHA using character recognition with nearly 90% accuracy (Bodkhe, 2021).

An additional format for CAPTCHA is reCAPTCHA, which requires users to enter letters from distorted images for authentication within the reCAPTCHA interface. The reCAPTCHA interface serves two purposes: to protect websites from bots and digitized text (Xu et al., 2020b). The reCAPTCHA is not immune to AI and OCR, posing significant threats to reCAPTCHA (Bodkhe, 2021). Although more complex text distortion can make CAPTCHA and reCAPTCHA difficult for machine hacking, it also makes the text more difficult for users to read.

Cloud security can be enhanced using Generating panOptic Turing Tests to Tell Computers and Humans Apart (GOTCHA), a recently developed image-based CAPTCHA that utilizes image labeling and recall for authentication. Fighting ubiquitous automated attacks on users' data and privacy involves distinguishing between humans and computers, authenticating a human user, and identifying computerized attacks (Dinh & Ogiela, 2022). CAPTCHAs require users to identify and match images with custom labeling options. Attackers can defeat image-based CAPTCHA using content-based image retrieval and annotation techniques. All CAPTCHA and reCAPTCHA systems rely on the Turing test. The Turing test refers to the ability of machines to deceive people into thinking that computers are human (Frankenfield, 2023). Security teams combine CAPTCHA and reCAPTCHA with other strategies to prevent the loss of financial information and fortify privacy. Involving GOTCHA interaction is a powerful tool in computer security.

Consumer Awareness

Employees and consumers represent a massive cybersecurity threat. The human user is the weakest link in any cybersecurity strategy (Legrand, 2022). Employees and consumers are responsible for 46% of cybersecurity incidents worldwide (Kaspersky Lab, 2017). Employees and consumers often conceal cybersecurity breaches. Forty-five percent of companies (over 1,000 employees) have experienced employees who hid cybersecurity incidents (Kaspersky Lab, 2017). A Kaspersky Lab (2017) survey found that uninformed or careless employees and consumers are the most likely cause of cybersecurity breaches. Human errors have substantially impacted IT security, increasing the likelihood of cybersecurity breaches (Legrand, 2022). Investigations of security breaches have revealed a substantial impact of human errors, leading to data breaches (Yadav, 2023).

Users write down passwords, hide the notes under the mouse pad, turn off security on their computers, give out passwords through socially engineered tricks, and access non-essential data for job requirements. Cybersecurity concerns for businesses include that 47% of employees and users have shared inappropriate data on their mobile devices, 46% have misplaced their handheld devices, and 44% have accessed inappropriate IT resources (Kaspersky Lab, 2017). Cybercriminals are aware that they can exploit human users by employing social science and psychological techniques to gain access through phishing emails, weak passwords, and fake tech support calls (Li et al., 2019). Phishing fraud is becoming the most popular cybercrime (Athulya & Praveen, 2020). IBM (2019) reported that 19% of the cybersecurity attacks involved the finance

and insurance industries. Some industries are particularly lucrative to cybercriminals, offering financial services such as bank account information and payment card data, which can be quickly monetized using cryptocurrency through the Dark Web (Hai Thanh Luong, 2023). Cybercriminals recognize that bank networks can rapidly transfer large sums of money into accounts controlled by criminals and may sell personally identifiable information (PII) on the dark web for a profit (Zaharia, 2019). To help address this problem, Elifoglu et al. (2018) have called for a better understanding of user behavioral theories to educate users on protecting mobile devices while transacting financial data.

The most widely used behavioral theories are general deterrence theory, the theory of planned behavior, protection motivation theory, social bond theory, and social learning theory. General deterrence theory examines the likelihood of organizations punishing users who fail to follow established security policies. The security action cycle, embedded within the general deterrence theory, serves as a model for addressing user security violations. The model comprises four stages: deterrence, prevention, detection, and remedies. Deterrence includes policies, guidelines, and awareness programs. Prevention occurs when deterrence fails, and organizations accomplish it through physical or procedural controls. Detection mechanisms address computer abuse by the user. Organizations implement remedies when they detect and deal with user computer abuse by employing policies and rules (Elifoglu et al., 2018).

A second relevant theory, the Theory of Planned Behavior, posits that a user's intentions can predict their behavior. A user's attitude, behavior, social factors, and control factors mainly affect the theory of planned behavior. Before a user adopts positive

behavior, they must be motivated to comply through a favorable appraisal (Substance Abuse and Mental Health Services Administration [SAMHSA], 2019). Users' perception of a legitimate policy will aid in the users' acceptance of policy compliance. The protection motivation theory refers to the users' motivation in response to threat and coping appraisal (SAMHSA, 2019). The coping appraisal includes self-efficacy, response efficacy, and response cost (Shillair, 2020). Self-efficacy is the user's ability to avert a potential loss. Response efficacy is the users' compliance with the policy. Response cost refers to the users' perceived opportunity costs, including monetary, time, and effort costs. The social bond theory is a common field of criminology, suggesting that strong bonds among users will lessen computer abuse. The Social Learning Theory posits that perceptions among user groups are influenced by their associations' actions and beliefs (Western Governors University, 2020). Users who hold negative perceptions of the industry are less likely to accept the correct policies and existing security measures (Western Governors University, 2020).

Information security is a top concern for CEOs. Educating users to be compliant when transmitting financial data on mobile devices strikes a balance between ease of use and effective policies. There are numerous challenges to teaching users about compliance with security strategies when transacting financial data over mobile devices. The end-users are often unaware of strong passwords, are not using MFA, fall for phishing scams, share passwords, lose their mobile devices, ignore system updates, turn off anti-virus, and use old software that is not supported (Kassner, 2020). Providing consumers with an easy-to-follow security training program is key to acceptance. One cybersecurity strategy

may be built into a financial app that encrypts financial data, thereby protecting financial transmission without requiring user involvement in security training.

Data Encryption

Data encryption translates the original computer code into a different form of code. The data is encrypted and sent to the source computer through an encryption key. As the receiving computer uses a decryption key, it reveals the original computer code. Data encryption is one of the most successful and powerful tools for organizations to transmit data securely (Lord, 2019). Data encryption uses encryption algorithms, playing a valuable role in protecting digital data. The algorithms provide confidentiality, authentication, integrity, and non-repudiation. Confidentiality protects data against unintentional, unauthorized, and unlawful access, including information privacy. Authentication of data is a process of confirming its integrity. Data authentication involves receiving data from a verified source that is accurate and correct. Integrity ensures the authenticity of the information, which has not been altered and comes from a known, verified source. Non-repudiation is the assurance that the entity or person who sent the data cannot deny sending that data. The U.S. Department of Commerce's NIST, in collaboration with the Advanced Encryption Standard (AES), has resulted in a \$250 billion economic impact over the last 20 years (NIST, 2020b). AES specifies a cryptographic algorithm to be used for data protection.

The AES algorithm is an asymmetric block cipher that encrypts data into ciphertext and then decrypts it, converting it back to the original data, known as plaintext (NIST, 2020a). Data encryption protects the privacy of communication between a

browser and servers. A secure session uses Transport Layer Security (TLS) Encryption protocol. The TLS protocol requires public and private keys. The browser and server know keys, which are randomly chosen numbers. Systems distribute keys to the browser, which uses the numbers to encrypt messages transmitted wirelessly or by wire to the server, which holds the keys for decryption. A padlock icon in the browser window indicates that the site is in secure mode.

The Gramm-Leach-Bliley Act, enacted in the United States, requires financial institutions, including banks, securities firms, insurance companies, and other financial service providers, to protect the integrity and security of their customers' data. The financial service provider is subject to significant criminal and civil penalties for breaches of consumer financial information. Any financial institution that processes financial data must encrypt all data transfers, protect against anticipated threats, and adhere to established standards and best practices to safeguard consumer data (Crane, 2019). The Gramm-Leach-Bliley Act requires financial institutions to protect non-public personal information (NPI) and to communicate how they share NPI with customers clearly. The Gramm-Leach-Bliley Act also requires financial institutions to protect non-public personal information (NPI) and inform customers how they share NPI. The Privacy of Consumer Financial Information regulation requires financial institutions to implement and maintain a comprehensive information security program. The IT control objectives of the Sarbanes-Oxley Act require financial institutions and other companies to determine whether encryption controls are necessary to protect the confidentiality of data transmitted over the Internet (Silent Circle, 2019).

The states have laws governing the transmission and encryption of protected data. Many states have laws requiring a secure connection or the encryption of Social Security numbers during transmission. The measure of an appropriate level of protection is the Card Industry Data Security Standard (PCI DSS) (Sulistyowati et al., 2020). The PCI DSS is a security standard developed by Visa, MasterCard, American Express, Discover, and JCB to ensure the safe transmission of financial data. The Payment Card Industry Security Standards Council (PCI SSC) manages PCI DSS. This independent body oversees financial data for credit card companies. All companies that store, process, and transmit cardholder financial data implement PCI DSS (PCI Compliance Guide, 2020). The PCI DSS is an independent body that regulates standards for participating credit card companies, constantly evolving and responding to new security threats.

Dynamic Card Verification

Dynamic card verification replaces a static CVV with a new CVV number generated at regular intervals. Manufacturers designed a dynamic card verification system with an electronic ink display powered by a thin lithium battery, generating a new CVV number at regular intervals that consumers can customize (Segal, 2019). Counterfeit card fraud had declined by 80% at brick-and-mortar stores, prompting thieves to shift their focus to online fraud for financial transactions (Segal, 2019). In 2016, Idemia introduced dynamic CVV Motion Code-enabled credit and debit cards, which display a changing e-ink number on the back of the card according to a Visa-supplied algorithm (Segal, 2019). Past tests by Idemia, which utilized over 600,000 cards and

processed more than 4 million transactions across 10 international locations, yielded no card-not-present fraud (Huffman, 2020).

Newer dynamic CVV cards create a new code periodically, unlike usual ones that maintain a static code. Some problems with the new dynamic CVV cards, which change the number too frequently, include the possibility that a customer might not complete an online transaction, potentially placing a faster drain on the lithium battery and resulting in the added expense of the new card. Cost is a significant variable, as a chip card costs \$2 to \$4 compared to a dynamic CVV card, priced at around \$15 (Segal, 2019). The new dynamic CVV cards support Visa and Mastercard and refresh automatically, freeing users from other tasks. The dynamic CVV card integrates with a mobile and server solution that aligns with this project. Credit card thieves are shifting to online fraud; dynamic CVVs are one more successful security measure in financial data transactions involving a credit card.

Hypertext Transfer Protocol Secure, Transport Layer Security, and Domain Name System

HyperText Transfer Protocol Secure (HTTPS) extends HTTP, and users widely employ it for secure communication over computer networks. Cybercriminals may develop effective ways to mitigate HTTPS data transfer in an encrypted format from the server. HTTPS is vulnerable to DigiNotar's breach, Apple's #gotofail, and OpenSSL's Heartbleed. Many security technologists are working to address the security issues with HTTPS. HTTPS transfers data from the server in an encrypted format and establishes an encrypted link between the web browser and a web server using TLS. TLS establishes an

encrypted link between the browser and the server, or between the server and the server, or between the client and the server. TLS ensures that the information in transit stays private and secure. The security provided includes website authentication and protection of transmitted data's privacy and integrity. It thwarts man-in-the-middle attacks and protects against eavesdropping and tampering with the transferred text. HTTPS is HTTP sent over TLS, using a TLS certificate, a digital certificate that provides encryption. HTTPS's main advantages are secure communication, data integrity, privacy and security, fast performance, search engine optimization (SEO), and safe future transmission (Crowe, 2020). The use of HTTPS is increasing, protecting many websites, securing accounts, safeguarding identities, and maintaining web browsing privacy.

HTTPS is a secure version of the HTTP protocol, which replaces HTTP's Secure Socket Layer with TLS for encryption and authentication. The RFC2818 digital certificate certification, or HTTP over TLS, specifies HTTPS (Russell, 2020). Eavesdroppers may be able to access IP addresses, port numbers, domain names, the amount of data sent, and the session duration, and the data remains encrypted by TLS (Russell, 2020). The encryption encompasses the request URL, website content, query parameters, headers, and cookies, ensuring that any financial transaction involving credit card numbers, banking information, and social security numbers remains secure. Organizations commonly use HTTPS and TLS with other security strategies.

The DNS protocol has been used for over thirty years (Bumanglag & Kettani, 2020). DNS is an essential method for resolving domain names into Internet Protocol (IP) addresses. The protocol lacks built-in security mechanisms to address confidentiality,

integrity, or availability, the CIA Triad. Malware may use the DNS to complete the attacker's objectives and establish command and control. The latest security enhancement for DNS is the use of HTTPS. HTTPS is a more modern approach to protecting transmitted data through browsing software.

Mobile Application Management, Enterprise Mobility Management, and Mobile Device Management

Mobile Application Management (MAM) controls devices, while Mobile Device Management (MDM) focuses on securing specific applications on mobile devices. These management techniques may be necessary due to the explosion of mobile technology. MAM is the software and services necessary for provisioning and controlling access to proprietary mobile apps. MDM is proprietary software that enables IT administrators to manage, secure, and enforce policies for smartphones and mobile devices. EMM is significant for security by using people, processes, and technology to manage mobile devices, wireless networks, and other mobile computing services. EMM is a system that prevents unauthorized access to enterprise applications, such as those offered by financial institutions. The security offered by EMM is password protection, encryption, and wipe technology, or the ability to have the device remotely wiped of all data (Rouse, 2019). Users expect mobile devices to operate efficiently and have high security levels, which drives the mobile market.

The concept of Bring Your Own Devices (BYOD) is driving MDM. MDM is a security solution that monitors, manages, and secures mobile devices, including laptops, smartphones, and tablets (Batool & Masood, 2020). The mobile operating system

developers and mobile device manufacturers control MDM. MDM features include device inventory and tracking, app distribution, remote wipe, password enforcement, app whitelisting and blacklisting, and data encryption. Device inventory and tracking can occur in real-time and may be automated.

Additionally, the business entity controls the distribution of the app to trusted users. The remote wipe is a security measure that allows a network administrator to remotely erase all data from a lost or stolen mobile device. Additionally, password enforcement is a set of rules that users must follow for IT security purposes. Additionally, app whitelisting specifies a list of approved software applications that users can install on their mobile devices.

Blacklisting is a network administration technique used to prevent the installation of unwanted apps or programs (Iwuozor, 2021). Whitelisting and blacklisting deter the installation of malware (Proctor, 2021).

Multi-Factor Authentication and Two-Factor Authentication

Passwords are a form of single-factor authentication and are not enough to secure mobile devices for mobile transactions (Cybersecurity and Infrastructure Security Agency, 2020). To help increase security, IT security teams require MFA and 2FA for mobile financial transactions. MFA mandates users to verify their identities by providing multiple pieces of evidence to access a device, website, or application (Alqahtani et al., 2020). The authentication factors may include knowledge, possession, and inheritance. Knowledge authentication involves information that only the user knows, such as passwords or answers to questions. Possession authentication is when the user supplies an

item, such as a one-time password or a YubiKey (a hardware authentication device). Finally, an individual's biometric authentication, such as a fingerprint, retina scan, or voice, is unique. MFA uses two or three of the previously listed authentication factors, whereas 2FA uses only two. The Payment Card Industry Data Security Standard (PCI DSS) no longer accepts 2FA, only MFA (Lebeaux, 2023). Organizations need at least two authentication factors to be PCI compliant.

Although end-users often prefer single-factor authentication (SFA) for its simplicity and user-friendliness, attackers exploit SFA, the weakest form of authentication, to compromise users' accounts. In contrast, MFA increases security because even if one credential becomes compromised, unauthorized users cannot meet the second authentication requirement (CISA, 2022). End users, the financial clients of various financial institutions, will not use tedious and slow authentication. The end users may find quick workarounds for the three authentication factors. Users have demonstrated the workarounds by writing password notes and placing them under keyboards (LaConte, 2019).

The three authentication factors are possession, knowledge, and inherence. Financial institutions may employ these factors in multifactor transaction authentication (Cybersecurity and Infrastructure Security Agency, 2022b). Authentication is a crucial safeguard that prevents unauthorized access and protects sensitive financial information (Cybersecurity and Infrastructure Security Agency, 2022a). Although MFA and 2FA are effective ways to protect financial transactions, requiring an MFA policy within an organization can reduce security threats to financial data by 99.9% (Sharp, 2019). MFA

or 2FA is an effective way to protect financial transactions (Maciej et al., 2019). End-users may perceive MFA as difficult or inconvenient. Many different authentication methods exist, differing in protection and cost. A new standard is on the horizon. This new standard is known as the Fast Identity Online (FIDO) alliance, which has developed FIDO2 (Noor, 2020). The Fast IDentity Online alliance includes the U.S. government, Australia, Germany, and the World Wide Web Consortium (W3C).

Virtual Private Networks

A VPN provides a secure connection method, adding security and privacy when using public and private networks, such as Wi-Fi and the internet (Federal Trade Commission, 2021b). VPNs hide IP addresses, change IP addresses, encrypt data transfers, mask locations, and provide access to blocked sites (Crawshaw, 2021). Connecting to a VPN conceals the actual IP address, providing anonymity. VPNs provide a different IP address that observers cannot trace back to the user's actual location. Further, a VPN will protect data by encrypting data transfers while using public Wi-Fi. Users can select any country of origin for their IP address. Because some countries may block websites while users are traveling there, a VPN typically allows access to all blocked sites. Governments worldwide experienced a 1,885% increase in ransomware attacks, and the healthcare industry saw a 755% increase in such attacks in 2021 (Taylor, 2022). One of the security solutions for mobile financial data transactions is an IP-based Virtual Private Network (IPVPN). The primary objective of a VPN is to establish a secure network tunnel on the public internet using encryption technology, which enables the transmission of data securely and prevents others from intercepting packets.

VPNs are essential for device security, as simple methods exist to intercept data transfers, such as Wi-Fi spoofing and Firesheep. Wi-Fi spoofing is counterfeiting an access point, tricking the user into connecting through a hacker's hotspot (Jiang et al., 2020). A Man-in-the-Middle attack allows a cybercriminal to intercept another user's Internet connection, retrieving all information transmitted, including passwords and financial data. The hacker may sign onto the user's financial site with all access privileges. Firesheep, an extension for the Firefox browser, utilized a packet sniffer to intercept unencrypted session cookies, revealing sensitive information. To help mitigate these kinds of attacks, Mobile Virtual Private Network (mVPM) performs better on a wireless network as VPN apps encrypt, or scramble, the data sent between (Federal Trade Commission, 2021a).

VPN encryption encodes data so that another computer with the correct decoder can read it. An encryption key is used to encrypt and decrypt data. Computers make a tunnel between Internet connections that can be encrypted. VPNs do more than encrypt and decrypt data. A site-to-site VPN uses Internet Protocol Security Protocol (IPSec) or Generic Routing Encapsulation (GRE). Using a VPN in VPN Tunneling Mode ensures the VPN encrypts the data during transmission. However, this secure method is not enough to prevent hacks (Karaymeh et al., 2019). The public Internet, wireless or wired, is not secure. Therefore, a VPN establishes a secure, private, internal network over an insecure public network. VPNs must utilize strong cryptography, such as the Internet Security Association and Key Management Protocol (ISAKMP) or the Internet Key Exchange (IKE) policy (National Security Agency, 2020).

Application Development

Building and deploying popular financial institution apps for mobile devices requires supporting various operating environments and portable computing devices such as smartphones or tablets. Mobile users comprise 97% of US adults who use applications to fulfill their different needs (Pew Research Center, 2024). Many mobile devices and their operating environments expose apps to intrinsic vulnerabilities; however, increased protection can mitigate them. Many financial institutions recognize mobile customized apps' ease of use and security power that address individual operating systems' vulnerabilities (Shahriar et al., 2020) Mobile banking apps can be used anywhere a network connection exists and offer 24/7 services: viewing balances, viewing recent transactions, making bill payments, transferring funds, contacting customer service, opening new accounts, and reordering checks. The use of customized mobile apps to access financial data offers improved security. Financial centers may leverage the security development in any customized mobile app. Mobile banking apps appeal to financial centers for cost savings and increased security while offering consumers a wide range of services that can be accessed quickly (Hossain Shahriar et al., 2020). Consumer adoption using mobile apps offers cost savings that are ten times cheaper than ATM transactions (Samojło, 2019).

Requiring clients of financial institutions to access and transmit financial data through a customized app with built-in security measures enhances security. Financial institutions enhance app security through MFA, use of Near Field Communication (NFC), employing end-to-end encryption, use of biometrics, real-time text and email

alerts, use of paperless banking, utilize behavior analysis, safe digitized documentation, and usage of secure access (Ozkan & Bicakci, 2020). Financial companies are transitioning from a reactive security discipline to a predictive and proactive approach by developing custom apps. Managed security services in financial apps have MFA built into custom mobile apps that do not store data, thereby limiting the risk of viruses on mobile devices (McCue, 2019).

Transition and Summary

This section includes a background and review of the literature regarding security, privacy, and reliability strategies for secure access to financial data. This review categorically organizes security techniques that secure the transmission of financial data. The search strategy included research libraries and databases, as well as the Walden University Library, ACM Digital Library, Pew Research Center, EBSCOhost (Computers, Applied Science & Technology), IEEE Computer Society Digital Library, ScienceDirect, Google Scholar, NIST, and ProQuest Computing. The literature focused on four key areas: (a) the two characteristics of cybernetics, extrinsic dimension and vulnerability, (b) security strategies, and (c) vulnerabilities.

The focus was on CAPTCHA, consumer awareness, data encryption, dynamic card verification, HTTPS, MAM, MFA, physical security, SSL, security token device, and VPNs. Cybersecurity professionals at financial institutions use security strategies to mitigate security breaches for their mobile customers. More security strategies are currently under development.

The literature review section aims to provide insight into financial transactions conducted over mobile devices, highlighting the lack of security policies among financial organizations. The research methodology appears to be disconnected from the coherence of research approaches that protect mobile financial transactions. Furthermore, the literature review highlights the adoption of security measures that help mitigate security breaches for their mobile customers. To successfully implement mobile financial transaction security, cybersecurity professionals must reduce security threat vectors to the institution and provide a proven security plan that governs mobile financial transactions.

The literature review focuses on using the general deterrence theory. General deterrence theory examines the likelihood that organizations will punish users for failing to adhere to established security policies. The security action cycle, embedded within the general deterrence theory, serves as a model for addressing user security violations. The model comprises four stages: deterrence, prevention, detection, and remedies. Deterrence comprises policies, guidelines, and awareness programs. However, prevention is most effective when deterrence fails, and physical or procedural controls can help mitigate security risks. Detection mechanisms address computer abuse by the user. Organizations implement remedies when they detect and deal with user computer abuse by employing policies and rules. Section 2 of the proposal identifies the role of the researcher and the active participants. Section 2 also highlights the research methods, the intended design, and the data collection method.

Section 2: The Project

Purpose Statement

This qualitative pragmatic inquiry aims to identify the cybersecurity strategies cybersecurity professionals use at financial institutions to mitigate data breaches for mobile customers who access financial data.

This project may benefit society by enabling the easy and secure transmission of mobile financial data, protecting people's livelihoods, and reducing operational and transactional risks. Identifying and implementing effective cybersecurity strategies can enhance the customer experience, promote responsible use, and help mitigate the threat of cybercrime. Positive social change may include customers who adopt mobile technology in greater numbers for financial data transmission, resulting in lower costs and fees.

Role of the Researcher

As the sole researcher for my project, I am the primary source of data collection. Institutional Review Board approval was obtained for this research project under protocol number 04-04-23-0599888. Yin (1981) stated that qualitative research requires the researcher to collect primary data. The final report requires data collection from all sources that informed the project. The sources that informed the project were participants and Internet sources. Researchers mitigated personal bias during data collection to prevent data corruption.

I am familiar with the topic, having covered numerous classes on cybersecurity at the master's level. My bank account was seriously compromised twice without any loss of funds, and I worked closely with my financial institution to mitigate both security breaches. With

professional experience, having taken classes on security at the master's level, and teaching cybersecurity tactics in the classroom at the undergraduate level, I have a logical basis for conducting the project. No personal or business relationships exist with the participants of the project. The most challenging aspect of data collection is that the sources of evidential support are relevant, and the researcher must be knowledgeable about their relevance (Yin, 1981). A protocol governs data collection, encompassing topics to explore, the minimum amount of data to collect, types of interviewees, types of documents to analyze, observations to make, and relevant evidence (Yin, 1981). I have no relationship with any participants and have not met them prior.

Congress established the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research to address issues related to the protection of human subjects in research (American Psychological Association, 2023). Ethical research, defined by the *Belmont Report*, requires adherence to all federal laws and regulations, a research project approved by an Institutional Review Board (IRB), protection of personally identifiable information, regulated scholarly and journalistic activities regarding the collection of personal information, and compliance assertion (Nagai et al., 2022). The seven guiding principles for ethical research are social and clinical value, scientific validity, fair subject selection, favorable risk-benefit ratio, independent review, informed consent, and respect for the subjects (Nagai et al., 2022).

I adhered to the seven principles by treating all human participants equally, fairly, and without harm, with respect to the interviewees' rights, before, during, and after conducting my project, staying within the confines of the *Belmont Report*. I have completed the National Institute of Health (NIH) Office of Extramural Research web-based training

course on protecting human research participants (see certificate in Appendix A). The researchers informed all participants that their names and identities would be kept anonymous. All participants were shown an informed consent form and were briefed not to disclose information obtained during the interviewing process, thereby maintaining participant confidentiality and further protecting their identities.

Bias affects ethical research and significantly influences project outcomes (Yin, 1981). Bias is a deviation or trend from the truth in data collection, analysis, interpretation, and publication, which can lead to misleading conclusions (Popovic & Huecker, 2024). I am using the conceptual model of cybernetics for this project. Cybernetics was employed as a conceptual model to elucidate the key factors that influence mobile device cybersecurity strategies employed by cybersecurity professionals. A conceptual framework that utilizes multiple dimensions of the case-theory relation facilitates researchers' navigation process, revealing relationships between the case and project (Luft et al., 2022). I took necessary measures to avoid bias in my case project. I used NCapture, a web browser extension for Chrome, which enables the gathering of web content to import into NVivo 15, facilitating qualitative data analysis. NVivo 15, the latest edition, provides tools to ask questions about the collected data. Data analysis would still involve a thematic analysis. I collected data from the websites of financial institutions, the U.S. government, and NIST's publicly available websites that govern mobile financial transactions. Data collection also involved publications by cybersecurity professionals on websites and/or in articles.

Research Method and Design

Method

Researchers conducting research studies employ one of three research methods (Galauner, 2021). These methods include (a) qualitative analysis, (b) quantitative analysis, and (c) mixed methods research. Qualitative research involves collecting, organizing, and interpreting transcriptions from notes and recordings (Bhandari, 2020b). I am employing a qualitative, pragmatic inquiry for this research, which focuses on collecting primary and secondary data, corroborating public documents, websites, and artifacts (Wickham, 2019). I researched the in-depth understanding, description, and explanation of the expert's perspective on what works and how it relates to the phenomenon of cybersecurity implemented to mitigate data breaches for mobile customers accessing financial data (Streefkerk, 2019). Qualitative analysis has improved rigor, and qualitative data reviewers expect researchers to have addressed negative issues from the start of the research project (Johnson et al., 2020). Implementing qualitative pragmatic inquiry for this research project is appropriate, as it allows the study to focus on real-world experiences (Kaushik & Walsh, 2019). One of the strengths of qualitative research is its ability to explain processes and patterns of evidence-based phenomena (Holtrop & Glasgow, 2020). Pragmatic inquiry research studies aim to answer questions focused on an in-depth understanding, description, and explanation of what works and how it relates to the phenomenon of interest (Wagenaar et al., 2022). Qualitative pragmatic inquiry may involve qualified business professionals from one's professional

or social networks, social media, government websites, and referrals from qualified participants (Harris, n.d.).

The goal of this project is not to test a hypothesis or work with variables. Quantitative methods utilize objective measurements and mathematical, statistical, or numerical data analysis collected through questionnaires, surveys, and polls (Bhandari, 2020c). Researchers may manipulate the quantitative data involving pre-existing statistical data (Williams, 2021). The structure for quantitative design follows the scientific method, which uses deductive reasoning to formulate a hypothesis (Rutgers University Libraries, 2021). The quantitative methodology was inappropriate for my research, as my goal was not to examine differences or relationships among variables or formulate and test hypotheses.

The quantitative research method did not meet this project's goals. Understanding the participants' experiences may enhance the interpretation of the research findings (Bhandari, 2020a). Qualitative researchers aim to understand the lived experiences of participants from their own perspectives (Pfeifer & Dolan, 2023). This project aims to understand the experiences and profound insights into the phenomenon of cybersecurity professionals.

Mixed-methods research combines qualitative and quantitative research methods within a single project. Mixed methods research advances the integration, or "mixing," of quantitative and qualitative data within a single case project or sustained inquiry program (George, 2023). The project did not fit a mixed-methods approach. Implementing a mixed methods research project combines methodologies that have been seen as

problematic, as quantitative and qualitative methodologies belong to separate and incompatible models (Vedel et al., 2019).

Research Design

The Qualitative Pragmatic Inquiry approach uses new data to formulate an understanding of a problem. It provides the means to address that problem (Morgan & Nica, 2020). Cybersecurity systems are complex, and history has taught us that cybersecurity complexity will continue to increase. Pragmatic approaches to qualitative analysis can be valuable for information security researchers, as they enable the strategic gathering of research through qualitative analysis (Ramanadhan et al., 2021). Pragmatism uses research designs that involve decisions based on answering the questions under investigation (University of Nottingham, 2022). The qualitative pragmatic inquiry approach was employed in this project by strategically combining and drawing on various sources.

NCapture, a web browser extension for Chrome, allowed the gathering of web content to be imported into NVivo 15. NVivo 15 provided qualitative data analysis. NVivo 15, the latest edition, provides tools to ask questions about the collected data. Data analysis would still involve a thematic analysis.

Several research methods were considered for this project, including narrative and phenomenological approaches (Neubauer et al., 2019). Some qualitative research approaches are narrative, phenomenology, and case studies (Hoover, 2021). The narrative method explores an individual's life (Turnbull et al., 2023). The narrative method is inappropriate because I am not exploring an individual's life (Dahlstrom, 2021).

Phenomenology aims to understand a phenomenon and is particularly suitable for researching people's experiences (Picton et al., 2017). Phenomenology is a research strategy well-suited for exploring life experiences (Neubauer et al., 2019).

Phenomenology is not suitable for the project, as it is not concerned with explaining life experiences.

Researchers use purposive sampling to select a sample based on a population (McCombes, 2019a). Targeting individuals with specific criteria may ensure data saturation. Identifying enough participants to meet the established research requirements was necessary. Research participants were selected for the project based on pre-established criteria, with an emphasis on minimizing bias as much as possible (Moser & Korstjens, 2023). Data saturation is critical to the project's success, as it must occur (Damyanov, 2023). I chose a project population based on a pre-described standard that will help achieve data saturation within the targeted population. Data saturation was the goal of all qualitative inquiry research studies (Yang et al., 2022). Concepts and evaluation of saturation involved qualitative research. Qualitative studies reach data saturation when researchers discover no new categories or themes (Damyanov, 2023). I utilized internal and external organizations' documents, a semistructured interview process, and a data triangulation methodology to ensure that the research had reached saturation. Data saturation becomes apparent when researchers triangulate all data types and discover no new content (Fusch et al., 2018).

Population and Sampling

I completed data collection through the websites of financial institutions, the U.S. government, and NIST's publicly available websites that govern mobile financial transactions. Data collection also involved publications by cybersecurity professionals on websites and/or in articles. The Federal Financial Institutions Examination Council (FFIEC) guidance states that all financial institutions must assign one information security officer responsible and accountable for implementing and monitoring the program (Morris & Rumph, 2020). The duties of a cybersecurity manager are intensifying and involve taking on new roles. The information security officer plays a dynamic role in the organization, providing decision-makers with the necessary information for effective governance (Morris & Rumph, 2020). Targeting cybersecurity professionals who met targeted roles through sampling may increase the depth of the project results.

The population for this research project consisted of individuals with experience in cybersecurity within financial institutions. For this project, I implemented purposive sampling to help identify data collection sources through financial institutions' websites, U.S. government websites, and NIST's publicly available websites governing mobile financial transactions. Data collection involved evaluating cybersecurity professionals' work through professional websites and articles that met the criteria to answer the research question. Purposive sampling is mainly used in qualitative research to identify and select data gathered from cases related to the project (Nikolopoulou, 2022). Using purposive sampling involves the least resources and quickly identifies individuals with

experience within the research project. There are several different purposive sampling strategies. Criterion sampling appears to be the most popular method for purposeful sampling (Nikolopoulou, 2022). Purposive sampling identifies common patterns, discovers variations, reduces variations, simplifies analysis, and facilitates group interviewing. The use of purposive criterion sampling allows for the selection of participants with extensive experience in cybersecurity skills. It provides a means to target those qualified individuals. The participants for this research project were selected using specific criteria to ensure success. The criteria for participant selection were (a) must be over 21 years of age; (b) must be a cybersecurity professional; (c) must know about IT mobile security related to financially transacted events over mobile networks, and (d) must be willing to share their experiences, whether positive or negative.

I achieved data saturation by targeting specific information generated by NVivo 15. Targeting cybersecurity professionals who share cybersecurity roles will ensure data saturation. A qualitative research project begins with a comprehensively scoped sampling plan that enables the selection of diverse participants and cases to provide rich data (Moser & Korstjens, 2023). Data saturation is crucial for ensuring the project's success. Data saturation has gained widespread acceptance as a methodology in qualitative research, and further data collection or analysis is not necessary once data saturation is achieved (Damyanov, 2023).

Data saturation is vital when determining sample size (Hennink & Kaiser, 2021). Several articles and books suggest that anywhere from five to 50 participants are adequate to achieve data saturation in qualitative research (Yang et al., 2022). Data saturation

determines sample size and differs for each project when no new information or themes are observed (Moser & Korstjens, 2023). Using the cultural consensus model, as few as 10 informants are needed to establish a consensus reliably (Atran et al., 2005). Yang et al. (2022) provided a comprehensive analysis of saturation concepts and their evaluation in qualitative research methodologies. I received IRB approval before proceeding (04-04-23-0599888) further into the interviewing process. The IRB review aims to ensure that researchers take appropriate steps to protect the rights and welfare of human subjects participating in the research. (U.S. Food & Drug Administration, 2019). I provided a consent form for the participants to review before the research interview. I reviewed the interview process with all participants and allowed them time to ask any questions or express concerns they might have.

Ethical Research

Anonymity and protection of research participants remain essential to data collection, as researchers must protect stakeholder identities (Dhirani et al., 2023). Protecting participants' privacy allows them to remain anonymous by collecting data in a private space, encrypting computer-based files, storing documents in a locked cabinet, and removing personal identifiers from project documents as soon as possible, thereby avoiding the collection of personal data identifiers (Purdue University, 2019). I obtained informed consent before conducting any interviews, and participants could refuse participation at any point (Roberts, 2019).

The Walden University IRB process requires preapproval before a researcher can begin the research. The IRB process ensures that researchers meet all requirements

related to the human rights of participants. Morally sound practices lead to an ethically based research project. I reminded participants that participation is voluntary; they can withdraw from the project at any time. Walden University will not grant credit for student work conducted without the IRB's ethics approval or that otherwise fails to comply with IRB requirements. To maintain compliance with the IRB process, I completed the National Institutes of Health (NIH) training and received a certificate of completion. I completed Certificate Number 2496885 in September 2017. Maintaining trust is paramount when conducting research. Protecting the research participants is required. I used a coding system for the research participants and the participants' financial centers.

Only I have access to the participants' names and code names, which will ensure their anonymity. I used code names, such as P1, P2, and so forth, instead of participant names. I guaranteed the participants' confidentiality throughout the entire research process. Once the interview process finished, I provided the participants with a bulleted summary of their interview comments to allow for participant review. I stored the information on my computer in a secure, encrypted vault. The Walden University IRB process requires researchers to destroy interview data five years after the CAO approves the completed project. I will accomplish this by setting a date on my Google Calendar and then deleting the files in an encrypted format.

Data Collection

Instruments

I was the primary data collection instrument for this qualitative pragmatic inquiry. The researcher is an active respondent in the research process, also known as researcher-

as-instrument (Pezalla et al., 2012). I analyzed the data, identifying themes and patterns until I reached data saturation. An experienced interviewer possesses the following skills: technical competence, interactive competence, attention to detail, leadership, good communication skills, and awareness of previous knowledge and personal bias (Helfferrich, 2019). Triangulation provides a method to promote social change, mitigate bias, and achieve data saturation, thereby adding depth to the collected data (Fusch et al., 2018). I used NCapture, a web-browser extension for Chrome, which enabled me to gather web content and import it into NVivo 15. NVivo 15 provided qualitative data analysis. NVivo 15, the latest edition, provided tools to ask questions about the collected data. The data analysis involved a thematic analysis. Semi-structured questions have a clear purpose, a defined content type, and a sequence of open-ended exploration, encouraging respondents to answer in their own words (George, 2022).

The data collection process requires identifying common themes and patterns through the interview process to reveal an understanding of the research question. I gathered information from websites using Ncapture. This project involved the websites of financial institutions, the U.S. government, and NIST, publicly available websites governing mobile financial transactions. Data collection involved cybersecurity professionals' publications through websites and/or articles.

Data Collection Technique

I gathered web content and imported it into NVivo 15. NVivo 15, the latest edition, provided tools to ask questions about the collected data. Data analysis involved thematic analysis. Scientific or academic research was handled objectively by a seasoned

interviewer. The participant bias stems from the respondents' desire to answer correctly rather than honestly. Identifying potential participant and researcher biases helped find the appropriate preventive measures (Pannucci & Wilkins, 2011).

I searched the targeted financial institutions' websites and open-source intelligence, obtained the written policies, and found institutional documents from the financial organizations contributing to the research. I gathered data from at least six mobile cybersecurity professionals.

Data Organization Techniques

Data collection techniques were employed to ensure the reliability of the data during my data collection process. Many qualitative studies employ rigorous standards to ensure trustworthiness and integrity throughout the data analysis process, including the use of computer software, peer review, and an audit trail (Johnson et al., 2020). An audit trail describes the step-by-step processes and decision-making throughout the project that the author maintains, which occurs prior to manuscript development, thereby enhancing confirmability (Johnson et al., 2020). Organizing the research before starting the process, with approved documentation procedures in place, is essential to ensure research integrity, organization, and efficiency. I began the data collection process by defining my research, choosing my methodology, and planning the data collection procedures (Bhandari, 2020a).

I used Microsoft Word, Excel, NCapture, and NVivo 15 to organize the notes and transcription for proper organization. Transcribing was completed and stored in Microsoft Word. Excel keeps track of data entry, storage, analysis, and visualization for

later analysis. NVivo 15, the latest edition, allows for a direct Excel file upload and conversion. NVivo 15 also provides tools to ask questions about the data collected.

Data Analysis Technique

A qualitative pragmatic inquiry project, often used for business research, best fits a specific subject for describing, comparing, evaluating, and understanding different aspects of a research problem (McCombes, 2019b). A qualitative project gathers data from credible sources to answer the overarching research question. Data analysis for qualitative case studies originates from multiple sources, is categorically aggregated, and seeks themes within the data. The interpretive phase, the final phase, involves generalizing the data (Capella University, n.d.). Thematic analysis of the data was conducted using NVivo 15, which transcribes the interviews and group responses, identifies and catalogs themes, establishes connections, facilitates comparisons within the data, and provides organization (McNiff, 2022). Excel codes and tracks themes in qualitative data by creating themes and sub-themes through columns, keeping the data organized and easy to examine. A researcher may create new themes and sub-themes in additional columns and examine how each participant's responses relate to these themes (Fearon, 2023). The method involves identifying a collection of themes from the data, with the hope that relevant insights about lessons learned from the case will emerge. Thematic analysis is a method of analyzing qualitative data gathered through interviews. Thematic analysis follows a six-step process: familiarization, coding, generating themes, reviewing themes, defining and naming themes, and writing up (Caulfield, 2019). The theoretical framework identified a theory cluster, categorized theories, specified the

relevant theories for the research, and outlined how the project will contribute to answering the research question. The conceptual framework illustrated the relationships among these ideas and their relevance to the research project (Edwards, 1998). Yin (2016) maintains that data must be checked and rechecked for accuracy; the analysis must be thorough and addressed, and then bias must be dealt with. Yin's five-phased cycle is: (a) compiling, (b) disassembling, (c) reassembling (and arraying), (d) interpreting, and (e) concluding (Yin, 2016). The formal analysis begins with compiling the field notes. Next, I break down the compiled data, constituting a disassembly procedure. I used NVivo 15 for qualitative data analysis to identify themes and emerging patterns, uncover richer insights, and produce articulated, defensible findings. I used NVivo 15 to qualitatively analyze textual and audiovisual data sources, organize and code multiple data sources, assign attributes to data for comparative purposes, and facilitate querying and searching data (Georgia State University Library, 2021). Establishing data patterns facilitates the identification of emerging themes by transforming codes into categories. It allowed the researcher to identify commonalities or patterns as they focused on the data during analysis.

Reassembly is the process of assembling arrangements and recombination. Fourth, interpreting the reassembled data and concluding is the final phase of interpreting the results. NVivo's latest edition, NVivo 15, provides an organized and structured approach to data analysis. The data is stored in one place, works efficiently with qualitative data, facilitates subgroup analysis, and helps researchers be more efficient. Using methodological triangulation for this project aided in understanding the

overarching research question through the combination of primary and secondary data collection methods. Understanding multiple data sources gave the researcher a firm foundation for answering the research question. I implemented data triangulation in this research. The data triangulation technique combines datasets. Data triangulation requires researchers to compare datasets for convergence, complementarity, and divergence, enabling methods to validate findings when they agree mutually. Researcher bias is always a concern. Triangulation minimized researcher bias (Bhandari, 2022).

Reliability and Validity

Reliability and validity are concepts used to evaluate the quality of research based on data. Reliability refers to consistency, while validity concerns the accuracy of a measure. A project demonstrates reliability when researchers duplicate its results with the same outcome. Validity is the consistent measure of what is to be measured (Middleton, 2019).

Dependability

Dependability is reasonably ensured for the project through repeatability, as evident in the interview protocols and questions (see Appendix B; Universal Teacher, 2019). When the interview commences, Dependability emphasizes the need for the researcher to account for the changing context within the research (Trochim, 2020). I used data triangulation and member checking to ensure the dependability of the data collected (Noble & Heale, 2019). The use of data-collecting instruments did remain consistent. I created an audit trail, enabling others to replicate similar results behind my research project (Carcary, 2020).

Credibility

Credibility involves demonstrating that the results of qualitative research are credible or believable by checking the sources in the project. The participants are crucial to judging the credibility. Credibility may depend on the researcher's training, experience, track record, status, and presentation (Johnson et al., 2020).

Transferability

Transferability is the researcher's responsibility for generalizing in the qualitative project. Transferability refers to the extent to which researchers can accurately generalize or apply qualitative research findings to other contexts. Transferability means researchers can apply the results to other contexts. Transferability in qualitative research refers to the extent to which the results of interview data can be applied beyond the bounds of the project (My Dissertation Coach, 2020).

Confirmability

Confirmability is the final step in establishing trustworthiness for a qualitative researcher. Confirmability concerns whether researchers base the project's findings on participants' narratives and words rather than on potential researcher biases. The findings are shaped more by participants than by a qualitative researcher (Complete Dissertation, 2021). Following Carcary (2020), who proposed that audit trails develop trustworthiness, I used a research audit trail to establish confirmability.

Transition and Summary

In Section 2, I provided details of my project, indicating that the purpose was to explore the strategies that cybersecurity professionals use at financial institutions to

mitigate data breaches for their mobile customers who access financial data. Section 2 covers data collection and analysis techniques to obtain the organization's data. The researcher is the primary instrument for data collection. I used data triangulation to create themes and patterns, ensuring data saturation. I employed a Qualitative Pragmatic Inquiry, which involved primary data collection through semi-structured interviews, as well as secondary data collection from corroborating public documents and websites.

In Section 3, I present the research findings and discuss how they have benefited entities and society through social change. I followed all guidelines regarding participants' ethical responsibilities and treatment, as required by the IRB and outlined in the *Belmont Report*. I recorded and documented the research findings, including conclusions, recommendations, and potential future projects.

Section 3: Application to Professional Practice and Implications for Change

Overview of Project

This qualitative pragmatic project aimed to identify the cybersecurity strategies cybersecurity professionals use at financial institutions to mitigate data breaches for mobile customers who access financial data. The targeted population consisted of cybersecurity professionals in the Southeast United States who have 3 years or more of experience protecting financial transactions on mobile devices. The cybersecurity professionals within these educational institutions all had experience successfully securing mobile devices within their respective institutions. The process included semi-structured interviews and interactive member checking to minimize bias. I conducted five interviews with cybersecurity professionals who have three or more years of experience protecting financial transactions on mobile devices. I collected data from five interviews, four U.S. government agencies, three banking associations, and 10 national banks to gather recommendations for protecting financially transacted data on mobile devices. Section 3 presents the findings of my research project on securing financial transactions over mobile devices. Information gathered from the five interviews, four U.S. government agencies, three banking associations, and 10 national banks on what they recommend to protect financial transactions over mobile devices, yielded rich data that provided themes. The conceptual framework was grounded in cybernetic theory to analyze the mechanisms to secure online financial transactions. Cybernetics provided a conceptual framework for understanding and describing natural and artificial systems by focusing on the principles of control, communication, and feedback loops. Cybernetics is

the scientific study of regulatory systems, control within those systems, and how the system regulates the flow of information (Olobia, 2021).

The interviews and data from online sources yielded rich data that provided six major themes to emerge in the research. Establishing themes required a continued review of the data obtained from five interviews, four U.S. government agencies, three banking associations, and ten national banks. Establishing themes and minimizing bias required data triangulation to ensure that online security recommendations protecting financially transacted data, obtained from publicly available resources, aligned with my research findings. Cybernetic theory served as the guiding conceptual framework for examining methods to secure online financial transactions. Cybernetics offers a conceptual framework for understanding and describing natural and artificial systems, focusing on the principles of control, communication, and feedback loops.

Presentation of the Findings

The central research question for this project was: What security strategies are cybersecurity professionals using to mitigate data breaches for mobile users accessing financial data? This qualitative pragmatic inquiry aimed to answer the project's central research question. For the analysis, my interviews included five participants, who addressed eight questions related to the research question. These participants included individuals from South Florida. After receiving the participant responses, I transcribed their inputs using NVivo 15, reviewed the transcriptions, and sent them to the individuals to validate the accuracy of the captured input. One participant requested changes, which I incorporated into my research.

Additionally, the five participants confirmed that I had transcribed the interviews correctly. The interview questions yielded six overarching themes. A qualitative research project achieves data saturation when researchers identify no new themes. (Rahimi & Khatooni, 2024). I identified themes through data analysis, utilizing NVivo 15, and conducted interviews with five participants. Additionally, I analyzed publicly available recommendations from four U.S. government sites, three seminal sources from well-known cybersecurity magazines, and ten banks' recommendations.

It became apparent that I had reached data saturation after the fifth interview, collecting data from online governmental sites, banking associations, and bank recommendations to their customers. No new insights or themes emerged, indicating that collecting further data would be redundant and not add valuable information to the project. The five participants have at least three years of experience protecting online financial transactions made by mobile devices. Six themes emerged from the research: protecting online financial transactions using mobile devices. Six themes became known through this project: (a) using dual and multifactor authentication, (b) applying a VPN, (c) checking accounts frequently, (d) creating authenticator apps, (e) encouraging use of strong passwords, and (f) promoting user education. I recorded the frequency of responses for the six themes in Table 2.

I present each theme in the following table, visualizing data results using NVivo 15 software. To understand the results presented in the table, first identify the central theme on the left side of the table. The table presents numerical counts in two columns: Participants and Documents. Numbers in the Participants column indicate how often

interviewees mentioned each theme. Likewise, under Documents, I collected the data through online sources.

Table 2 shows zero participant recommendations for “Checking Accounts Frequently”, “Applying a VPN”, and “Using Strong Passwords.” Cybersecurity professionals do not recommend frequently checking financial accounts for several reasons. The user may be overloaded with anxiety, which distracts from meaningful, preventative steps (NIST, 2023). A VPN’s primary function is to encrypt an internet connection and mask an IP address, not to be used as an authentication tool. A VPN will not protect a user’s financial accounts if someone already knows their username and password. MFA secures user logins by verifying identity, while a VPN secures the data as it travels across a network (New Jersey Cybersecurity & Communications, 2025). Using strong passwords may lead to users writing down the passwords, making typos, and experiencing password fatigue. Users may be overwhelmed with the directive to create long and complex passwords, leading to employee workarounds that compromise security (Rooney et al. 2024).

All participants in this study made minor, insignificant comments about checking accounts frequently, using a VPN, and employing strong passwords. Some questions addressed in this project involved asking: “What cybersecurity is the most effective in mitigating data breaches for mobile customers who access financial data?” Financial institutions’ strategies to mitigate security breaches for mobile customers have changed to newer techniques, with MFA emerging as a clear choice.

Table 2*Themes*

Themes	Participants	Documents
	Count	Count
Using DFA/MFA	5	13
Check Accts Frequently	0	2
Authentication App	2	2
User Education	2	7
Applying a VPN	0	6
Strong Passwords	0	12

Note. DFA/MFA = Duo Factor Authentication and Multifactor Authentication; VPN = Virtual Private Network.

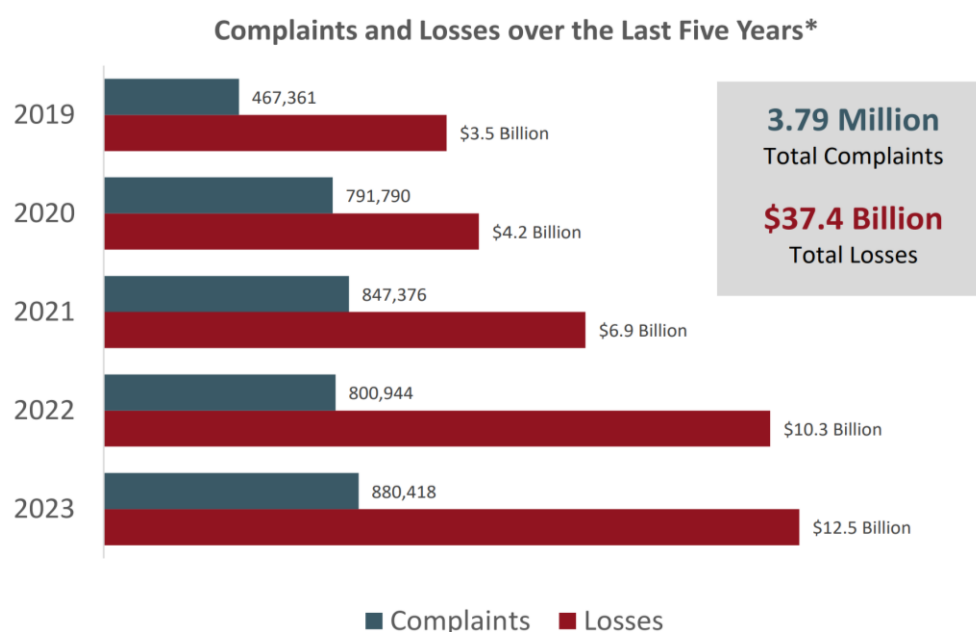
Theme 1: Using Dual and Multifactor Authentication

A password is a single type of factor. The most common types of factors are (a) something you know, which includes a password or PIN; (b) something you have, which includes a smartphone, a token device, and a secure USB password key; and (c) something you are, which includes a fingerprint, retina scan, and facial recognition. MFA requires a user to present two or more credentials to identify the user's identity. Dual or multifactor authentication works by registering a third-party app, such as the Microsoft Authenticator App, as the second factor. Microsoft states multifactor authentication has blocked over 99.2% of account-compromised attacks (Najshahid, 2025). CISA (2024) found that using MFA makes your accounts 99% less likely to be hacked. All participants who took part in the live interviews unanimously recommended 2FA or MFA. Thirteen out of 17 online sources recommended 2FA or MFA. MFA and 2FA are necessary for organizations to protect user accounts, assets, and data. Breaking through single-factor authentication is easy for cybercriminals. Single-factor authentication often uses only one

password. The subset of MFA is 2FA, which requires users to submit two types of authentication. MFA requires at least two types of authentication, so 2FA is a form of MFA, but not all MFAs are 2FAs. Providing online security presents challenges for many financial organizations and large financial institutions due to many factors, including the increasing sophistication of cyber threats, the vast amounts of sensitive data they handle, and the need to balance security with user convenience. The Federal Bureau of Investigation (2023), which publishes the Internet Crime Complaint Center Report (IC3), reported that total losses from 2019 to 2023 exceeded \$37 billion, as shown in Figure 1. Cybersecurity & Communications Integrated Cell (2024) reported that 2FA and MFA can block 99.9% of attacks against online accounts.

Figure 1

Internet Crime Complaint Center Report (IC3)



Note. Accessibility Description: Chart includes yearly and aggregate data for complaints and losses from 2019 to 2023. Adapted from Federal Bureau of Investigation (2023).

The first central theme from the research was the importance of dual and multifactor authentication. All participants in my project stated the importance of using MFA as an integral component of their cybersecurity practices. Participant 1 stated, “Nowadays, we are pushing towards having some sort of multi-factor authentication for the clients.” Participant 2 stated, “The biggest bang for your buck anyone can use now is multi-factor authentication.” Participant 3 stated, “We are switching users to MFA.” Participant 4 stated, “What we are using now is MFA.” Participant 5 stated, “MFA is effective when the application is on the end user’s phone.” DFA and MFA significantly increase security by requiring multiple verification methods to access an account.

Theme 1: Connection to Literature

Cybernetics is the science of control and communication in systems, with a focus on feedback systems (Wiener, 1961). Cybernetics conceptualizes systematic configurations of interconnected systems that can be programmed to enable regulation and adaptation. Using the cybernetic theory, MFA can be understood and enhanced. Cybersecurity professionals might have prevented failures in information security and related projects if they had sufficiently incorporated cybernetic principles while implementing security mechanisms and projects (Kushal & Arun, 2017). Cybernetic principles will guide the setting of policies, which are regulations and implementations that control. Cybernetics, developed by Wiener in 1948, can be considered a relatively recent science of control. Control theory examines how a control stimulus generates a system's output, which is then measured by the sensors (Peng et al., 2022). MFA is the control mechanism. The control system comprises two components: the control object

and the controller (Peng et al., 2022). Cybernetics is concerned not with the nature of entities but with their behavior patterns, focusing on what an entity does and is capable of doing. The regulation is that only approved users will have access to sensitive information. Control and regulation are inherent to any successful organization. A cybernetic management approach, known as a “hard systems approach,” can self-regulate, maintain a steady state, and retrieve information (Antai & Hellberg, 2024). Applying cybernetic principles to MFA helps to initiate more adaptive, intelligent, and robust security systems. Developing cybersecurity may be based on cybernetics, utilizing control theory, systems theory, and information theory to inform the design of regulatory security systems, ultimately enhancing online security (Yan, 2022). Cybernetics for the Doctorate of Information Technology (DIT) interview process examined the technological controls of security systems that protect mobile financial data transactions. Cybernetics studies the controls of any system that employs technology (Loshkarev, 2021).

As a theoretical framework, cybernetics underpins security design by emphasizing feedback, control, and regulation, principles exemplified in mechanisms such as MFA. Cybernetics can provide a framework for understanding how to plan and implement MFA. MFA uses cybernetic security mechanisms through feedback loops, which enhance the integrity of authentication systems (CISA, 2024). The synergy of cybernetic security and MFA protects sensitive data (Hudson, 2022). This type of system will enhance cybersecurity for online financial transactions.

In an interdisciplinary field, cybernetics examines the regulation and information flow mechanisms of complex systems. Cybernetics is the conceptual framework that drives this research, which aims to observe the strategies employed by cybersecurity professionals in implementing security for financial transactions made by their mobile customers using mobile devices. Cybernetics is an appropriate conceptual framework model to explain the critical factors that affect mobile device cybersecurity strategies, as demonstrated by the use of MFA. Cybernetics encompasses eight key characteristics: feedback, threshold, energy, intelligent systems, human behavior and psychology, automata theory, game theory, and quantitative analysis (Kushal & Arun, 2017). The system generates feedback loops in MFA when it responds to authentication attempts. Each feedback loop can be considered a control mechanism that maintains system integrity. Using thresholds in MFA, a loop may escalate due to failed login attempts, generating a correction for the user. Adaptive MFA systems may adjust authentication requirements based on risk assessment. Each state and transition within MFA is regulated by system inputs and logical processes, reflecting core cybernetic principles of control, feedback, and adaptive regulation. The theory of games involving MFA raises the complexity of factors when bad actors try to access a system, thereby increasing the required steps for authentication.

Weiner (1961) proposed the theory of the game in cybernetics. Entering a password illustrates game theory by representing a communicative exchange between the user and the system. The machine displays whether the password was correct or incorrect. If the password is correct, the machine displays the contents of what the user

wants, demonstrating communication between the machine and the user. Game Theory is widely used in information security (Kushal & Arun, 2017). Wiener's cybernetic philosophy provides a conceptual framework that researchers can apply to address research challenges in information security. Cybernetics' range of uses includes identifying needs for management information, developing policies, and managing financial resources (Bell et al., 2021).

Theme 2: Check Accounts Frequently

In this project, only two articles and no participants stated the importance of checking accounts frequently. Discovering a breach at that point is more reactive security than proactive security. Checking accounts frequently can help minimize losses, although it is essential to note that it will not prevent intrusion. Constantly checking accounts is time-consuming and tedious for multi-account holders. Misinterpretations may arise from misidentifying some transactions as not legitimate. Some institutions recommend checking all financial accounts frequently. Those institutions state that preventing an intrusion is paramount to checking accounts frequently.

Cybernetics is not commonly used to verify financial accounts, as it is not a direct application in this field. Using a cybernetic approach to protect online financial systems involves automating the monitoring of financial accounts to alert users to unusual activity and spending patterns (Luna, 2024). Cybernetics is the study of the use of feedback loops in self-regulating systems. The cybernetic framework will help design systems that alert for automated transfers, limit withdrawals, or lock authorized cards. Cybernetics is not a

tool used directly to protect accounts. However, its principles may enhance automation in monitoring and managing financial accounts through feedback loops.

All participants stated that it is good practice to check financial accounts frequently. Although preventing data breaches remains the primary goal, no organization is 100% protected from a financial security breach (Mahon, 2021). Identifying a breach early may save a significant financial loss. PNC Bank recommends checking online financial accounts at least twice a week for a balanced approach. Bank Five states that customers must check their financial accounts frequently to spot unusual activity quickly. Chase Bank advises checking financial accounts at least once every few days. Citizens Bank's approach is to check online financial accounts based on usage. Checking accounts with numerous debits and credits requires frequent review. Account holders must check an inactive savings account at least once a month. Discover recommends logging in every day to catch a data breach early. Citibank recommends monitoring financial accounts at least once a week. TD Bank recommends that you monitor your online financial accounts once a week as a good starting point. A combination of seventeen articles by financial institutions and government sites recommends checking online financial accounts frequently, which means at least twice a week if not daily.

Theme 2: Connection to Literature

The U.S. Department of Defense utilizes effective monitoring, which is critical for network security and a fundamental component of the Risk Management Framework, an automated method for checking financial accounts. Automating account checking is a recommended method for consumers to monitor their financial accounts more efficiently.

Automation will facilitate the installation of advanced security measures, expedite cybersecurity processes, and enable swift, informed cybersecurity decisions (NIST, 2020a). Cybernetic principles are foundational ideas in interdisciplinary studies that use biological, mechanical, social, or digital control systems (ScienceDirect, 2024). When checking accounts frequently, the cybernetic connection for account alerts is an automated financial account alert through feedback looping (Albasheer et al., 2022). The end user is alerted to check a financial account that has been compromised manually. Account alerts inform users through text, email, or push notifications about activity in their bank accounts, such as balance changes, transactions, or suspicious activity. The user will then manually check the financial accounts. Applying cybernetic principles to financial accounts, systems will automatically monitor changes in financial data and inform the user.

Theme 3: Authentication App

An authentication app is used in mobile technology, providing an extra layer of security. The app is often designed and implemented by a specific institution. The institution can enhance control over user access by offering increased security within the app. Two participants and two articles recommended the use of an authentication app. The authentication app may allow users to set up MFA in a more secure environment. Authentication apps generate one-time passwords that change frequently, making it difficult for a threat actor to identify. Phishing risks decrease as codes are generated within the app and not sent via email or SMS. Usually used through a smartphone, some disadvantages may arise. The phone may run low on battery power or become

inaccessible. Moving an app to another phone is difficult. Malicious apps may mimic legitimate ones, causing users to experience a steeper learning curve and longer account access times. Compatibility issues may include using a VPN. Not all VPNs are compatible with all authentication apps.

Cybernetic principles can guide the design of authenticator apps, providing a framework for implementing monitoring systems built into the app. Apps monitor deviations in user behavior, triggering a feedback loop alerting a financial institution or the user (Samojło, 2019). Cybernetics offers a systematic framework for designing and analyzing control loops (Geckeler, 2020). Using a cybernetic framework, a system for ongoing account monitoring may have a control loop in which transactional data serve as inputs. The system bases its decision outputs on user feedback when it detects deviations from preselected patterns. This feedback-driven regulation enables continual account monitoring.

Theme 3: Connection to Literature

Building and deploying popular financial institution apps for mobile devices requires supporting various operating environments and portable computing devices such as smartphones or tablets. Mobile users comprise 97% of U.S. adults who use applications to fulfill their different needs (Pew Research Center, 2024). MAM, EMM, and MDM are management techniques for controlling mobile device security. MAM controls the device, whereas MDM focuses on specific applications to secure mobile devices. MAM is the software and services necessary for provisioning and controlling access to proprietary mobile apps. Cybernetic design in MAM supports ongoing

monitoring and feedback loops to detect app anomalies, policy violations, and security threats.

MDM is proprietary software that enables IT administrators to manage, secure, and enforce smartphone and mobile device policies. Applying cybernetic principles in MDM leads to the design and implementation of proprietary app development, enabling security management to control, secure, and enforce policies. Cybernetics, as a control mechanism in complex MDM app development, utilizes feedback systems that continuously collect data on device status, user behavior, and compliance, then respond through an automated response based on that system. MDM is a security solution that monitors, manages, and secures mobile devices, including laptops, smartphones, and tablets (Batool & Masood, 2020).

EMM is significant for security by using people, processes, and technology to manage mobile devices, wireless networks, and other mobile computing services. EMM is a system that prevents unauthorized access to enterprise applications, such as those offered by financial institutions. The security offered by EMM is password protection, encryption, and wipe technology, or the ability to have the device remotely wiped of all data (Rouse, 2019). Cybernetics plays a crucial role in the design of EMM, employing closed-loop control to provide continuous feedback and adapt decision-making to the established criteria (Franklin et al., 2020). Considering the cybernetic model, EMM functions as the control center, using feedback from other subsystems and comparing it to the desired states.

Theme 4: User Education

Two participants and seven articles recommended user education. Patel (2019) found IT security's weakest link is human users. Humans can undermine any security system. Employees' mistakes lead to security incidents 88% of the time (Patel, 2019). These can occur through mistakes or a lack of knowledge. Providing an ongoing education program for cybersecurity training to educate users is expensive and tedious. Barriers to a cybersecurity training program include a lack of time, resources, and employee motivation, according to the National Cybersecurity Alliance (2024). No program has been developed in a reliable and foolproof way to educate the workforce in cybersecurity compliance, according to ISC2 (2025). One way to train the workforce is to send them phishing simulations, which include fake but realistic-looking emails, to test employees' ability to recognize phishing emails. This technique will demonstrate if the employee training regarding phishing emails is successful.

A component of cybernetics is the science of communication in systems that interact with humans (Olobia, 2021). Applying cybernetics to user education enables users to learn effectively while receiving immediate feedback. When users fail authentication, the system recognizes the failure and responds by providing learning scenarios that correct the failed behaviors.

Theme 4: Connection to Literature

Cybernetics aids user education by providing feedback, suggesting behavior modification, and continuous learning. Cybernetics is characterized by feedback, as complex systems adapt to environmental factors through feedback (Jakubik, 2021). The

cybernetic approach to users classifies users as an integral part of a self-regulating system, with real-time feedback and behavioral reinforcement that shape decision-making. By integrating cybernetic principles into user education, organizations can develop adaptive learning environments that provide users with continuous feedback and corrective actions. Control theory is a system's output generated by a control stimulus, with the output measured (Peng et al., 2022). The control system comprises two components: the control object and the controller (Peng et al., 2022).

Theme 5: Applying a VPN

A VPN encrypts data for transmission by establishing a digital connection between a user's computer and a VPN server. Six articles and no participants recommended a VPN. Benefits of using a VPN include preventing unauthorized access to a connection by people, software, and web browsers. A VPN hides personal information from hackers and masks a user's real IP address and location. The VPN blocks browsing habits.

A VPN should provide enhanced cybersecurity, but this is not always the case. Some of the disadvantages of using a VPN include a slower internet connection. The data encryption may slow down transmission rates. VPNs may collect a user's data, have weak security, and use less advanced algorithms. VPNs are not compatible with some devices. Premium VPNs are expensive and can impact budgets. VPNs may allow users to access various sites that are blocked in specific geographic locations. Various countries ban VPNs to restrict access. A VPN will not protect against voluntary data releases.

Cybernetics, a project of control, provides feedback loops in a VPN connection by providing information on latency, packet loss, and encryption integrity (Kristel et al., 2024). Suppose the quality of a VPN connection drops. In that case, the cybernetically designed system may switch servers and protocols, maintaining a secure and stable connection. VPNs employ cybernetic monitoring to detect disconnections and may trigger disconnect procedures to prevent data loss.

Theme 5: Connection to Literature

A VPN provides a secure connection method, adding privacy while using public and private networks, such as Wi-Fi and the internet (The Federal Trade Commission, 2021b). VPNs that employ cybernetic theory actively utilize the control, communication, and adaptive feedback mechanisms that enable secure and reliable data transmission over untrusted networks. A Mobile Virtual Private Network (mVPN) performs better on a wireless network, as VPN apps encrypt, or scramble, the data sent between devices (Federal Trade Commission, 2021a).

Looking at a VPN through the cybernetic lens reveals a self-regulatory control system. A VPN operates as a closed-loop feedback system. A VPN responds to environmental inputs and enforces rules to maintain the system's desired secure state. One of the security solutions for mobile financial data transactions is an IP-based Virtual Private Network (IPVPN). The primary objective of a VPN is to establish a secure network tunnel on the public internet using encryption technology, which enables the transmission of data securely and prevents others from intercepting packets.

Theme 6: Strong Passwords

No participants and twelve articles recommended strong passwords. The participants in this project said that strong passwords can present problems that lead to data breaches. Complex passwords can be challenging to remember. Complex passwords are difficult to remember, and employees often will write down the password and place it under the mouse pad. Entering complex passwords takes more time, reducing productivity with the worker. Shoulder surfing may occur when the user takes more time to complete them. Complex passwords do not guarantee security. MFA protects an account when the threat actor has obtained the password (Solomon, 2024).

Increasing computing power is rendering many passwords ineffective in protecting financial accounts. Modern computers can crack a brute-force password more quickly using graphics processing units (GPUs). GPUs and parallel processing can try billions of password combinations per second (Ibrahim Alkhwaja et al., 2023). Smart Guessing Algorithms and AI utilize specialized password-cracking tools to reveal complex passwords. Complex passwords will not protect against phishing, malware, or password reuse threats.

Passwords are insecure because they can be shared, guessed, or stolen. Over 50% of younger individuals admit to sharing passwords with friends, and 59% report reusing passwords across multiple sites (iProov, 2021). iProov (2021) stated that in the United States, 60% of consumers needed to change a password due to a data breach, and the average American abandoned 16 online purchases every year because of forgotten passwords. The end of the password could be near.

Cybernetics will direct strong password creation. Feedback loops in password creation provide real-time feedback on password complexity and strength, informing users if password requirements are not met. Users can utilize cybernetic principles to create policies that adjust passwords to meet requirements through control loops. Cybernetics involves adapting policies based on inputs and environmental factors. Cybernetics monitors ongoing communication, reporting security leaks on the dark web. The cybernetic principle applies to the complexity of passwords by providing feedback on complexity, involving a control system that enforces policies, facilitates adaptation, and corrects errors (Kristel et al., 2024).

Theme 6: Connection to Literature

Passwords are a form of single-factor authentication and are not enough to secure mobile devices for mobile transactions. To help increase security, IT security teams require MFA and 2FA for mobile financial transactions. MFA mandates users to verify their identities to provide multiple pieces of evidence to access a device, website, or application (Alqahtani et al., 2020). Passwords are controls for user access to mobile systems. In cybernetics, passwords are in a closed-loop feedback system. In a cybernetically designed system, the device and software monitor user authentication attempts, detecting anomalies such as failed login patterns, and then compare them to the established criteria, generating a response. When a user inputs a correct password, this prompts for MFA, which increases security because even if one credential becomes compromised, unauthorized users cannot meet the second authentication requirement (CISA, 2022).

I made a notable observation about Theme 5 (using VPNs), which revealed that only 6 out of 17 banks and government sites recommended using VPNs. Twelve of 17 banks and governmental sites recommended strong passwords. None of the cybersecurity professionals in the participant group recommended VPNs and strong passwords for cybersecurity. The constantly evolving security landscape necessitates additional security measures beyond a VPN or a strong password. Many cybersecurity professionals do not emphasize VPNs and strong passwords because they are aware of more advanced threats, and these tools have inherent limitations. Although banks and other public institutions often promote these strategies as a first line of defense, experienced cybersecurity professionals focus on higher security standards that address the deeper vulnerabilities in modern systems (CISA, 2020, 2025). Checking accounts frequently will only reveal that an attack has occurred, and does not offer protection for an account.

Applications to Professional Practice

This qualitative pragmatic inquiry aims to identify the cybersecurity strategies cybersecurity professionals use at financial institutions to mitigate data breaches for mobile customers who access financial data. The participants agreed that using MFA mitigated unwanted financial transactions and account intrusions. Financial institutions' specific IT problem is that some cybersecurity professionals lack effective strategies to implement cybersecurity measures that mitigate data breaches for their mobile customers who access financial data.

Cybersecurity has evolved throughout the years. Cybersecurity professionals were often reactive in mitigating data breaches to financial accounts. Some of the tools

invented by cybersecurity professionals were passwords, antivirus software, and firewalls. These tools faced many limitations. Suppose a threat actor discovers one factor of authentication. In that case, MFA increases the challenge for a hacker to gain access to financial information. Cybersecurity professionals revolutionized security for mobile financial transactions by introducing MFA. CISA (2024) reported that MFA blocks 99% of automated account hacking attempts. In the 1980s, hackers realized that the widespread adoption of personal computers by businesses and individuals created opportunities for the exploitation of digitally stored data (National Cybersecurity Alliance, 2024). Hacking mitigation techniques, which involved antivirus software and firewalls, emerged in the early 1980s and 1990s. This research project employed cybernetic theory as its contextual framework. Cybernetic theory states that systems react to outputs generated and then use that information to control a cycle of MFA further. MFA feedback mechanisms prompt users to take action after they enter an initial password, demonstrating the cybernetic principle of regulation and control. Tax preparers are required to use MFA to protect clients. As of June 2023, the IRS mandates that financial institutions, tax preparers, and tax preparation companies of all sizes must use MFA to protect clients' sensitive information (IRS, 2024).

Companies are turning to the cloud to provide storage and other services. MFA protects sensitive information in cloud accounts. Organizations protect remote desktop access by using MFA. The Health Insurance Portability and Accountability Act (HIPAA) requires protection for individuals' health information. MFA will put firms in compliance. Legal firms with large databases containing clients' sensitive information

utilize MFA for enhanced client protection. The federal government and the vendors they work with mandate the use of MFA for federal agencies. The FTC Safeguards Rule requires businesses that handle consumer data to maintain robust security measures to protect customer information from unauthorized access (Federal Trade Commission (2024). There is considerable demand for MFA from companies that currently use it and are considering adopting it in the future (Introspective Market Research. (2025).

Implications for Social Change

Mobile devices are rapidly changing the day-to-day business activities of global business and financial organizations. Mobile devices are poised to replace traditional financial operations and processes (Damen, 2021). Financial institutions add consumer value by offering mobile secure content and threat management. According to the Pew Research Center (2021), 97% of Americans own cell phones. Wi-Fi hotspots in coffee shops, libraries, airports, hotels, universities, and other public places are convenient. However, these systems often fail to provide adequate security (Federal Trade Commission, 2021a). Positive social change may result from the security strategies developed by this project, enabling cybersecurity professionals at financial institutions to implement best practices that protect their mobile customers' financial transactions while on Wi-Fi hotspots in various public places, such as coffee shops, libraries, airports, hotels, universities, and other public venues, which may decrease fraud.

Information security awareness procedures and policies developed for this project regarding mobile financial transactions may provide an additional layer of security for individuals using public networks. Mobile financial consumers and institutions may

experience social change through cost savings as more people adopt the convenience of mobile financial transactions, driven by mitigated mobile security concerns. Financial centers and consumers who utilize mobile technology in financial transactions can save time and transportation costs, reduce the need for employees to complete transactions, and contribute to the “green theme” by minimizing paperwork (Pazarbasioglu et al., 2020).

Recommendations for Action

This qualitative pragmatic inquiry revealed the importance of using MFA. Implementing MFA represents a crucial step in enhancing account security and mitigating cyber threats. Identifying major software, systems, and client needs is a first step. Then, implement MFA wherever possible in identified areas that require cyber protection, prioritizing systems and accounts that require immediate protection. Users, whether employees or clients, must be educated on the use and value of MFA. The users need clear communication explaining what MFA is and why it is important. Organizations and users that transmit financial data need to recognize the benefits that MFA provides in mitigating intrusions, thereby protecting both institutional assets and customer information. Organizations seeking to implement effective MFA must navigate the tension between security requirements and user productivity. The selected authentication mechanisms should provide robust protection while avoiding unnecessary complexity that could frustrate users or encourage workarounds. This balance is particularly crucial for small businesses, where 43% of companies with 250 or fewer employees suffer data

breaches (Gasnick, 2023). Formalized policies that define MFA requirements and implementation standards ensure consistent application across all organizational levels.

Using authenticator factors includes something you know, something you have, and something you are. The user must select at least two authentication factors to ensure security. The more layers added, the more secure the accounts will be. Using an SMS-based MFA is a good starting point, but it is not comprehensive. The mobile devices' Subscriber Identity Module (SIM) is vulnerable to SIM swapping and interception (Brennan & Smith, 2022). Push-based authentication is a user-friendly method that requires user input. Two-factor authentication usually involves the user's PIN on mobile devices. Through social engineering, push authentication may reveal a personal PIN to a hacker. The hacker may send fake push requests from the users' known companies. Hardware tokens provide a higher level of security. Hardware tokens are physical devices that resemble a USB drive, generating a unique, time-based code (Microsoft Ignite, 2025). Users must enter the code quickly, as the MFA and hardware-based device require. Organizations must implement MFA on accounts with sensitive information, including financial information, email, and cloud storage. Employees and stakeholders need to be convinced and trained on the successes of using MFAs. Organizations should strike a balance between strong security and user convenience, creating seamless and easy experiences. Administrative accounts must use MFA. Administrative accounts provide users with policies and passwords. The information is very valuable to hackers or other threat actors. Institutions must research the compliance standards required by the General Data Protection Regulation (GDPR), HIPAA, and the Payment Card Industry

Data Security Standard (PCI DSS; IT Governance, 2025). Often, the compliance standards require MFA. MFA can also include biometric identification. Biometric identification may include fingerprints, face recognition, and retinal scans. MFA provides a critical layer of security that protects access to accounts with sensitive information. Institutions must balance security with MFA while keeping the user's convenient experience.

Recommendations for Further Project

Cybernetics and MFA are two distinct but related fields. When both are involved with each other, they provide valuable information regarding protecting online financial information. Cybernetics, when applied to a security system designed for MFA, should yield more levels of security. Through cybernetic analysis, researchers can assess MFA feedback loops and determine how MFA may counter future security threats. Researchers can apply cybernetic frameworks to evaluate MFA feedback mechanisms and anticipate system responses to emerging attack vectors. Balance in a security system needs to be in place, as user fatigue results from strict systems that require complex MFAs. Cybernetics may project human behavior to build more adaptive MFA systems. Cybernetics could aid in creating AI systems that would augment the human element in MFA. Cybernetics is user-machine communication. MFA may need to adapt human actions and feedback, and cybernetics can help understand how to simplify those processes while enhancing security. Creating autonomous security systems that are self-regulating is a part of cybernetics. Security systems can become self-regulating, combining both cybernetics

and MFA techniques. Cybernetics and MFA techniques can guide autonomous response reporting.

In the future, biocybernetics and security may involve MFA containing unique user brainwave patterns for authentication. Quantum computers have incredible computational power that could break any encryption method. Cybernetic models may design MFA systems that will mitigate attacks by quantum computing. MFA frameworks incorporate biometric modalities including fingerprints, facial recognition, iris scans, and voice recognition. Cybernetically designed, AI-driven MFA biometric systems may evolve and succeed, protecting systems from quantum computer attacks.

Reflections

In more than 16 years of teaching computer-related courses, I have observed relatively few significant changes in the instructional approaches to this field. Staying up-to-date is challenging. When I began the doctoral degree, I investigated the security strategies used by cybersecurity professionals to mitigate data breaches for mobile users accessing financial data. I was at the data collection point when my participants backed out, citing they had received notices not to speak with anyone about their institutions' security policies. This setback delayed my progress approximately one year as I reapproached the IRB and revised my project to employ a pragmatic approach. Another challenge was learning how to write with a scholarly voice. I have learned how to conduct research, scholarly writing, and analyze data. I networked to find participants. No other method worked. Finding and interviewing my participants took about three months.

Attending courses at Walden University's DIT program has greatly impacted my students at two state colleges and a university. Walden University heightened my awareness that project-based learning modalities prove most effective in teaching students, as these approaches foster competitiveness and promote self-directed learning. My schools use a skills assessment management system from third-party educational software developers. Automated assessment systems grade student projects while generating real-time feedback. I often remind my students that they have the best learning experience with project-based learning.

When I began my project, my preconceived bias was that VPNs would be widely recommended and used by cybersecurity professionals to mitigate online threats. Subsequent research established that MFA affords superior comprehensive protection compared to earlier authentication methods. I realized that security to protect financial transactions was evolving faster than my studies. I ensured reliability and credibility, triangulated the data, and used member checking. I applied NVivo 15 to develop data-driven themes through inductive analysis, thus minimizing the risk of researcher-imposed bias or data skewing. Summary and Project Conclusions

Cyber threats are evolving at a rapid pace. Organizations' reliance on reactive security paradigms rather than proactive frameworks has resulted in billions of dollars in financial losses. Finally, a newer technique, MFA, has been found to mitigate over 99% of intrusions (CISA, 2024). The federal government requires an MFA for many financial institutions, tax preparers, and other institutions that handle sensitive consumer

information. Cybersecurity professionals must develop a culture that embraces MFA as a fundamental layer of defense in any security strategy.

My project's problem statement is "The financial institutions' specific IT problem is that some cybersecurity professionals lack strategies to implement cybersecurity in mitigating data breaches for their mobile customers who access financial data." This project's findings suggest that MFA's demonstrated effectiveness as a cybernetic control mechanism regulating access and system behavior has contributed to its widespread adoption within the cybersecurity professional community. Much financial data was breached, with many large-scale data breaches reported only a few years ago. Global data breach incidents exact an average financial toll of \$4.9 million per organization (IBM, 2024). The proliferation of MFA implementation among financial institutions correlates with significant reductions in breach-related financial losses (IBM, 2025).

References

- Alkhwaja, I., Albugami, M., Alkhwaja, A., Alghamdi, M., Abahussain, H., Alfawaz, F., Almurayh, A., & Min-Allah, N. (2023). Password cracking with brute force algorithm and dictionary attack using parallel programming. *Applied Sciences*, 13(10), 5979–5979. <https://doi.org/10.3390/app13105979>
- Albasheer, H., Md Siraj, M., Mubarakali, A., Elsier Tayfour, O., Salih, S., Hamdan, M., Khan, S., Zainal, A., & Kamarudeen, S. (2022). Cyber-attack prediction based on network intrusion detection systems for alert correlation techniques: A survey. *Sensors*, 22(4), Article 1494. <https://doi.org/10.3390/s22041494>
- Ali, L. (2019). Cyber crimes-a constant threat for the business sectors and its growth (a study of the online banking sectors in GCC). *The Journal of Developing Areas*, 53(1), 267-279.
- Alicea, B., Parent, J., & Singh, U. (2020). *Observer-dependent collective behavior for biologically-inspired processing models*. Openreview.net. <https://openreview.net/forum?id=FiwgkEEemXOg>
- Alqahtani, A. A. S., Alamleh, H., Gourd, J., & Alnuhait, H. (2020). TS2FA: Trilateration system two factor authentication. *2020 3rd International Conference on Computer Applications & Information Security (ICCAIS)*, 1–4. <https://doi.org/10.1109/ICCAIS48893.2020.9096825>
- Alqahtani, F. H., & Alsulaiman, F. A. (2020). Is image-based CAPTCHA secure against attacks based on machine learning? An experimental study. *Computers & Security*, 88. <https://doi.org/10.1016/j.cose.2019.101635>

- American Bankers Association. (2023). *Consumer Survey Banking Methods 2023*.
<https://www.aba.com/about-us/press-room/press-releases/consumer-survey-banking-methods-2023#:~:text=The%20national%20survey%20found%20that>
- American Psychological Association. (2018, April 19). Cybernetic epistemology. In *APA dictionary of psychology*. <https://dictionary.apa.org/cybernetic-epistemology>
- American Psychological Association. (2023). *Human research protections*.
<https://www.apa.org/research-practice/conduct-research/human>
- American Society for Cybernetics. (n.d.). *Cybernetics prehistory: Circularity*. <https://asc-cybernetics.org/foundations/history/prehistory7.htm>
- Antai, I., & Hellberg, R. (2024). Characterizing the defense industry for risk management: a systems approach. *Journal of Defense Analytics and Logistics*, 8(1), 38–55. <https://doi.org/10.1108/jdal-08-2023-0008>
- Apter, M. J. (1970). Cybernetics: A Case Study of a Scientific Subject-Complex. *Sociological Review*, 18(1), 93–116. <https://doi.org/10.1111/j.1467-954X.1970.tb03177.x>
- Arnott, B. (2023). *9 BYOD security best practices you need to know*. Forcepoint.
<https://www.forcepoint.com/blog/insights/byod-security-best-practices>
- Athulya, A., & Praveen, K. (2020). Towards the detection of phishing attacks. *2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184)*, 337–343. <https://doi.org/10.1109/ICOEI48184.2020.9142967>
- Atran, S., Medin, D. L., & Ross, N. O. (2005). The cultural mind: Environmental decision making and cultural modeling within and across populations.

Psychological Review, 112(4), 744–776. <https://doi.org/10.1037/0033-295X.112.4.744>

Atske, S. (2023). *What Americans know about AI, cybersecurity, and big tech*. Pew Research Center: Internet, Science & Tech.

<https://www.pewresearch.org/internet/2023/08/17/what-americans-know-about-ai-cybersecurity-and-big-tech/>

August, V. (2021). Network concepts in social theory: Foucault and cybernetics.

European Journal of Social Theory, 34(1), Article 136843102199104.

<https://doi.org/10.1177/1368431021991046>

Awan, H. (2023). *5 tips to ensure secure mobile device use in the workplace*. Efani.

<https://www.efani.com/blog/secure-mobile-device-use-in-workplace>

Balleine, B. W., & Dezfouli, A. (2019). Hierarchical action control: Adaptive

collaboration between actions and habits. *Frontiers in Psychology*, 10, Article

2735. <https://doi.org/10.3389/fpsyg.2019.02735>

Bardin, A., & Ferrari, M. (2022). Governing progress: From cybernetic homeostasis to

Simondon's politics of metastability. *Sociological Review*, 70(2), 248–263.

<https://doi.org/10.1177/00380261221084426>

Barker, E., & Barker, W. (2019). *Recommendation for Key Management, Part 2: Best Practices for Key Management Organizations*.

<https://doi.org/10.6028/NIST.SP.800-57pt2r1>

Bartock, M., Souppaya, M., Cherfaoui, M., Xie, J., & Cleary, P. (2022). Hardware

enabled security: NISTIR. <https://doi.org/10.6028/nist.ir.8320c.ipd>

- Batool, H., & Masood, A. (2020). Enterprise mobile device management requirements and features. *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Computer Communications Workshops (INFOCOM WKSHPS)*, 109–114.
<https://doi.org/10.1109/INFOCOMWKSHPS50562.2020.9162763>
- Bederna, Z., & Rajnai, Z. (2022). Analysis of the cybersecurity ecosystem in the European Union. *International Cybersecurity Law Review*, 3(35-49).
<https://doi.org/10.1365/s43439-022-00048-9>
- Bell, G., Gould, M., Martin, B., McLennan, A., & O'Brien, E. (2021). Do more data equal more truth? Toward a cybernetic approach to data. *Australian Journal of Social Issues (John Wiley & Sons, Inc.)*, 56(2), 213–222.
<https://doi.org/10.1002/ajs4.168>
- Bhandari, P. (2020a). *Data Collection | A Step-by-Step Guide with Methods and Examples*. Scribbr. <https://www.scribbr.com/methodology/data-collection/>
- Bhandari, P. (2020b). *What is Qualitative Research? | Methods & Examples*. Scribbr. <https://www.scribbr.com/methodology/qualitative-research/>
- Bhandari, P. (2020c). *What Is Quantitative Research? | Definition, Uses, and Methods*. Scribbr. <https://www.scribbr.com/methodology/quantitative-research/#:~:text=Quantitative%20research%20is%20the%20process>
- Bhandari, P. (2022). *A beginner's guide to triangulation in research*. Scribbr. <https://www.scribbr.com/methodology/triangulation/>
- Bhattacharjee, A. (2012). *Social science research: Principles, methods, and practices*.

Digital Commons @ University of South Florida.

https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1002&context=oa_textbooks

Bindas, D. V. (2020). Information warfare within the context of cybernetic epistemology.

RUDN Journal of Philosophy, 24(2), 297–302. <https://doi.org/10.22363/2313-2302-2020-24-2-297-302>

Bodkhe, P. (2021). CAPTCHA techniques: An overview. *International Journal on*

Recent and Innovation Trends in Computing and Communication, 5(9), 15-21.

https://www.researchgate.net/publication/350382694_CAPTCHA_Techniques_An_Overview

Brennan, B., & Smith, K. (2022). *FBI Tech Tuesday: SIM swapping*. Federal Bureau of

Investigation. <https://www.fbi.gov/contact-us/field-offices/phoenix/news/press-releases/fbi-tech-tuesday-sim-swapping>

Britannica. (2021). Editors of encyclopedia. *Cybernetics*. *Encyclopedia Britannica*.

<https://www.britannica.com/science/cybernetics>

Bumanglag, K., & Kettani, H. (2020). On the Impact of DNS Over HTTPS Paradigm on

Cyber Systems. *2020 3rd International Conference on Information and Computer Technologies (ICICT)*, 494–499. <https://doi.org/10.1109/ICICT50521.2020.00085>

Bunyakati, P., & Sammapun, U. (2019). On secret management and handling in mobile

application development life cycle: A position paper. *2019 34th IEEE/ACM*

International Conference on Automated Software Engineering Workshop (ASEW), 77–80. <https://doi.org/10.1109/ASEW.2019.00033>

- Burrell, G., & Morgan, G. (1979). *Sociological paradigms and organisational analysis*. Heinemann Educational Books.
- Busse, C., Kach, A., & Wagner, S. (2016). Boundary conditions: What they are, how to explore them, why we need them, and when to consider them. *Organizational Research Methods*, 1-36. <https://doi.org/10.1177/1094428116641191>
- Capella University. (n.d.). *Qualitative data analysis methods*. Campustools.capella.edu. https://campustools.capella.edu/BBCourse_Production/PhD_Colloquia_C4C/Track_3/phd_t3_u06s6_qualanalysis.html
- Carcary, M. (2020). The research audit trail: Methodological guidance for application in practice. *Electronic Journal of Business Research Methods*, 18(2). <https://doi.org/10.34190/jbrm.18.2.008>
- Caulfield, J. (2019). *How to do thematic analysis*. Scribbr. <https://www.scribbr.com/methodology/thematic-analysis/>
- Chakravarty, S., & Varma, P. (2020). Feature Selection and Evaluation of Permission-based Android Malware Detection. *2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184)*, 795–799. <https://doi.org/10.1109/ICOEI48184.2020.9142929>
- Chepin, E. (2021). Robotics: From first-order cybernetics to third-order cybernetics. *Procedia Computer Science*, 190, 130–136. <https://doi.org/10.1016/j.procs.2021.06.016>
- Chigbu, U. E. (2019). Visually hypothesising in scientific paper writing: Confirming and refuting qualitative research hypotheses using diagrams. *Publications*, 7(1), 22.

<https://doi.org/10.3390/publications7010022>

Chuang, L.-W., Chiu, S.-P., Tian, H.-W., & Wang, L.-S. (2020). Investigating Consumer Behavioral Intention in Smart Technology Context. *2020 IEEE International Conference on Consumer Electronics - Taiwan (ICCE-Taiwan)*, 1–2.

<https://doi.org/10.1109/ICCE-Taiwan49838.2020.9258165>

CISOMAG. (2020). AI-powered cybersecurity: From automated threat detection to adaptive defense. CISO MAG | Cyber Security Magazine.

<https://cisomag.eccouncil.org/ai-in-cybersecurity>

Claudinei Morin, d. S., Rafael, T., Robson de, O. A., Georges, D. A. N., Gildásio Antonio de Oliveira Júnior, J., Orozco, A. L. S., & García Villalba, L. J. (2020). Methodology for forensics data reconstruction on mobile devices with Android operating system, applying in-system programming and combination firmware. *Applied Sciences*, 10(12), 4231. <https://doi.org/10.3390/app10124231>

Columbus, L. (2020). *Detecting & stopping bot attacks with better AI*. Forbes.

<https://www.forbes.com/sites/louiscolombus/2020/08/28/detecting--stopping-bot-attacks-with-better-ai/?sh=2bafbcae1410>

Complete Dissertation. (2021). *What is confirmability in qualitative research, and how do we establish it?* <https://www.statisticssolutions.com/what-is-confirmability-in-qualitative-research-and-how-do-we-establish-it/>

Crane, C. (2019). *Compliance*. <https://www.thesslstore.com/blog/10-data-privacy-and-encryption-laws-every-business-needs-to-know/#6-gramm-leach-bliley-act-%E2%80%94-united-states>

- Crawshaw, D. (2021). Everything VPN Is New Again. *Communications of the ACM*, 64(4), 130–134. <https://doi.org/10.1145/3434230>
- Crowe, A. (2020). HTTP or HTTPS? Why you need a secure site. *Search Engine Journal*. <https://www.searchenginejournal.com/technical-seo/http-https-why-secure-sitecrow>
- Cybersecurity & Communications Integrated Cell. (2024). Multi-factor authentication (MFA): A critical step for account security. Nj.gov. <https://www.cyber.nj.gov/guidance-and-best-practices/account-security/multi-factor-authentication/multi-factor-authentication-mfa-a-critical-step-for-account-security>
- Cybersecurity and Infrastructure Security Agency. (2019). *Information sharing and awareness*. <https://www.cisa.gov/information-sharing-and-awareness>
- Cybersecurity and Infrastructure Security Agency. (2020). *Enterprise VPN security*. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-073a>
- Cybersecurity and Infrastructure Security Agency. (2022a). *Multi-factor authentication (MFA)*. <https://www.cisa.gov/resources-tools/resources/multi-factor-authentication-mfa>
- Cybersecurity and Infrastructure Security Agency. (2022b). *Shields up*. <https://www.cisa.gov/shields-up>
- Cybersecurity and Infrastructure Security Agency. (2024). *Multifactor authentication*. <https://www.cisa.gov/topics/cybersecurity-best-practices/multifactor-authentication>

Cybersecurity and Infrastructure Security Agency. (2025). *Why a strong password isn't enough: Your guide to multifactor authentication.*

<https://www.cisa.gov/resources-tools/training/why-strong-password-isnt-enough-your-guide-multifactor-authentication>

D'Agostino, M., Schwester, R., Carrizale, T., & Melitsk, J. (2019). *CUNY Academic Works CUNY Academic Works A study of e-government and e-governance: an empirical A study of e-government and e-governance: an empirical examination of municipal websites examination of municipal websites.*

https://academicworks.cuny.edu/cgi/viewcontent.cgi?article=1298&context=jj_pubs

Dahlstrom, M. F. (2021). The narrative truth about scientific misinformation.

Proceedings of the National Academy of Sciences, 118(15), Article e1914085117.

<https://doi.org/10.1073/pnas.1914085117>

Damen, A. (2021). *Fintech vs traditional banks: Competition or collaboration?* MONEI.

<https://monei.com/blog/fintech-vs-traditional-banks/>

Damyantov, M. (2023). *What is data saturation in qualitative research?* Dovetail.com.

<https://dovetail.com/research/data-saturation/>

Dhirani, L. L., Mukhtiar, N., Chowdhry, B. S., & Newe, T. (2023). Ethical dilemmas and privacy issues in emerging technologies: A review. *Sensors*, 23(3), Article 1151.

<https://doi.org/10.3390/s23031151>

Dinapoli, T. (2021). *New York State Comptroller Local Government Management Guide Information Technology Governance.* <https://www.osc.state.ny.us/files/local->

[government/publications/pdf/information-technology-governance.pdf](#)

- Dinh, N., & Ogiela, L. (2022). Human-artificial intelligence approaches for secure analysis in CAPTCHA codes. *EURASIP Journal on Information Security*, 2022(1). <https://doi.org/10.1186/s13635-022-00134-9>
- Donevski, M., & Zia, T. (2022). Cyber diversity index for sustainable self-control of machines. *Cybernetics and Systems*, 1–27.
<https://doi.org/10.1080/01969722.2022.2081896>
- Drexel University. (2021). Role of Artificial Intelligence in Cybersecurity. College of Computing & Informatics. <https://drexel.edu/cci/stories/role-of-AI-in-cybersecurity/#:~:text=The%20role%20of%20AI%20in>
- Edwards, D. (1998). *Types of Case Study Work: A Conceptual Framework for Case-Based Research*. ResearchGate.
https://www.researchgate.net/publication/38415151_Types_of_Case_Study_Work_A_Conceptual_Framework_for_Case-Based_Research
- Elifoglu, I. H., Abel, I., & Taşseven, Ö. (2018). Minimizing insider threat risk with behavioral monitoring. *Review of Business*, 38(2), 61-73.
- Farrar, J., Hausserman, C., & Pinto, O. (2020). Trust and compliance effects of taxpayer identity theft: A moderated mediation analysis. *Journal of the American Taxation Association*, 42(1), 57–77. <https://doi.org/10.2308/atax-52404>
- Fearon, D. (2023). *Guides: Qualitative Data Analysis Software (nVivo, Atlas.TI, and more): Qualitative Data Analysis Software (QDAS) overview*. Guides.library.jhu.edu. <https://guides.library.jhu.edu/QDAS>

Federal Bureau of Investigation. (2023). *Internet crime report*.

https://www.ic3.gov/annualreport/reports/2023_ic3report.pdf

Federal Deposit Insurance Corporation. (2022). *Cybersecurity*.

<https://www.fdic.gov/resources/consumers/consumer-assistance-topics/cybersecurity.html>

Federal Deposit Insurance Corporation. (2012). *Mobile payments: An evolving landscape*
– *Winter 2012 Vol. 9, Issue 2*.

<https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin12/siwin12-2012-article01.html>

Federal Trade Commission. (2021a). *How to safely use public Wi-Fi networks*. *Consumer Information*. <https://consumer.ftc.gov/articles/how-safely-use-public-wi-fi-networks>

Federal Trade Commission. (2021b). *Virtual private network (VPN) apps on mobile devices*. *Consumer advice*. <https://consumer.ftc.gov/articles/virtual-private-network-vpn-apps-mobile-devices>

Federal Trade Commission. (2024). *FTC Safeguards Rule: What Your Business Needs to Know*. Federal Trade Commission. <https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know>

Frankenfield, J. (2023). *What is the Turing Test?* Investopedia.

<https://www.investopedia.com/terms/t/turing-test.asp>

Franklin, J. (2019). *Mobile Device Security*. Nist.gov.

<https://www.nccoe.nist.gov/publication/1800-4/VoIB/>

- Franklin, J. M., Howell, G., Boeckl, K., Lefkovitz, N., Nadeau, E., Shariati, B., Ajmo, J. G., Brown, C. J., Dog, S. E., Javar, F., Peck, M., & Sandlin, K. F. (2020). Mobile Device Security: Corporate-Owned Personally-Enabled (COPE). *NIST SPECIAL PUBLICATION 1800-21*. <https://doi.org/10.6028/nist.sp.1800-21>
- Fusch, P., Fusch, G. E., & Ness, L. R. (2018). Denzin's paradigm shift: Revisiting triangulation in qualitative research. *Journal of Social Change, 10*(1), 19–32. <https://doi.org/10.5590/JOSC.2018.10.1.02>
- Galauner, B. (2021). *Pfeiffer Library: Research Methodologies: What are research methods?* Library.tiffin.edu. <https://library.tiffin.edu/researchmethodologies/whatareresearchmethods>
- Gasnick, R. (2023). *Best Practices for Multi-Factor Authentication (MFA)*. Miles IT Company. <https://www.milesit.com/mfa-best-practices/>
- Geckeler, I. (2020). *The Cybernetic Loop: Cheat Codes For Life*. Medium. <https://medium.com/@iangeckeler/the-cybernetic-loop-cheat-codes-for-life-abdfae08ca00>
- Gelles-Watnick, R. (2024). *Americans' Use of Mobile Technology and Home Broadband*. Pew Research Center: Internet, Science & Tech. <https://www.pewresearch.org/internet/2024/01/31/americans-use-of-mobile-technology-and-home-broadband/#:~:text=In%20a%20far%20cry%20from>
- George, T. (2021). *Mixed methods research | Definition, guide & examples*. scribbr.com: <https://www.scribbr.com/methodology/mixed-methods-research/>
- George, T. (2022). *Semi-Structured Interview | Definition, Guide & Examples*. Scribbr.

<https://www.scribbr.com/methodology/semi-structured-interview/>

George, T. (2023). *An Introduction to Mixed Methods Research*. Scribbr.

<https://www.scribbr.com/methodology/mixed-methods-research/>

Georgia State University Library. (2021). *NVivo qualitative data analysis software:*

NVivo - What is it? research.library.gsu.edu/nvivo:

<https://research.library.gsu.edu/nvivo>

Gomes, V., Reis, J., & Alturas, B. (2020). Social Engineering and the Dangers of

Phishing. *2020 15th Iberian Conference on Information Systems and*

Technologies (CISTI), Information Systems and Technologies (CISTI), 2020 15th

Iberian Conference On, 1–7. <https://doi.org/10.23919/CISTI49556.2020.9140445>

Gontovnikas, M. (2021). The 9 Most Common Security Threats to Mobile Devices in

2021. Auth0 - Blog. [https://auth0.com/blog/the-9-most-common-security-threats-](https://auth0.com/blog/the-9-most-common-security-threats-to-mobile-devices-in-2021/)

[to-mobile-devices-in-2021/](https://auth0.com/blog/the-9-most-common-security-threats-to-mobile-devices-in-2021/)

Goodman, C. (2019). *Using artificial intelligence in cybersecurity*. Balbix.

[https://www.balbix.com/insights/artificial-intelligence-in-](https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/#:~:text=Breach%20Risk%20Prediction%20%E2%80%93%20Accounting%20for)

[cybersecurity/#:~:text=Breach%20Risk%20Prediction%20%E2%80%93%20Acc](https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/#:~:text=Breach%20Risk%20Prediction%20%E2%80%93%20Accounting%20for)

[ounting%20for](https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/#:~:text=Breach%20Risk%20Prediction%20%E2%80%93%20Accounting%20for)

Grevtseva, G. Y., Mulvukova, A. G., Balikaeva, M. B., Shumilova, E. A., & Ignatkin, A.

N. (2019). *The Cybernetic Approach as the Digital Competence of the Future*

Electronics Engineers. IEEE Xplore.

<https://doi.org/10.1109/ITQMIS.2019.8928353>

Hai Thanh Luong. (2023). Foundations and trends in the darknet-related criminals in the

last 10 years: a systematic literature review and bibliometric analysis. *Security Journal*. <https://doi.org/10.1057/s41284-023-00383-4>

Harris, K. (n.d.). *Academic Guides: Capstone Documents: DBA Capstone: Traditional Capstone Options*. Academicguides.waldenu.edu.

<https://academicguides.waldenu.edu/research-center/program-documents/dba/traditional-capstone-options>

Hayes, D., Cappa, F., & Le-Khac, N. A. (2020). An effective approach to mobile device management: Security and privacy issues associated with mobile applications.

Digital Business, 1(1), 100001. <https://doi.org/10.1016/j.digbus.2020.100001>

Helfferrich, C. (2019). *Die Qualität Qualitativer Daten: Manual für die Durchführung von qualitativen Interviews*. Wiesbaden: VS Verlag. Chapter 5.2.

Hennink, M., & Kaiser, B. N. (2021). Sample Sizes for Saturation in Qualitative research: a Systematic Review of Empirical Tests. *Social Science & Medicine*, 292,

114523. <https://doi.org/10.1016/j.socscimed.2021.114523>

Hill, M. (2022). *8 notable open-source security initiatives of 2022*. CSO Online.

<https://www.csoonline.com/article/3673089/8-notable-open-source-security-initiatives-of-2022.html>

Hitaj, D., Hitaj, B., Jajodia, S., & Mancini, L. V. (2021). Capture the Bot: Using

Adversarial Examples to Improve CAPTCHA Robustness to Bot Attacks. *IEEE Intelligent Systems, IEEE, IEEE Intell. Syst*, 36(5), 104–112.

<https://doi.org/10.1109/MIS.2020.3036156>

Holtrop, J. S., & Glasgow, R. E. (2020). Pragmatic research: an introduction for clinical

practitioners. *Family Practice*, 37(3), 424–428.

<https://doi.org/10.1093/fampra/cmz092>

Hoover, L. (2021). *5 Qualitative Research Designs and Research Methods*. GCU.

<https://www.gcu.edu/blog/doctoral-journey/5-qualitative-research-designs-and-research-methods>

House Subcommittee on Cybersecurity. (2023). *Mace: We must have reliable safeguards against malicious cyber activity*. United States House Committee on Oversight

and Accountability. [https://oversight.house.gov/release/mace-we-must-have-reliable-safeguards-against-malicious-cyber-](https://oversight.house.gov/release/mace-we-must-have-reliable-safeguards-against-malicious-cyber-activity%EF%BF%BC/#:~:text=The%20Council%20of%20Economic%20Advisors)

[reliable-safeguards-against-malicious-cyber-](https://oversight.house.gov/release/mace-we-must-have-reliable-safeguards-against-malicious-cyber-activity%EF%BF%BC/#:~:text=The%20Council%20of%20Economic%20Advisors)

[activity%EF%BF%BC/#:~:text=The%20Council%20of%20Economic%20Advisors](https://oversight.house.gov/release/mace-we-must-have-reliable-safeguards-against-malicious-cyber-activity%EF%BF%BC/#:~:text=The%20Council%20of%20Economic%20Advisors)

Hu, V. (2022). *Blockchain for Access Control Systems*. Csrc.nist.gov.

<https://csrc.nist.gov/publications/detail/nistir/8403/final>

Hudson, J. (2022). *The Synergy of Cloud Computing and Cybersecurity: Ensuring Device*

Protection and Data Integrity. <https://doi.org/10.13140/RG.2.2.30312.99847>

Huffman, L. (2020). *Credit Card CVV Number: What is it and How to Find It?* Forbes

Advisor. <https://www.forbes.com/advisor/credit-cards/what-is-a-credit-card-cvv-number/>

IBM. (2019). *X-Force threat intelligence index*.

<https://www.securindex.com/downloads/8b9f94c46a70c60b229b04609c07acff.pdf>

IBM. (2024). *Cost of a data breach report 2024*. IBM.

<https://www.ibm.com/reports/data-breach>

IBM. (2025). *IBM X-Force 2025 Threat Intelligence Index*. IBM.

<https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/2025-threat-intelligence-index>

Intel. (2021). What Is a Trusted Platform Module (TPM) Intel?

<https://www.intel.com/content/www/us/en/business/enterprise-computers/resources/trusted-platform-module.html>

Introspective Market Research. (2025). *Multi-Factor Authentication (MFA) Market Trends and Challenges*. Introspective Market Research.

<https://introspectivemarketresearch.com/reports/multifactor-authentication-mfa-market/>

iProov. (2021). *The Disadvantages and Problems with Passwords* | iProov.

Www.iproov.com. <https://www.iproov.com/blog/forgotten-passwords-increasing-websites-abandonment-rate>

IRS. (2024). *Multi-factor authentication: Key protection to tax professionals' security arsenal now required* | Internal Revenue Service. Irs.gov.

<https://www.irs.gov/newsroom/multi-factor-authentication-key-protection-to-tax-professionals-security-arsenal-now-required>

ISC2. (2023). *#CybersecurityAwarenessMonth - Multifactor Authentication (MFA): Enhancing Digital Security*. Wwww.isc2.org.

<https://www.isc2.org/Insights/2023/10/Cybersecurity-Awareness-Month-Multifactor-Authentication>

ISC2. (2025). *Educating the Workforce About Cybersecurity*. Isc2.org.

<https://www.isc2.org/insights/2025/06/educating-the-workforce-about-cybersecurity?queryID=721c4b8f4b2e322ffe5c736b006c67d7>

IT Governance. (2025). *Compliance | IT Governance USA*. Wwww.itgovernanceusa.com.

<https://www.itgovernanceusa.com/compliance>

Iwuozor, J. (2021). Whitelisting vs. Blacklisting: Which Is Better? ESecurityPlanet.

<https://www.esecurityplanet.com/applications/whitelisting-vs-blacklisting-which-is-better/>

Jain, P. (2021). *Encryption: A Tradeoff Between User Privacy and National Security*.

American University. <https://www.american.edu/sis/centers/security-technology/encryption.cfm>

Jakubik, M. (2021). *Interplay between cybernetics and philosophy as an essential condition for learning*. 19. 79-97.

https://www.researchgate.net/publication/353546868_Interplay_Between_Cybernetics_and_Philosophy_as_an_Essential_Condition_for_Learning

Jiang, Z., Zhao, K., Li, R., Zhao, J., & Junzhao, D. (2020). PHYAlert: identity spoofing attack detection and prevention for a wireless edge network. *J Cloud Comp* 9, 5.

<https://doi.org/10.1186/s13677-020-0154-7>

Johnson, J. L., Adkins, D., & Chauvin, S. (2020). A Review of the Quality Indicators of

Rigor in Qualitative Research. *American journal of pharmaceutical education*, 84(1), 7120. <https://doi.org/10.5688/ajpe7120>

Karaymeh, A., Ababneh, M., Qasaimeh, M., & Al-Fayoumi, M. (2019). Enhancing Data

Protection Provided by VPN Connections over Open WiFi Networks. 2019 2nd International Conference on New Trends in Computing Sciences (ICTCS), Trends in Computing Sciences (ICTCS), 2019 2nd International Conference on New, 1–6. <https://doi.org/10.1109/ICTCS.2019.8923104>

Karjaluoto, H., Shaikh, A. A., Saarijärvi, H., & Saraniemi, S. (2019). How perceived value drives the use of mobile financial services apps, *International Journal of Information Management*, 47, 252-261.

<https://doi.org/10.1016/j.ijinfomgt.2018.08.014>

Kaspersky. (2020). *AI and Machine Learning in Cybersecurity — How They Will Shape the Future*. www.kaspersky.com. <https://www.kaspersky.com/resource-center/definitions/ai-cybersecurity>

Kaspersky Lab. (2017). Kaspersky Lab survey: One-in-four hide cybersecurity incidents from their employers. Business Wire (English).

https://usa.kaspersky.com/about/press-releases/2017_kaspersky-lab-survey-one-in-four-hide-cybersecurity-incidents-from-their-employers

Kassner, M. (2020). Cybersecurity pros: Are humans really the weakest link?

TechRepublic. <https://www.techrepublic.com/article/cybersecurity-pros-are-humans-really-the-weakest-link/>

Kastberg, P. (2020). Modelling the reciprocal dynamics of dialogical communication: On the communication-philosophical undercurrent of radical constructivism and second-order cybernetics. *Sign Systems Studies*, 48(1), 32–55.

<https://doi.org/10.12697/SSS.2020.48.1.03>

- Kaushik, V., & Walsh, C. A. (2019). Pragmatism as a Research Paradigm and Its Implications for Social Work Research. *Social Sciences*, 8(9). MDPI.
<https://doi.org/10.3390/socsci8090255>
- Kaviani, F., Robards, B., Young, K. L., & Koppel, S. (2020). Nomophobia: Is the fear of being without a smartphone associated with problematic use? *International Journal of Environmental Research and Public Health*, 17(17), 6024.
<https://doi.org/10.3390/ijerph17176024>
- Kontesoy, K. (2022). *What is the difference between HSM and TSM? | Teleport*. Goteleport.com. <https://goteleport.com/blog/tpm-vs-hsm-difference/>
- Kovalchuk, S. V., Kopanitsa, G. D., Derevitskii, I. V., Matveev, G. A., & Savitskaya, D. A. (2022). Three-stage intelligent support of clinical decision making for higher trust, validity, and explainability. *Journal of Biomedical Informatics*, 127, 104013. <https://doi.org/10.1016/j.jbi.2022.104013>
- Kristel, R., A.-F., & Saunders, C. (2024). The whole of cyber defense: Syncing practice and theory. *The Journal of Strategic Information Systems*, 33(4), 101861–101861.
<https://doi.org/10.1016/j.jsis.2024.101861>
- Kushal, A., & Arun, M. (2017). Relation between cybernetics and information security: from Norbert Wiener’s perspectives. *Kybernetes*, 46(10), 1654–1673.
<https://doi.org/10.1108/K-04-2017-0129>
- LaConte, C. (2019). *The challenges of multi-factor authentication in your security program*. ITProPortal. <https://www.itproportal.com/features/the-challenges-of-multi-factor-authentication-in-your-security-program/>

- Lebeaux, B. (2023). *Preparing for the New PCI DSS 4.0 MFA Requirements* | RSA Blog. RSA. <https://www.rsa.com/resources/blog/multi-factor-authentication/preparing-for-the-new-pci-dss-4-0-mfa-requirements/>
- Legrand, J. (2022). *Humans and Cybersecurity— The Weakest Link or the Best Defense?* ISACA. <https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/humans-and-cybersecurity-the-weakest-link-or-the-best-defense>
- Lewis, B. (n.d.). *Information Warfare*. Irp.fas.org. <https://irp.fas.org/eprint/snyder/infowarfare.htm>
- Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cybersecurity; emerging trends and recent developments. *Energy Reports*, 7(7), 8176–8186. Sciencedirect. <https://doi.org/10.1016/j.egy.2021.08.126>
- Li, Y., Xiong, K., & Li, X. (2019). Understanding User Behaviors When Phishing Attacks Occur. *2019 IEEE International Conference on Intelligence and Security Informatics (ISI), Intelligence and Security Informatics (ISI), 2019 IEEE International Conference On*, 222. <https://doi.org/10.1109/ISI.2019.8823468>
- Lord, N. (2019). What is data encryption? Definition, best practices & more. digitalguardian.com: <https://digitalguardian.com/blog/what-data-encryption>
- Loshkarev, A. V. (2021). Cybernetic control model: Doctrine, practice, technology. *The European Proceedings of Social & Behavioural Sciences*. <https://doi.org/10.15405/epsbs.2021.04.02.119>
- Luft, J. A., Jeong, S., Idsardi, R., & Gardner, G. (2022). Literature reviews, theoretical frameworks, and conceptual frameworks: An introduction for new biology

education Researchers. *CBE—Life Sciences Education*, 21(3).

<https://doi.org/10.1187/cbe.21-05-0134>

Luna, C., de la. (2024). *What is Cybersecurity Automation? Benefits and Challenges*.

ESecurity Planet. <https://www.esecurityplanet.com/networks/automation-in-cyber-security/>

Maciej, B., Imed, E. F., & Kurkowski, M. (2019). Multifactor Authentication Protocol in a Mobile Environment. *IEEE Access*, 7, 157185–157199.

<https://doi.org/10.1109/ACCESS.2019.2948922>

Mahon, D. (2021). *For Today's CISO, It's All About Incident Response and Resilience*.

Memberclicks.net.

https://isma1.memberclicks.net/index.php?option=com_dailyplanetblog&view=entry&category=cyber-security&id=6:for-today-s-ciso-it-s-all-about-incident-response-and-resilience

Marginingsih, R., Widiyanti, W., Susilowati, I. H., Retnowulan, J., & Soraya, I. (2019).

Mobile payment as financial transactions in the digital era: An empirical analysis.

IOP Conference Series: Materials Science & Engineering, 662(2), 1.

Mayer, R. V. (2021). Development of Information-Cybernetic Thinking in Students of

Pedagogical Universities. *Education Sciences & Psychology*, 60(3), 54–60.

Mayr, H. C., & Thalheim, B. (2021). The triptych of conceptual modeling. *Softw Syst*

Model 20, 7–24. <https://doi.org/10.1007/s10270-020-00836-z>

McCombes, S. (2019a). *How to Do a Case Study*. Scribbr.

<https://www.scribbr.com/methodology/case-study/>

McCombes, S. (2019b). *Sampling Methods | Types and Techniques Explained*. Scribbr.

<https://www.scribbr.com/methodology/sampling-methods/>

McCombes, S. (2019c). *What is a case study? | definition, examples & methods*. Scribbr.

<https://www.scribbr.com/methodology/case-study/>

McCue, T. J. (2019). *Is your mobile banking app secure? Three tips to stay safe*.

forbes.com: <https://www.forbes.com/sites/tjmccue/2019/08/30/is-your-mobile-banking-app-secure-three-tips-to-stay-safe/#4918f86c16c2>

McLennan, A. (2022). *What can cybernetics and a toaster teach us about cybersecurity and AI?* ANU School of Cybernetics.

<https://cybernetics.anu.edu.au/news/2022/07/12/what-can-cybernetics-and-a-toaster-teach-us-about-cyber-security-and-ai/>

McNiff, K. (2022). *Data Analysis Software Blog | NVivo*. Wwww.qsrinternational.com.

<https://www.qsrinternational.com/nvivo-qualitative-data-analysis-software/resources/blog/thematic-analysis-of-interview-data-nvivo>

Microsoft. (2022). *Trusted Platform Module Technology Overview (Windows 10)* -

Microsoft 365 Security. Docs.microsoft.com. <https://docs.microsoft.com/en-us/windows/security/information-protection/tpm/trusted-platform-module-overview>

Microsoft Ignite. (2025). *OATH tokens authentication method - Microsoft Entra ID*.

Microsoft.com. <https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-oath-tokens>

Middleton, F. (2019). *Reliability vs Validity in Research | Differences, Types and*

Examples. Scribbr. <https://www.scribbr.com/methodology/reliability-vs-validity>

Mishra, P., Pandey, C. M., Singh, U., Keshri, A., & Sabaretnam, M. (2019). Selection of Appropriate Statistical Methods for Data Analysis. *Annals of Cardiac Anaesthesia*, 22(3), 297–301. NCBI. https://doi.org/10.4103/aca.ACA_248_18

Mitra, M. (2019). *Advances in Cybernetics Technology*. 1. 1-3.

<http://doi.org/10.31031/COJEC.2018.01.000519>

Morgan, D. L., & Nica, A. (2020). Iterative Thematic Inquiry: A New Method for Analyzing Qualitative Data. *International Journal of Qualitative Methods*, 19, 1–11. <https://doi.org/10.1177/1609406920955118>

Morris, M., & Rumph, J. (2020). *It's not a short list: Financial institution ISO roles and responsibilities*. <https://www.wipfli.com/insights/articles/fi-ra-information-security-officer-responsibilities>

Moser, A., & Korstjens, I. (2023). Series: Practical guidance to qualitative research. Part 7: Qualitative evidence synthesis for emerging themes in primary care research: Scoping review, meta-ethnography and rapid realist review. *European Journal of General Practice*, 29(1). <https://doi.org/10.1080/13814788.2023.2274467>

Müller, K. H. (2018). Second-Order Science and New Cybernetics. *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, 625–655. https://doi.org/10.1007/978-3-319-09069-6_15

My Dissertation Coach. (2020). *What is transferability in qualitative research?* My Dissertation Coach. <https://mydissertation.coach/q-and-a/what-is-transferability-in-qualitative-research>

- Nagai, H., Nakazawa, E., & Akabayashi, A. (2022). The creation of the Belmont Report and its effect on ethical principles: a historical study. *Monash Bioethics Review*, 40(2). <https://doi.org/10.1007/s40592-022-00165-5>
- Najshahid. (2025). *Plan for mandatory Microsoft Entra multifactor authentication (MFA) - Microsoft Entra ID*. Microsoft.com. <https://learn.microsoft.com/en-us/entra/identity/authentication/concept-mandatory-multifactor-authentication?tabs=dotnet>
- National Cybersecurity Alliance. (2024). *How Cyber Education for Employees Safeguards Your Business - National Cybersecurity Alliance*. Staysafeonline.org. <https://www.staysafeonline.org/articles/how-cyber-education-for-employees-safeguards-your-business>
- National Institute of Standards and Technology. (2020a). *Automation support for security control assessments: Software vulnerability management*. NIST, 4 (NISTIR 8011). U.S. Department of Commerce. <https://www.nist.gov/news-events/news/2020/04/automation-support-security-control-assessments-software-vulnerability>
- National Institute of Standards and Technology. (2020b). *Completely automated public Turing test to tell computers and humans apart (CAPTCHA)*. U.S. Department of Commerce. https://csrc.nist.gov/glossary/term/Completely_Automated_Public_Turing_test_to_tell_Computers_and_Humans_Apart
- National Institute of Standards and Technology. (2023). *Is your cybersecurity strategy falling victim to these 6 common pitfalls?* U.S. Department of Commerce.

<https://www.nist.gov/news-events/news/2023/03/your-cybersecurity-strategy-falling-victim-these-6-common-pitfalls>

National Security Agency. (2020). *Securing IPsec Virtual Private Networks*.

<https://media.defense.gov/2021/Sep/16/2002855930/-1/->

[1/0/SECURING_IPSEC_VIRTUAL_PRIVATE_NETWORKS_EXECUTIVE_SUMMARY_2020_07_01_FINAL_RELEASE.PDF](#)

Neubauer, B., Witkop, C., & Varpio, L. (2019). How Phenomenology Can Help Us Learn from the Experiences of Others. *Perspectives on Medical Education*, 8(2), 90–97.

NCBI. <https://doi.org/10.1007/s40037-019-0509-2>

New Jersey Cybersecurity & Communications. (2025). *MFA, VPNs, & Firewalls*. Nj.gov.

<https://www.cyber.nj.gov/guidance-and-best-practices/back-to-basics/identity-and-access-management-patch-management/mfa-vpns-firewalls>

Nikolopoulou, K. (2022). *What is purposive sampling? | definition & examples*. Scribbr.

<https://www.scribbr.com/methodology/purposive-sampling/>

Noble, H., & Heale, R. (2019). Triangulation in Research. *Evidence-Based Nursing*,

22(3), 67–68. <https://doi.org/10.1136/ebnurs-2019-103145>

Noor, A. (2020). FIDO: Fast IDentity Online. *ISSA Journal*, 18(12), 22–26.

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis.

International Journal of Qualitative Methods, 16(1), 160940691773384.

<https://doi.org/10.1177/1609406917733847>

Olobia, L. (2021). *Implications of Social Cybernetics Theory of*

Communication. *Global Scientific Journal (GSJ)* 9(12),

https://www.globalscientificjournal.com/researchpaper/Smith_s_Social_Cybernetic_Strategies_for_Asynchronous_Learning_Implications_of_Social_Cybernetics_Theory_of_Communication.pdf

Ozkan, C., & Bicakci, K. (2020). Security Analysis of Mobile Authenticator Applications. 2020 International Conference on Information Security and Cryptology (ISCTURKEY), Information Security and Cryptology (ISCTURKEY), 2020 International Conference On, 18–30.

<https://doi.org/10.1109/ISCTURKEY51113.2020.9308020>

Panagia, D. (2021). On the Possibilities of a Political Theory of Algorithms. *Political Theory*, 49(1), 109–133. <https://doi.org/10.1177/0090591720959853>

Pannucci, C. J., & Wilkins, E. G. (2011). Identifying and Avoiding Bias in Research. *Plastic and Reconstructive Surgery*, 126(2), 619–625.

<https://doi.org/10.1097/prs.0b013e3181de24bc>

Patel, A. (2019). *Humans Are IT Security's Weakest Link*. ISACA.

<https://www.isaca.org/resources/news-and-trends/industry-news/2024/humans-are-it-securitys-weakest-link>

Patzia, M. (n.d.). *Anaxagoras* | *Internet Encyclopedia of Philosophy*. Internet Encyclopedia of Philosophy.

<https://iep.utm.edu/anaxagoras/#:~:text=Most%20commentators%20maintain%20that%20Anaxagoras>

Pazarbasioglu, C., Mora, A., Uttamchandani, M., Natarajan, H., Feyen, E., & Saal, M. (2020). Digital Financial Services.

<https://pubdocs.worldbank.org/en/230281588169110691/Digital-Financial-Services.pdf>

PCI Compliance Guide. (2020). PCI compliance guide.

<https://www.pcicomplianceguide.org/faq/#1>

Peña-Ayala, A., & Cárdenas-Robledo, L. A. (2019). A cybernetic method to regulate learning through learning strategies: A proactive and reactive mechanism applied in U–Learning settings. *Computers in Human Behavior*, 98, 196–209.

<https://doi.org/10.1016/j.chb.2019.03.036>

Peng, Z., Rathod, P., Niu, N., Bhowmik, T., Liu, H., Shi, L., & Jin, Z. (2022). Testing software’s changing features with environment-driven abstraction identification. *Requirements Engineering*, 27(4), 405–427. [https://doi.org/10.1007/s00766-022-](https://doi.org/10.1007/s00766-022-00390-8)

[00390-8](https://doi.org/10.1007/s00766-022-00390-8)

Peters, G. C. (2022). *Text - S.3600 - 117th Congress (2021-2022): Strengthening American Cybersecurity Act of 2022*. [Www.congress.gov](http://www.congress.gov).

<https://www.congress.gov/bill/117th-congress/senate-bill/3600/text>

Petrosyan, A. (2023). *Global cybercrime estimated cost 2028*. Statista.

<https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide>

Pew Research Center. (2019). *Are Americans Embracing Mobile Payments?*

[Pewtrusts.org. https://www.pewtrusts.org/en/research-and-analysis/issue-briefs/2019/10/are-americans-embracing-mobile-payments](https://www.pewtrusts.org/en/research-and-analysis/issue-briefs/2019/10/are-americans-embracing-mobile-payments)

Pew Research Center. (2021). *Mobile Fact Sheet*. Pew Research Center: Internet, Science & Tech; Pew Research Center. <https://www.pewresearch.org/internet/fact->

[sheet/mobile/](#)

Pew Research Center. (2024). *Mobile fact sheet*.

<https://www.pewresearch.org/internet/fact-sheet/mobile/>

Pezalla, A. E., Pettigrew, J., & Miller-Day, M. (2012). Researching the researcher-as-instrument: an exercise in interviewer self-reflexivity. *Qualitative research: QR*, 12(2), 165–185. <https://doi.org/10.1177/1487941111422107>

Pfeifer, M. A., & Dolan, E. L. (2023). Venturing into Qualitative Research: A Practical Guide to Getting Started. *Scholarship and Practice of Undergraduate Research*, 7(1), 10–20. <https://doi.org/10.18833/spur/7/1/2>

Picton, C. J., Moxham, L., & Patterson, C. (2017). The use of phenomenology in mental health nursing research. *Nurse Researcher*, 25(3), 14.

<https://doi.org/10.7748/nr.2017.e1513>

Popa, E. V. (2022). The Use of Cybernetic Systems Based on Artificial Intelligence as Support for the Decision-Making Process in the Military Field. *Revista Academiei Fortelor Terestre*, 27(4), 386–393. <https://doi.org/10.2478/raft-2022-0047>

Popovic, A., & Huecker, M. R. (2024). *Study Bias*. PubMed; StatPearls Publishing.

<https://www.ncbi.nlm.nih.gov/books/NBK574513/#:~:text=In%20academic%20research%2C%20bias%20refers>

Proctor, D. (2021). Cybernetics and Digital Whiteness: Exposure to Radicalization through Feedback Loops. *2021 IEEE Conference on Norbert Wiener in the 21st Century (21CW), Norbert Wiener in the 21st Century (21CW), 2021 IEEE*

- Conference On*, 1–5. <https://doi.org/10.1109/21CW48944.2021.9532566>
- Purdue University. (2019). *Important considerations for protecting human research participants*. <https://www.purdue.edu/research/dimensions/important-considerations-for-protecting-human-research-participants>
- Rahimi, S., & Khatooni, M. (2024). Saturation in Qualitative research: an Evolutionary Concept Analysis. *International Journal of Nursing Studies Advances*, 6(1), 100174. <https://doi.org/10.1016/j.ijnsa.2024.100174>
- Ramanadhan, S., Revette, A. C., Lee, R. M., & Aveling, E. L. (2021). Pragmatic approaches to analyzing qualitative data for implementation science: an introduction. *Implementation Science Communications*, 2(1). <https://doi.org/10.1186/s43058-021-00174-1>
- Raza, M. (2020). *The Chief Information Security Officer (CISO) Role Explained*. BMC Blogs. <https://www.bmc.com/blogs/ciso-chief-information-security-officer/>
- Rezk, S. S., & Gamal, S. (2020). An Organizational Cybernetics Framework for Designing a Viable Higher Education System. *Systemic Practice & Action Research*, 33(6), 703–724. <https://doi.org/10.1007/s11213-019-09505-9>
- Richardson, K. E. (2024). *How Has Technology Changed Education?* Purdue University College of Education. <https://education.purdue.edu/2024/01/how-has-technology-changed-education/>
- Roberts, A. K. (2019). *Important considerations for protecting human research participants*. Dimensions of Discovery. <https://www.purdue.edu/research/dimensions/important-considerations-for->

[protecting-human-research-participants/](#)

Rodeck, D. (2021). What Is Blockchain? Forbes Advisor.

<https://www.forbes.com/advisor/investing/cryptocurrency/what-is-blockchain/>

Rooney, M. J., Levy, Y., Li, W., & Kumar, A. (2024). Comparing experts' and users' perspectives on the use of password workarounds and the risk of data breaches.

Information and Computer Security, 33(12). <https://doi.org/10.1108/ics-05-2024-0116>

Rosenkranz, C., & Holten, R. (2007). Combining cybernetics and conceptual modeling.

Proceedings of the 2007 ACM Symposium: Applied Computing, 1228–1233.

<https://doi.org/10.1145/1244002.1244269>

Rouse, M. (2019). *Mobile device management (MDM)*.

<https://searchmobilecomputing.techtarget.com/definition/mobile-device-management>

Russell, A. (2020). What is HTTPS?. <https://www.ssl.com/faqs/what-is-https>

Rutgers University Libraries. (2021). *Research guides: Systematic reviews in the health sciences: Types of research within qualitative and quantitative*.

Libguides.rutgers.edu. <https://libguides.rutgers.edu/c.php?g=337288&p=2273209>

Salahdine, F., & Kaabouch, M. (2019). Social Engineering Attacks: A Survey. *Future Internet*, 11(4), 89. <https://doi.org/10.3390/fi11040089>

Samojło, G. (2019). *How mobile apps are changing the banking industry: 5 examples*.

<https://www.netguru.com/blog/mobile-apps-in-banking-examples>

Schwaninger, M. (2003). A Cybernetic Model to Enhance Organizational Intelligence.

Systems Analysis Modelling Simulation, 43(1), 53–65.

<https://doi.org/10.1080/02329290290001029>

Schweizer, V., & Lazurko, A. (2020). Cross-impact Balances: A Method for Bridging Social Systems and Cybernetics. *2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Systems, Man, and Cybernetics (SMC), 2020 IEEE International Conference On*, 4486–4492.

<https://doi.org/10.1109/SMC42975.2020.9283480>

ScienceDirect. (2024). *Cybernetics - an overview | ScienceDirect Topics*.

Www.sciencedirect.com. <https://www.sciencedirect.com/topics/social-sciences/cybernetics>

Secure Technology Alliance. (2020). *Secure Technology Alliance 2020, a secure technology alliance payments council white paper, Dynamic Security Code Cards: A Primer*. <https://www.securetechalliance.org/wp-content/uploads/Dynamic-Security-Code-Card-WP-Final-July-2020.pdf>

Security.org Team. (2023). *Credit Card Fraud 2021 Annual Report: Prevalence, Awareness, and Prevention*. Security.org. <https://www.security.org/digital-safety/credit-card-fraud-report/>

Segal, B. (2019). Will dynamic CVVs become the ultimate in credit card security?

<https://www.creditcards.com/credit-card-news/dynamic-cvv-credit-card-security>

Shahriar, H., Zhang, C., Talukder, A., & Islam, S. (2020). Mobile application security using static and dynamic analysis. *Studies in Computational Intelligence*, 443–459. https://doi.org/10.1007/978-3-030-57024-8_20

- Sharma, P. (2019). A contemplate on multifactor authentication. *2019 6th International Conference on Computing for Sustainable Global Development (INDIACom)*, 824–827.
- Sharp, S. (2019). The future of authentication. <https://www.scmagazineuk.com/future>
- Shevlin, R. (2021). *Mobile banking adoption in the United States has skyrocketed (but so have fraud concerns)*. Forbes.
<https://www.forbes.com/sites/ronshevlin/2021/07/29/mobile-banking-adoption-has-skyrocketed-but-so-have-fraud-concerns-what-can-banks-do/?sh=2a4c5bbb5dc6>
- Shillair, R. (2020). Protection Motivation Theory. *The International Encyclopedia of Media Psychology*, 1–3. <https://doi.org/10.1002/9781119011071.iemp0188>
- Silent Circle. (2019). Encryption laws: Legal requirements for sensitive transmissions. <https://www.silenteircle.com/encryption-laws>
- Simon Fraser University. (2022). *Academic writing: What is a literature review?* | SFU Library. www.lib.sfu.ca. <https://www.lib.sfu.ca/about/branches-depts/slc/writing/assignments/lit-review>
- Simplilearn. (2020). *The most effective data encryption techniques*. Simplilearn.com. <https://www.simplilearn.com/data-encryption-methods-article>
- Singh, S. (2023). *What is ethnographic research? Methods and Examples* | *Researcher Life*. Researcher Life. <https://researcher.life/blog/article/what-is-ethnographic-research-methods-and-examples/>
- Sobers, R. (2019). *110 Must-Know Cybersecurity Statistics for 2020*. Inside out Security.

<https://www.varonis.com/blog/cybersecurity-statistics>

Soh, F., & Grover, V. (2020). Effect of release timing of app innovations based on mobile platform innovations. *Journal of Management Information Systems*, 37(4), 957–987. <https://doi.org/10.1080/07421222.2020.1831763>

Solomon, S. (2024). *8 Multi factor authentication types and how to choose*. Frontegg. <https://frontegg.com/blog/multi-factor-authentication-types>

Streefkerk, R. (2019). *Qualitative vs. quantitative research | Definitions, differences & methods*. Scribbr. <https://www.scribbr.com/methodology/qualitative-quantitative-research/>

Substance Abuse and Mental Health Services Administration. (2019). *Enhancing motivation for change in substance use disorder treatment*. U.S. Department of Health and Human Services. https://store.samhsa.gov/sites/default/files/d7/priv/tip35_final_508_compliant_-_02252020_0.pdf

Sulistiyowati, D., Handayani, F., & Suryanto, Y. (2020). Comparative analysis and design of cybersecurity maturity assessment methodology using NIST CSF, COBIT, ISO/IEC 27002, and PCI DSS. *JOIV: International Journal on Informatics Visualization*, 4(4), 225–230. <https://doi.org/10.30630/joiv.4.4.482>

Tamir, M. (2020). Effortful emotion regulation as a unique form of cybernetic control. *Perspectives on Psychological Science*, 16(1), 94–117. <https://doi.org/10.1177/1745691620922199>

Tataroiu, R., Stancu, F. A., & Tranca, D. C. (2019). Energy Considerations regarding

transport layer security in wireless IoT devices. *2019 22nd International Conference on Control Systems and Computer Science (CSCS)*, 337–341.

<https://doi.org/10.1109/CSCS.2019.00060>

Taylor, A. (2022). *There's a huge surge in hackers holding data for ransom, and experts want everyone to take these steps*. Fortune.

<https://fortune.com/2022/02/17/ransomware-attacks-surge-2021-report/>

Theofanidis, D., & Fountouki, A. (2019). Limitations and delimitations in the research process. *Perioperative Nursing (GORNA)*, 7(3), 155–162.

<http://doi.org/10.5281/zenodo.2552022>

Thumbadoo, R. V., & Taylor, D. R. F. (2021). Circle of All Nations Digital Global Village – William Commanda's Indigenous Cybernetic Navigation into the Age of Information Technology. *2021 IEEE Conference on Norbert Wiener in the 21st Century (21CW)*, 1–5. <https://doi.org/10.1109/21CW48944.2021.9532529>

Trochim, W. (2020). *The research methods knowledge base*. Conjointly.com.

<https://conjointly.com/kb/qualitative-validity/>

Trusted Computing Group. (2022). *Trusted Platform Module (TPM) summary*.

[https://trustedcomputinggroup.org/resource/trusted-platform-module-tpm-summary/#:~:text=TPM%20\(Trusted%20Platform%20Module\)%20is](https://trustedcomputinggroup.org/resource/trusted-platform-module-tpm-summary/#:~:text=TPM%20(Trusted%20Platform%20Module)%20is)

Tse, D. (2022). *Cybersecurity and technology risk in virtual banking*. ISACA.

<https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-and-technology-risk-in-virtual-banking>

Turnbull, D., Chugh, R., & Luck, J. (2023). Systematic-narrative hybrid literature review:

A strategy for integrating a concise methodology into a manuscript. *Social Sciences & Humanities Open*, 7(1), Article 100381.

<https://doi.org/10.1016/j.ssaho.2022.100381>

TutorialsPoint. (2022). *Cyber security strategies*.

https://www.tutorialspoint.com/information_security_cyber_law/cyber_security_strategies.htm

Ullah, S., Kiani, U. S., Raza, B., & Mustafa, A. (2022). Consumers' intention to adopt m-payment/m-banking: The role of their financial skills and digital literacy.

Frontiers in Psychology, 13. <https://doi.org/10.3389/fpsyg.2022.873708>

Umpleby, S. A., Medvedeva, T. A., & Lepskiy, V. (2019). Recent developments in cybernetics, from cognition to social systems. *Cybernetics and Systems*, 50(4),

367–382. <https://doi.org/10.1080/01969722.2019.1574326>

Universal Teacher. (2019). *Dependability in qualitative research*. Universalteacher.com.

<https://universalteacher.com/1/dependability-in-qualitative-research/>

University of Nottingham. (2022). *Understanding pragmatic research*.

<https://www.nottingham.ac.uk/helmopen/rlos/research-evidence-based-practice/designing-research/types-of-study/understanding-pragmatic-research/section03.html#:~:text=Pragmatism%20involves%20research%20designs%20that>

University of the Sunshine Coast. (2022). Audit and Assurance Framework - Governing Policy. Www.usc.edu.au. <https://www.usc.edu.au/about/policies-and-procedures/audit-and-assurance-framework-governing-policy>

- University of West Florida. (2021). *LibGuides: Literature Review: Conducting & Writing: Organizing/Writing*. Uwf.edu.
<https://libguides.uwf.edu/c.php?g=215199&p=1420568>
- USAID. (2021). *What are the elements of a regulatory framework for mini-grids? | Mini-Grids Support Toolkit | Energy | U.S. Agency for International Development*.
 Www.usaid.gov. <https://www.usaid.gov/energy/mini-grids/regulation/elements>
- U. S. Department of Defense. (2020). *Interoperability of information technology, including national security systems*.
<https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/833001p.pdf>
- U. S. Department of Defense. (2022). *Acrobat accessibility report*. Dodcio.defense.gov.
<https://dodcio.defense.gov/Portals/0/Documents/Library/CSResourceReferenceGuide.pdf>
- U. S. Department of Homeland Security. (2019). *Secure cyberspace and critical infrastructure*. <https://www.dhs.gov/secure-cyberspace-and-critical-infrastructure>
- U. S. Food & Drug Administration. (2019). *Institutional review boards (IRBs) and protection of human subjects in clinical trials*. U.S. Department of Health and Human Services. <https://www.fda.gov/about-fda/center-drug-evaluation-and-research-cder/institutional-review-boards-irbs-and-protection-human-subjects-clinical-trials#:~:text=Under%20FDA%20regulations%2C%20an%20Institutional>
- Utah State University. (2022). *Compliance Framework*. www.usu.edu.
<https://www.usu.edu/compliance/framework-overview>
- Vedel, I., Kaur, N., Hong, Q. N., El Sherif, R., Khanassov, V., Godard-Sebillotte, C.,

Sourial, N., Yang, X. Q., & Pluye, P. (2019). Why and How to Use Mixed Methods in Primary Health Care Research. *Family Practice*, 36(3), 365–368.

<https://doi.org/10.1093/fampra/cmy127>

Wadhwa, P. (2023). *Top Three Cyber Security Goals*. Sprinto.

<https://sprinto.com/blog/cyber-security-goals/>

Wagenaar, H., Kieslich, K., Hangel, N., Zimmermann, B., & Prainsack, B. (2022).

Collaborative comparisons: A pragmatist approach towards designing large-scale, comparative qualitative research. *SSM - Qualitative Research in Health*, 100172.

<https://doi.org/10.1016/j.ssmqr.2022.100172>

Wang, P., Gao, H., Rao, Q., Luo, S., Yuan, Z., & Shi, Z. (2021). A Security Analysis of Captchas With Large Character Sets. *IEEE Transactions on Dependable and Secure Computing*, 18(6), 2953–2968.

<https://doi.org/10.1109/TDSC.2020.2971477>

Western Governors University. (2020). *A guide to social learning theory in education*.

wgu.edu: <https://www.wgu.edu/blog/guide-social-learning-theory-education>

The White House. (2021). Executive order on improving the nation’s cybersecurity. The

White House. [https://www.whitehouse.gov/briefing-room/presidential-](https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/)

[actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/](https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/)

Wickham, R. (2019). Secondary Analysis Research. *Journal of the Advanced*

Practitioner in Oncology, 10(4), 395–400. NCBI.

<https://doi.org/10.6004/jadpro.2019.10.4.7>

Wiener, N. (1961). *Cybernetics: Or, Control and communication in the animal and the*

machine. New York: M.I.T. Press.

Williams, T. (2021). *Why is quantitative research important?* gcu.edu.

<https://www.gcu.edu/blog/doctoral-journey/why-quantitative-research-important>

Winters, T. (2019). *StackPath*. www.securityinfowatch.com.

<https://www.securityinfowatch.com/cybersecurity/article/21081424/how-to-use-open-standards-to-improve-security-and-performance-testing>

The World Bank. (2021). Digital Regulation Platform. Digitalregulation.org.

<https://digitalregulation.org/enhancing-the-protection-and-cyber-resilience-of-critical-information-infrastructure/>

Xu, W., Hu, G., Ho, D. W. C., & Feng, Z. (2020a). Distributed Secure Cooperative Control Under Denial-of-Service Attacks From Multiple Adversaries. *IEEE Transactions on Cybernetics, IEEE Transactions on, IEEE Trans. Cybern*, 50(8), 3458–3467. <https://doi.org/10.1109/TCYB.2019.2896160>

Xu, X., Liu, L., & Li, B. (2020b). A survey of CAPTCHA technologies to distinguish between human and computer, *Neurocomputing*, Volume 408, Pages 292-307.

Yadav, R. (2023). *People Security: A Comprehensive Framework and Model*. Threatcop.

<https://threatcop.com/blog/people-security-management-a-comprehensive-framework-and-model/> <https://doi.org/10.1016/j.neucom.2019.08.109>

Yan, D. (2022). *A Systems Thinking for Cybersecurity Modeling*.

<https://arxiv.org/pdf/2001.05734>

Yang, L., QI, L., & Zhang, B. (2022). Concepts and evaluation of saturation in qualitative research. *Advances in Psychological Science*, 30(3), 511.

<https://doi.org/10.3724/sp.j.1042.2022.00511>

Yin, R. K. (1981). The case study as a serious research strategy. *Science Communication*, 3(1), 97-114. <https://doi.org/10.1177/107554708100300106>

Yin, R. K. (2016). *Qualitative research from start to finish*.

eli.johogo.com/Class/Qualitative%20Research:

<http://eli.johogo.com/Class/Qualitative%20Research.pdf>

Young, A. (2021). The Role of AI in Modern Endpoint Security. CSO Online.

<https://www.csoonline.com/article/3639843/the-role-of-ai-in-modern-endpoint-security.html>

Zaharia, A. (2019). *Banks Under Attack: Tactics and Techniques Used to Target Financial Organizations - Security News*. Wwww.trendmicro.com.

<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/banks-under-attack-tactics-and-techniques-used-to-target-financial-organizations>

Zaid Almahirah, M. S. (2021). The Effect of Smart Blockchain Contracts on the Financial Services Industry in the Banking Sector in Jordan. *Ilkogretim Online*, 20(5), 1845–1853. <https://doi.org/10.17051/ilkonline.2021.05.203>

Zakrzewska, M., & Miciuła, I. (2021). Using e-government services and ensuring the protection of sensitive data in EU member countries. *Procedia Computer Science*, 192, 3457–3466. <https://doi.org/10.1016/j.procs.2021.09.119>

Zeybek, M., Yilmaz, E. N., & Alper Dogru, I. (2019). A Study on Security Awareness in Mobile Devices. 2019 1st International Informatics and Software Engineering

Conference (UBMYK), Informatics and Software Engineering Conference (UBMYK), 2019 1st International, 1–6.

<https://doi.org/10.1109/UBMYK48245.2019.8965476>

Zhao, Y., & Bacao, F. (2021). How Does the Pandemic Facilitate Mobile Payment? An Investigation on Users' Perspective under the COVID-19 Pandemic. *International Journal of Environmental Research and Public Health*, 18(3), 1016.

<https://doi.org/10.3390/ijerph18031016>

Zheng, Y., Li, Z., Xu, X., & Zhao, Q. (2021). Dynamic defenses in cyber security: Techniques, methods, and challenges. *Digital Communications and Networks*,

8(4). <https://doi.org/10.1016/j.dcan.2021.07.006>

Zion Market Research. (2019). *Artificial Intelligence (AI) In Cyber Security Market Will Reach to USD 30.9 Billion By 2025: Zion Market Research*. GlobeNewswire News Room. [https://www.globenewswire.com/news-](https://www.globenewswire.com/news-release/2019/08/28/1907655/0/en/Artificial-Intelligence-AI-In-Cyber-Security-Market-Will-Reach-to-USD-30-9-Billion-By-2025-Zion-Market-Research.html)

[release/2019/08/28/1907655/0/en/Artificial-Intelligence-AI-In-Cyber-Security-Market-Will-Reach-to-USD-30-9-Billion-By-2025-Zion-Market-Research.html](https://www.globenewswire.com/news-release/2019/08/28/1907655/0/en/Artificial-Intelligence-AI-In-Cyber-Security-Market-Will-Reach-to-USD-30-9-Billion-By-2025-Zion-Market-Research.html)

Appendix A: NIH Certificate of Compliance



Appendix B: Interview Protocol

- Greet the participant and help them feel at ease.
- Thank the participant for taking the interview.
- Ensure the participant is advised that they can withdraw from the interview at any time without any penalty.
- Advise the participant that the recording has begun and ensure strict confidentiality of the recorded content.
- Being in this interview will involve a small amount of time recording a ten questions. With the protections in place, this semi-structured interview would pose minimal risk to your well-being. The interview questions will not number more than 10
- I will identify the participants and date of interview.
- I will begin the interview with the questions provided.
- I plan to interview five to ten security professionals. I will review the online security policies of two or more companies to ensure data saturation.

Interview Questions

What security strategies are in use by cybersecurity professionals at financial institutions to mitigate security breaches for their mobile customers?

1. How do you use your cybersecurity to mitigate data breaches for mobile customers who access financial data?

Probe: What cybersecurity do you have at your disposal?

2. What cybersecurity has been found to be the most effective in mitigating data breaches for mobile customers who access financial data?

3. What cybersecurity measures do you identify as least effective?
4. How do you perceive successful techniques enabling users in current cybersecurity strategies?
5. What is your evaluation of the current cybersecurity that mitigates data breaches for your mobile customers?
6. What challenges do you face regarding protecting financially transmitted information using mobile devices?
7. How would you describe the effects of cybersecurity on mitigating data breaches for your mobile customers who access financial data?
8. Is there anything else you would like to add reflecting on your cybersecurity for data breaches used by mobile customers who access financial data?