Journal of Financial Risk Management, 2024, 13, 576-603
https://www.scirp.org/journal/jfrm
ISSN Online: 2167-9541
ISSN Print: 2167-9533

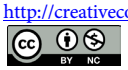
Third-Party Information Security: Generic Qualitative Inquiry in Banking and Financial Services

Genemar Arthur Lazo

College of Technology and Engineering, Westcliff University, Irvine, CA, USA
Email: genemarlazo@westcliff.edu

How to cite this paper: Lazo, G. A. (2024). Third-Party Information Security: Generic Qualitative Inquiry in Banking and Financial Services. *Journal of Financial Risk Management, 13*, 576-603.
https://doi.org/10.4236/jfrm.2024.133027

Received: August 17, 2024
Accepted: September 24, 2024
Published: September 27, 2024



Abstract

Problem: Although IT security frameworks and solutions are available, banking and financial organizations encounter challenges in accepting security technology to secure the organization and its third-parties. **Purpose:** The purpose of the study is to explore implementation strategies for banking and financial IT third-party security solutions to determine impediments to full acceptance of available security tools related to access control and data protection. **Method:** The technique selected for this project is qualitative inquiry. **Population:** The project question was explored via interviews. The researcher used purposeful and convenience sampling methods to identify participants who work within the banking and financial services industry in the United States. **Results:** The researcher conducted a thematic analysis using the UTAUT framework applied to access controls, and data protection was completed during the review. The themes identified included the key factors for increasing the acceptance of security solutions for banking and financial services organizations and related third-parties for access controls and data protection: assessments, executive sponsorship, oversight of the implementation, requirements management, sufficient planning, and testing of technical solutions. **Implications/Practical Uses:** This project's recommendations include assessments for third-parties, training, and scoping requirements. The researcher may propose increased communication, assessment methodologies, and tools for protecting data, services, and third-parties.

Keywords

Banking, Financial Services, Information Security, Access Controls, Data Protection, APIs, Application Program Interfaces, Web Application Security, Third-Party, Supplier, Vendor, Security Assessments

1. Introduction

In recent years, security incidents have occurred and exposed the data of individuals throughout the world (Alsowail & Al-Shehari, 2022; Buker, 2021; Leung, 2018; Tarlow, 2019). The travel and tourism industries were shaken by the loss of personal information of 500 million records, including financial data across the worldwide Starwood brand of the hotel conglomerate Marriott (Mest, 2019; Tarlow, 2019). Investigations into the security breach estimate that the data may have been leaked as early as 2014 (Mest, 2019; Tarlow, 2019). A security incident involving Facebook affected 50 million users that allowed unauthorized access by any third-party application using Facebook's single sign-on login solutions, including Google and Twitter (Barrett & Newman, 2018). Banking and financial services organizations have challenges preventing and addressing ongoing security events involving third-parties through the implementation of information technology security solutions and adherence to established security best practices (Alsowail & Al-Shehari, 2022; Barrett & Newman, 2018; Buker, 2021; Leung, 2018; Ly et al., 2015; Plachkinova, 2018; Varma et al., 2022; Wewege et al., 2020). The research study will concentrate on mitigating business risks related to the IT security of organizations and their third-parties to reduce potential losses. Third-parties are external entities to an organization, which stores, processes, or maintains data or services, such as vendors (Sfoglia, 2019). The research study will provide an overview of business, security, and technical frameworks, related requirements, and best practices for organizations to secure their organization and third-parties. Financial services organizations have significant obstacles preventing and addressing security events/risks involving third-parties (Barrett & Newman, 2018). The research study will concentrate on the acceptance of security technologies for mitigating risks related to banking/financial organizations and their third-parties.

For banking services and financial services organizations to succeed, the companies must provide expedient, efficient, and secure transactions (Malik, 2020; Mayur, 2018; Yee Yen, 2011). Banking and financial transactions may result in data loss, unauthorized data disclosure, identity theft, and monetary losses (AbuShanab & Pearson, 2007; Bronson, 2022; Chitreddy et al., 2024; Malik, 2020; Mayur, 2018; Ogudebe, 2022; Yee Yen, 2011). An organization's third-party may engage a fourth party to conduct specific services that disclose banking data (Knudson, 2021). The numerous downstream vendors may lead to additional risk exposure by increasing the attack surfaces (Knudson, 2021; Levtsov, 2017).

Barriers to the acceptance of security solution technologies include the following: availability, ease of use, employee perceptions, lack of research, underdeveloped procedures, and ineffective security strategies (AbuShanab & Pearson, 2007; Malik, 2020; Mayur, 2018; Savage, 2017; Yee Yen, 2011). This generic qualitative inquiry aims to understand better managing technology risks related to IT security for banking and financial services organizations and corresponding third-parties. The research study will review frameworks and solutions for applicability to

addressing business risks by accepting IT security solutions within organizations and third-parties. The research site and professional networking site LinkedIn (https://www.linkedin.com) are critical in the success of the data aggregation required to satisfy the research question.

Problem of Practice

The monetary losses worldwide due to cyber-attacks have reached $575 billion annually (Naylor, 2016). In addition to economic losses, companies rely on brand recognition and trust to maintain customer relationships (Plachkinova, 2018). The general business problem is increased security breaches due to using third-parties for specialized services and integrating systems (Qazi, 2022; Sloboda & Demianyk, 2020). The specific business problem is adequate industry standards or tools exist with evidence of some degree of implementation, but these standards are not being fully accepted during implementation within banking and financial services organizations and their third-parties (Bronson, 2022; Barrett & Newman, 2018; Cleary & McLarney, 2019; Plachkinova, 2018; Qazi, 2022; Sloboda & Demianyk, 2020). Companies should place increased importance on building a solid security posture by enforcing vendor management and IT security frameworks to minimize and prevent security events for organizations with third-parties (Plachkinova, 2018). The success of cyberattacks primarily depends on implementing best practices and IT solutions in access control mechanisms and security awareness (Mohsen, 2016; Williams, 2021). Without proper network security when managing the perimeter of organizations like externally facing websites, permissions distributed to third-parties, including controlling access to an organization's data and the operational capabilities within the technical environments, may be inadvertently and unknowingly exposed (Knudson, 2021).

2. Purpose of the Project

The purpose of the study is to explore implementation strategies for banking and financial IT third-party security solutions to determine impediments to full acceptance of available security tools related to access control and data protection. The generic qualitative inquiry project aims to gain a deeper understanding of the experiences, perspectives, and strategies of technology professionals in the U.S. regarding the effective use of technology for risk management of banking and financial services organizations and associated third-parties.

2.1. Project Need

There is a need to better mitigate third-party IT security risks associated with banking and financial services organizations (Knudson, 2021; News Bites, 2020). Ransomware risks have been driven by managing third-party risk for banking and financial services security measures and solutions, such as increased resources and time to patch (Knudson, 2021; Lusher, 2018). Governance over the supply chain and downstream vendors (fourth parties) may manage risks associated with complex

attack surfaces (Knudson, 2021; News Bites, 2020). Ransomware risks may be addressed by increasing intelligence and response times to practice patching and vulnerability management (Knudson, 2021; News Bites, 2020).

2.2. Project Question(s)

PQ: How do organizations improve the level of acceptance of security standards and technologies during implementation in banking and financial services industries to reduce IT security risks related to third-parties?

2.3. Project Justification

Businesses and financial market interactions rely increasingly on the Internet and automated technologies to support monetary transactions (Ula et al., 2011). As the number of dependencies on banking and financial services expands, the threats and security breaches increase, resulting in trillion dollars in losses (Ula et al., 2011). Network management procedures should only allow authorized users to system controls and escalated access to confidential data servers (NACHA, 2022; Weinstock, 2014).

Threats have evolved, and new technologies have been adopted, introducing unknown risks associated with third-parties via collaboration platforms, cloud services, smart devices, and mobile apps representing varying forms of cyber risk (Chitreddy et al., 2024; Cleary & McLarney, 2019; Fielding, 2020). Frameworks and best practices are industry standards used as guides to provide technical and process-driven measures to address IT risks and threats (Cleary & McLarney, 2019; Fielding, 2020). The focal point of the study was to document challenges, experiences, and perceptions regarding the acceptance of security controls and measures of security team members at a banking or financial services institution.

2.4. Approach for the Project

An approved site and LinkedIn were used to locate and identify potential participants who meet the project's inclusion criteria available and volunteered to participate in a 45-minute audio-recorded interview composed of a series of questions to facilitate conversations for data collection. The approved research site was a bank located in the western region of the USA. The interviews aim to explore the respondents' perceptions regarding the effectiveness of strategies to secure the organization and their third-parties. Semi-structured interviews were designed with open-ended questions based on the UTAUT framework. A supporting interview guide (**Appendix**) is in place to ensure the interview is well organized and results coincide with the intended purpose. The project's applied framework was used to develop the questions to prompt responses from each participant. Interview questions were designed to explore the organization's third-party information security perception for analysis to generate a thematic analysis of the acceptance of IT solutions related to third-party information security.

The study used UTAUT (Unified Theory of Acceptance and Use of Technology)

research model to support and guide research work for gaining a deep understanding of addressing risk using security solutions in the banking and financial services industry along with related third-parties (AbuShanab & Pearson, 2007; Ashraf et al., 2021; Noble et al., 2022; Nunes et al., 2022; Savage, 2017; Stoppok et al., 2022).

2.5. Applied Framework

Previous uses of the UTAUT framework to understand the acceptance of emerging technologies such as mobile devices for banking, security solutions, and safety apps used to mitigate the results of a pandemic surge (AbuShanab & Pearson, 2007; Ashraf et al., 2021; Fujimori et al., 2022; Noble et al., 2022; Nunes et al., 2022; Savage, 2017). The focus of UTAUT framework within this study was to investigate the acceptance of access control and data protection solutions, including multifactor authentication, Privileged Access Management (PAM) and Data Loss Prevention (DLP) tools for third-parties during implementation (Alsowail & Al-Shehari, 2022; Colnago et al., 2018; Pennic, 2022; Stoppok et al., 2022; Wewege et al., 2020).

UTAUT is well established for measuring interest in the use of technology, including influential factors such as peer pressure, organizational support, and voluntary use, as well as additional factors such as experience, age, and gender (Nunes et al., 2022; Stoppok et al., 2022). Uses of the UTAUT include the ability to identify and explore the use and behavior of technology, attitude towards technology, value of adaptation, and effects of innovation, both positive and negative (Nunes et al., 2022; Stoppok et al., 2022). UTAUT has psychological variables that were used to evaluate the interview guide on security solutions mapped: Effort Expectancy (EE), Facilitating Condition (FC), Performance Expectancy (PE), and Social Influence (SI) (Nunes et al., 2022; Stoppok et al., 2022).

PE is the anticipated increase in individual performance using technology (Ashraf et al., 2021; Noble et al., 2022). In the setting of security solutions, the anticipated result is the securitization of an environment by deploying the security solution and any other advantages or benefits (Ashraf et al., 2021; Noble et al., 2022; Stoppok et al., 2022). EE is the usability of the technology (Noble et al., 2022; Stoppok et al., 2022). User acceptance increases as the perceived effort to use the technology decreases (Ashraf et al., 2021; Noble et al., 2022; Stoppok et al., 2022). SI is the perceived benefit of people of importance (Ashraf et al., 2021; Fujimori et al., 2022; Noble et al., 2022; Stoppok et al., 2022). In security solutions, SI can be measured by the leadership's perceived benefit of deploying security solutions (Colnago et al., 2018; Fujimori et al., 2022; Noble et al., 2022; Stoppok et al., 2022).

PE, EE, and SI are direct indicators of acceptance of technologies (Ashraf et al., 2021; Stoppok et al., 2022). Facilitating conditions are environmental indicators of actual use behavior (Nunes et al., 2022; Stoppok et al., 2022). FC includes factors that may increase the actual use of technology, such as user training or other

supporting infrastructure (Ashraf et al., 2021; Buker, 2021; Nunes et al., 2022; Stoppok et al., 2022). The Unified Theory of Acceptance and Use of Technology (UTAUT) framework provides evaluation criteria for the adaptation of information security solutions based on acceptance and intention of solutions used to address the NACHA requirements related to third-parties: access controls and data protection (Ashraf et al., 2021; Stoppok et al., 2022).

Figure 1 is an illustration of the business problem and research question mapping. Although third-party security requirements exist for the banking and financial industries, security controls and data protection issues continue to proliferate in third-party environments (Dhillon et al., 2017; Elzamly et al., 2017). Primary risks for third-party hosted and managed environments in banking and financial services such as cloud computing include data protection, security capabilities, and user requirements (Chitreddy et al., 2024; Ghelani et al., 2022). Third-party resources share technology-diverse environments where business rules for accessing data and computing devices (Demetriou et al., 2015). The research paper explored access control, and data protection security requirements in place to protect consumers and deter unauthorized disclosure of non-public information (NACHA, 2021, 2022; PCI, 2022; Wewege et al., 2020).

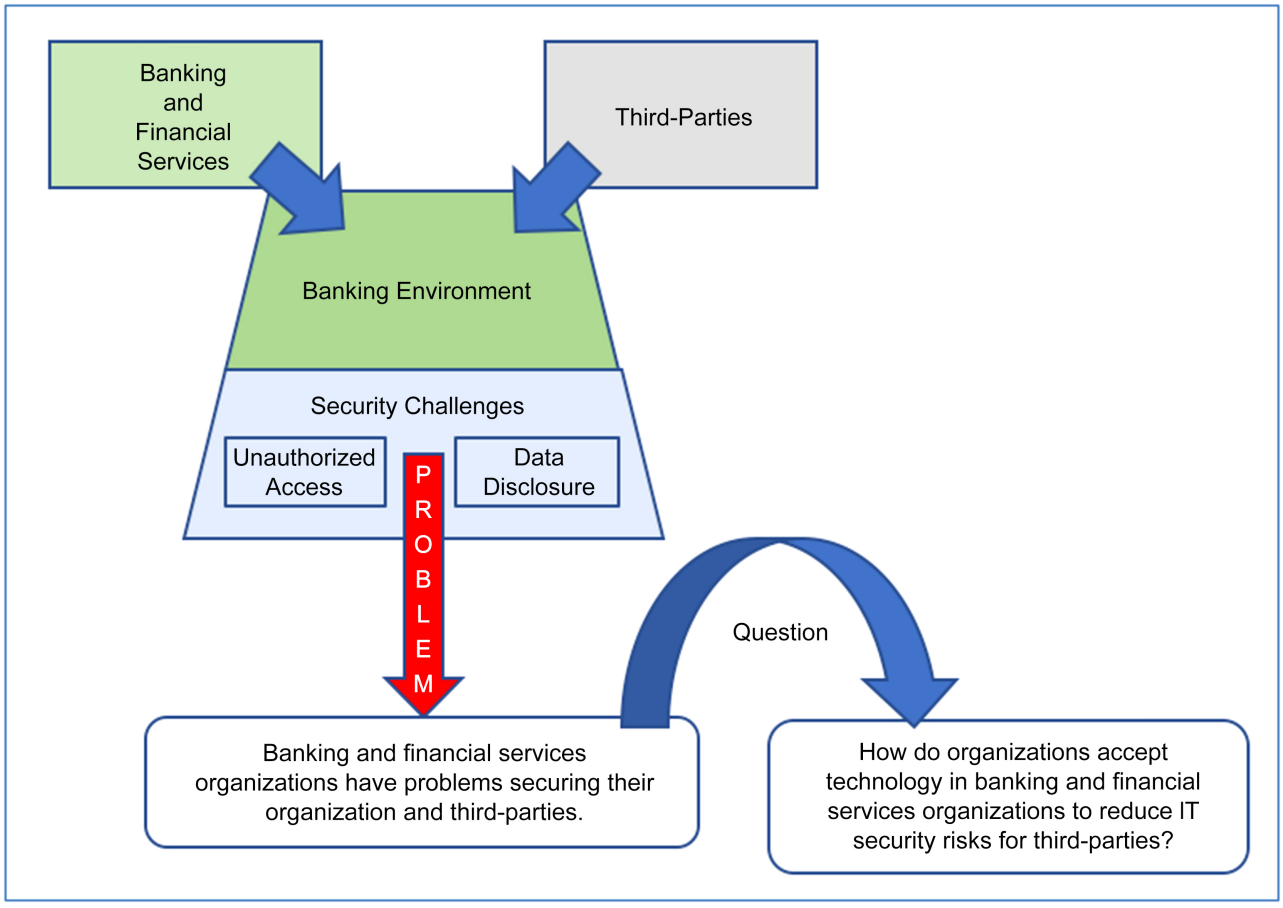


Figure 1. Business problem and research question mapping. Source: Dhillon et al. (2017).

Data Protection. In 2017, a third-party subcontractor misconfigured a cloud instance, resulting in the disclosure of 20,000 customer records for Scottrade Bank (Boggavarapu, 2021). Third-parties may offer lower costs of resources and technology innovations that cannot be readily developed by banks and financial services organizations (Thomson, 2018; Wewege et al., 2020). To optimize processes and reduce costs, banks, and financial services share non-public data to meet customer expectations and enhance the suite of monetary services by leveraging third-party service providers (NACHA, 2021; Thomson, 2018; Wewege et al., 2020). As a result, banking and financial services operations are becoming customer data-centric (Krell, 2022; NACHA, 2021; PCI, 2022; Wewege et al., 2020). When sharing non-public data from banking and financial services organizations with third-parties, additional controls and measures should be deployed to secure the organizational data efficiently in the new environment (Dhillon et al., 2017).

In 2020, NACHA guided banks, financial organizations, and their third-parties' requirements specific to bank account numbers (NACHA, 2021, 2022). Requirement 23, of the NACHA ACH Audit Guide, requires that all points in the transaction cycle (storage, transmission, presentation) must be secured at a commercially reasonable level within applicable regulatory guidelines (NACHA, 2021). Bank account numbers must be transmitted using encryption, masking, obfuscation, truncation, and similar industry methods (NACHA, 2021, 2022). Encryption features may be deployed when transmitting bank information using strong authentication such as TLS or Internet Protocol Security (IPSec) (NACHA, 2021, 2022; Nunes et al., 2022; PCI, 2022). When using web services, third-parties may be required to connect securely to banks and other financial services through APIs or other protected means to transmit data (Wewege et al., 2020). The literature reviewed included data protection solutions such as encryption and Data Loss Prevention (DLP) tools for third-parties (Alsowail & Al-Shehari, 2022; Pennic, 2022; Stoppok et al., 2022). DLP solutions can identify financial information exfiltrated via BlueTooth, USB, and email (Alsowail & Al-Shehari, 2022). DLP solution advancements can monitor the copying and pasting of non-public data to peripheral applications (Alsowail & Al-Shehari, 2022). The future of data protection includes machine learning to identify the probability of data exfiltration containing non-public customer information, such as bank account data (Alsowail & Al-Shehari, 2022). Systems with data in transit should have security measures such as encryption logging analysis and monitoring (NACHA, 2021, 2022; Nunes et al., 2022; PCI, 2022; Varma et al., 2022).

Policies and processes for the governance of financial data for financial organizations and their third-parties are required by FINRA, NACHA, and PCI-DSS (Buker, 2021; NACHA, 2022; PCI, 2022). Banks and financial organizations should contact vendors to request recommendations and protection measures for customer financial information and update policies and procedures (NACHA, 2021, 2022). Technical documentation of financial organizations and third-parties should include inventories of systems that contain customer financial data, current capabilities

of data protection, and mapping of data traversal through banking and financial services organizations using data flow diagrams (NACHA, 2021, 2022; Nunes et al., 2022).

Access Controls. JP Morgan Chase had 350,000 wealth management customer records disclosed due to deficient access controls (Peters, 2015). Access controls are in place to ensure users are valid, prevent unauthorized access, and allow the alerting and monitoring of suspicious behavior heuristics (Buker, 2021; Wewege et al., 2020). Unauthorized access to data such as birth date, financial information, and social security number within systems may result in adverse consequences for the data owner (Buker, 2021). Access control solutions have been a focus of organizations including Amazon, Apple, and Google to deploy access control security solutions such as Two-Factor Authentication (2FA), biometric access, and Privileged Access Management (PAM) (Colnago et al., 2018; Wewege et al., 2020).

Cybersecurity requirements exist to ensure access management measures are in place for availability, confidentiality, and integrity (Buker, 2021; NACHA, 2022; PCI, 2022). NACHA requirements ensure that customer financial information's over access controls include security policies and procedures created to clearly outline the corporate compliance rules to manage administrative and third-party access to sensitive financial data (NACHA, 2021). Access control security solutions should include internal and third-party administrative/elevated roles management via Privileged Access Management (PAM) for third-parties or similar solutions (Pennic, 2022; Stoppok et al., 2022).

UTAUT Theoretical Analysis. In the case of financial data and systems, users may feel more exposed and vulnerable due to the risks associated with safety, security, trust, and privacy (Nunes et al., 2022). Users may be more attuned to adapting to new technology (Nunes et al., 2022). UTAUT constructs are helpful to the research's theoretical framework to gain a meaningful understanding of the business problems in addition to measuring the intention of acceptance and usage of IT security solutions related to the IT security solutions, regulations and standards used for securing banking and financial services and related third-parties (Buker, 2021; Nunes et al., 2022; NACHA, 2022).

Evolution of banking technology. The study included research to identify countermeasures for risks that organizations may utilize in banking and financial services for managing third-parties in people, processes, and technology (Legowo et al., 2020). Traditional banking is evolving due to the introduction of emerging technology in the financial industry called fintech (Sloboda & Demianyk, 2020; Wewege et al., 2020). Barclays, Central Bank, Chase, World Bank, and other banks have deployed digital solutions to streamline retail and commercial banking, reduce costs, improve the speed of service, and implement security measures (Sloboda & Demianyk, 2020; Wewege et al., 2020). This generic qualitative inquiry aims to explore a deep understanding of how a banking/financial services organization manages business risk related to information security for banking and financial services related to third-parties. FinTech (or "Financial Technologies") is at the

forefront of innovation for banking and financial services organizations, allowing for the transformation of business models and digital strategies (Kellezi et al., 2021; Kolpakova & Evdokimova, 2017; Legowo et al., 2020; Wewege et al., 2020). FinTech services are avenues for businesses to meet financial requirements of the business (Bryant, 2016; Kellezi et al., 2021; Kolpakova & Evdokimova, 2017; Legowo et al., 2020; Wewege et al., 2020). Fintech services may consist of institutions such as credit organizations, clearing organizations, mutual insurance companies, pension funds (government and non-government), investment fund management institutions, leasing and securities companies (Bryant, 2016; Kellezi et al., 2021; Kolpakova & Evdokimova, 2017; Legowo et al., 2020; Wewege et al., 2020).

Third-parties. Third-parties have been used since the 1970s to outsource various functions, including fintech, to banks at a fraction of the cost (Bryant, 2016; Kellezi et al., 2021; Legowo et al., 2020; Thomson, 2018; Wewege et al., 2020). Third-party usage allows for cost-cutting, improved revenue streams, and enhanced user experiences (Bryant, 2016; Kellezi et al., 2021; Legowo et al., 2020; Wewege et al., 2020). Outsourced functions of the banking and financial services industry include periodic billing systems and core business transactional systems (Bryant, 2016; Kellezi et al., 2021; Legowo et al., 2020; Wewege et al., 2020). As the complexity of the programs and systems increases, so does the risk (Bryant, 2016; Kellezi et al., 2021; Legowo et al., 2020; Wewege et al., 2020). Third-party risks include activities related to credit/compliance, data access and distribution, marketing, operational, reputation, and strategy (Bryant, 2016; Kellezi et al., 2021; Legowo et al., 2020; Thomson, 2018; Wewege et al., 2020). Although the services provider is outsourced, the financial services organizations' obligations to the risks to the customers remain (Bryant, 2016; Kellezi et al., 2021; Legowo et al., 2020; Thomson, 2018; Wewege et al., 2020). Third-parties associated with security events result from a lack of controls implemented and operating effectively (Bryant, 2016; Cleary & McLarney, 2019; Kellezi et al., 2021; Legowo et al., 2020; Wewege et al., 2020). Malicious actors are finding newer avenues to attack organizations in addition to reinventing older techniques to exploit vulnerabilities (Bryant, 2016; Qazi, 2022). The improved attacks have been used against banking and financial services organizations and vendors (Bryant, 2016; DeFleice, 2022). The risk associated with banks and financial services and third-parties includes the lack of information and preparedness to combat cybercrime (Bryant, 2016).

2.6. Previous Efforts to Address the Problem

Banks have proven to be profitable targets for hackers, resulting in a cumulative loss of $1 billion (Pomerleau, 2019). Malicious actors launched malware attacks against Polish banks, affecting over 200 branches (Pomerleau, 2019). Previous efforts to address the problem include evaluating risk management tools and frameworks to manage third-parties banking and financial services risks to predict

incidents such as cyber-terrorism attacks (Pomerleau, 2019). In an information security survey of 9500 organizational leaders from over 120 countries completed by PWC (Price Waterhouse Coopers), PWC discovered several vital statistics (Pomerleau, 2019):

- Forty percent of participants noted disruption as the major threat of cyber-attacks.
- Thirty-nine percent communicated the unauthorized disclosure of data.
- Thirty-two percent expressed issues about product quality.

As part of the research completed by Pomerleau, 2019, an online survey was sent to participants requesting experiences with supporting details in the banking and financial industries, specifically aimed at Chief Security Officers (CSO) and Chief Information Security Officers (CISO). Through a population of 44 participants, ten survey participants responded. Of the total 12 core themes discussed in the research, several were related to this research project, including (Pomerleau, 2019):

- Well-Timed Information-Sharing for Preventative Measures.
- Mechanisms to Share Information.
- Opposing Missions & Objectives for Institutions.
- Ambiguous Roles, Responsibilities, and Processes for Protection Measures.
- Cyber Incidents at Banks.
- Cross-Industry Intelligence Sharing.
- Improve Cyber-Intelligence Sharing.
- Data Governance for Sharing.
- Required Security Networking.

Organizations have issues preventing and addressing ongoing security events involving financial organizations and related third-parties implementing of information technology solutions and adherence to established security best practices (Plachkinova, 2018; Barrett & Newman, 2018; Wewege et al., 2020).

Access Controls. In 2013, Target encountered a security incident that included over 70 million customer financial records through a security flaw at one of Target's vendors, Fazio Mechanical Services (Crosman, 2017; Plachkinova, 2018). Data breaches from human error cost an average of $4.7 million (Boggavarapu, 2021; Harrison & Jurgens, 2017). Malicious actors have used third-party access to elevate profiles beyond assigned authorized access, including permissions to users' financial data and profiles (Mohsen, 2016). Role-Based Access Control (RBAC) methodology includes authentication, authorization, and logging based on organizational responsibilities (Li, 2022). Access controls may consist of additional verification of financial services and third-party applications using biometric access, digital certificates, and Artificial Intelligence (AI) authorized usage (Li, 2022; Wewege et al., 2020). Administrative access over banking financial services and their third-parties may include Identity, Authentication, and Access Management (IAAM), Security Event and Incident Management (SEIM), and Privileged Access Management (PAM) (Li, 2022; Wewege, 2020).

Data Protection. In April 2017, a Scottrade Bank customer data exfiltration event resulted in 20,000 financial records becoming publicly available through vendor-managed cloud servers (Boggavarapu, 2021; Crosman, 2017). Data protection breaches are facilitated via malware, phishing, spyware, or unauthorized individual, inclusive of unauthorized third-parties (O'Rourke, 2022; Tissera et al., 2017). Countermeasures to prevent future financial data disclosures of third-parties include encryption of data, policies and procedures, vendor background checks, and technology solutions in place to effectively monitor data (Crosman, 2017; Scott, 2022; Tissera et al., 2017). Additionally, policies should be implemented to ensure strong passwords and multifactor authentication (O'Rourke, 2022; PCI, 2022).

Technology Frameworks for Financial Services Related to Third-Parties. High-value targets of threat actors include corporate entities, critical infrastructures, banking, financial organizations, and related third-parties (Burton, 2018; Turunen & Kari, 2020). The Cyber Deterrence Framework includes creating a comprehensive list of threats to banking and financial services entities. Malicious individuals and organizations are classified as deterrable actors and deterring actors (Burton, 2018). Deterrable (or malicious) actors launch the threat against the target (Burton, 2018). Deterring actors such as government agencies, police, and private sectors conduct activities to protect targets (Burton, 2018). The output of the exercise does not provide detailed security requirements and countermeasure solutions to prevent and remediate attacks against unauthorized access and data disclosure (Akdag, 2017; Burton, 2018). Banking and financial services organizations must take additional steps to understand and implement deterrence measures in the environment, such as access control and data protection (Akdag, 2017).

Banking and financial services applications depend on cloud services and web applications to meet customer needs (Chitreddy et al., 2024; Unigwe, 2021; Wewege et al., 2020). Websites are used to complete financial transactions using customer information, including non-public data such as bank account information (Anak Agung Bagus & Gusti Made, 2019). Banks leverage web applications and APIs to expose consumer financial information to third-parties (Kellezi et al., 2021; Qazi, 2022; Wewege et al., 2020). OWASP Top 10 addresses vulnerability guidance based on data and functionality threats in public APIs and web application environments (Kellezi et al., 2021; Qazi, 2022). OWASP Top 10 security requirements establish guidance to share financial data with customers and third-parties for internet-based technologies (Kellezi et al., 2021; Qazi, 2022). Organizations use OWASP Top 10 security measures in all API and web application development phases into post-production deployments (Kellezi et al., 2021; Qazi, 2022).

NACHA (National Automated Clearing House Association) governs Automated Clearing House (ACH) regulations (Krell, 2022; NACHA, 2021). The NACHA security standard applies to all payment processors, businesses, governments, and

third-parties that send two million or more ACH payments yearly (NACHA, 2021). Bank-to-bank transactions are validated through an independent entity and then sent through batch credit and debit ledger entries via the Automated Clearing House (ACH) (Krell, 2022; McGinnis, 2020; Treasure Department, 2020). In 2018, ACH transactions surpassed $51 trillion in financial transactions in total (McGinnis, 2020). The security framework required for the ACH Network requires organizations that exceed the 2 million transactional thresholds per year to render bank account numbers unreadable regardless of the financial institution used in payment processing transmission (NACHA, 2021). Encryption requirements align with the PCI-DSS (Requirement 3) framework to protect cardholder data, and the NACHA requirements to protect bank account data exist (NACHA, 2021; PCI, 2022). PCI-DSS framework requirement 3.4 establishes data protection by requiring PAN (Primary Account Number) data to be rendered unreadable anywhere stored, such as backup, digital, and logs (PCI, 2022). NACHA requirements in End User briefing denote bank account numbers should be protected and unreadable when stored electronically through methods such as encryption, masking/truncation, and tokenization for financial institution solutions, including vendor/supplier environments (Krell, 2022; NACHA, 2021).

Three of the frameworks included specific security requirements for customer data in the financial services industry (Cleary & McLarney, 2019; NACHA, 2021; PCI, 2022; Tanoh, 2022; Ula et al., 2011):

- ISG (Information Security Governance).
- NACHA (National Automated Clearing House Association).
- PCI-DSS (Payment Card Industry Data Security Standard).

Based on the framework evaluation and considering its applicability to banking and financial services, NACHA was selected for the interview guide (NACHA, 2021).

3. Data Collection Results

The data collection methodology contained open-ended semi-structured interview questions. The researcher completed the interviews using an interview schedule. The video conferencing tool Zoom was utilized to conduct the interviews via virtual conferencing. The interviews were all conducted in California, and all participants were from throughout the United States. Six participants were found using the snowball method and worked at research site A, a banking/financial services organization located in the western region of the United States. The researcher identified four additional participants using the researcher's personal LinkedIn.com account. They currently work for banking/financial services organizations throughout the United States. In preparation for the interviews, participants were asked to complete a screening survey (**Appendix**). Once the screening results were reviewed as satisfactory, the researcher extended a formal invitation to the potential participant that included details of the study and consent. As part of the invitation, the researcher proposed a time and date, but offered flexibility for other dates and

times to accommodate the participants' schedule. One participant had to reschedule three times and two participants had to reschedule two times due to work schedule obligations. Table 1 contains the demographic characteristics for participants in the study.

Table 1. Sample demographics.

Demographic Characteristics			
Participants by Title	Years of Banking Experience	Years of Information Security Experience	Gender
Chief Information Security Officer (CISO)	More than 10 years	More than 10 years	M
Managing Director, IT Risk and Compliance	More than 10 years	More than 10 years	F
Deputy CISO and Managing Director of Information Security Architecture	More than 10 years	More than 10 years	M
Director, Information Security Engineering	3 to 10 years	More than 10 years	M
Senior Director, Associate General Counsel	3 to 10 years	3 to 10 years	M
Senior Director, Corporate Procurement	3 to 10 years	3 to 10 years	M
SVP; Compliance & Operational Risk Manager	More than 10 years	More than 10 years	M
Senior Cybersecurity Specialist	More than 10 years	More than 10 years	M
Senior IT Risk Analyst and Advisor	More than 10 years	3 to 10 years	M
Principal Consultant and Managing Partner	3 to 10 years	More than 10 years	M

The scheduled time for interviews was 60 minutes. All interview recordings concluded between the 45 - 60 minutes. At the beginning of each interview, the researcher reviewed that each participant willingly, and the participants validated previous responses to the participant screening questionnaire, including the request to be recorded first and an opportunity for each participant to request any inquiries regarding the study. The researcher used the interview guide (**Appendix**) to facilitate the discussion.

Interviews about the research were conducted between 10/24/2023 and 11/28/2023. Audio transcriptions were created by the Zoom conferencing service and uploaded into Dedoose. After the researcher validated the recordings matched the transcription, each volunteer received a copy of the proofread transcription of their interview to identify any areas for corrections or updates. The researcher received no updates from the research volunteers based on the transcriptions

sent.

4. Data Analysis

The qualitative inquiry research investigated the full user acceptance of security solutions with experts working to secure banking/financial services organizations and their third parties. The researcher collected and analyzed data using the UTAUT framework to discuss effective approaches related to the securitization of non-public banking information such as ACH data related to access controls and data protection. The general problem is banking and financial services organization and their third-party environments have proven to be difficult/problematic when implementing security standards and solutions. The researcher's goal was to explore solutions to the project question: How do organizations improve the level of acceptance of security standards and technologies during implementation in banking and financial services industries to reduce IT security risks related to third-parties?

Data analysis was accomplished using a thematic review. The qualitative analysis tool, Dedoose, was utilized by the researcher to aggregate data and categorize the source files using coding. Coding was completed through several rounds of tagging, categorizing, and re-categorizing participant responses within the Dedoose toolset. The researcher leveraged thematic analysis to explore multiple interviews and summarize key data elements (Cotton, 2022).

5. Transcripts and Coding

The researcher conducted thematic analysis by reviewing the data attributes in detail to identify recurring topics and code responses. First, the researcher completed a manual review of the transcription. The researcher completed a manual review of the exported transcription files from the Zoom conferencing software. The researcher was careful to align the verbiage with the recording while preparing any corrections for import into the Dedoose software for analysis. While performing manual assessment of the transcription, the researcher identified recurring themes throughout the transcriptions. Additionally, as each transcript was reviewed the question responses were coded. The researcher started the analysis by importing the automated zoom transcriptions created during the interviews. Subsequently, the researcher manually reviewed the transcription files again using the Dedoose toolsets and corrected any types or misunderstandings as a result of the automated transcription process in Dedoose. While analyzing the transcription, the researcher documented recurring responses from interviewees. Each interviewee's answers recorded in the transcripts were reviewed and coded by the researcher in Dedoose aligning similar responses using coding. With additional reviews of the transcripts, codes were consolidated if the data represented similar concepts (for example, technological challenges and organizational challenges were combined into obstacles). **Table 2** contains the deductive and inductive coding summarizing the data from the interviews.

Table 2. Coding by participant.

Deductive Code	Inductive Code	Number of Participants
Assessment		
	Automated	10
	Manual	10
Security Area		
	Access Controls	10
	Data Protection	10
Security Challenges		
	Complexity of Solutions	10
	Data Exfiltration	10
	Emerging Technology	8
	Resource Availability—Organizational	7
	Resource Availability—Third Parties	7
	Third-Party Data Protection	10
	Third-Party Security Event	10
	Third-Party Standards	10
	Third-Party Vulnerabilities	10
	User Behavior	9
Security Solutions		
	APIs	5
	Behavioral Heuristics	4
	CMDB—Configuration Management Database	2
	Certificates	4
	Contractual Agreements, Policies, Requirements, and Training	10
	DLP—Data Loss Prevention	10
	Dedicated Network Connection or VPN Tunneling	5
	Directory Services	10
	Encryption	8

Continued

	IDS/IPS—Intrusion Detection System	5
	Malware Protection	4
	Multifactor Authentication (2FA, MFA)	9
	Other Security Solutions	9
	Platform Security	10
	Policy Management Tool	9
	SIEM—Security Incident Event Management	7
	Threat Intelligence Tools	9
UTAUT Factors for Successful Implementation of Third-Party Security		
Facilitating Condition	Budget	7
Effort Expectancy	Ease or Complexity of Implementation and Use	10
Social Influence	Executive Sponsorship—Third-Party Security Initiatives	10
Performance Expectations	Perceived Performance throughout the Life of the Solution	10
Facilitating Conditions	Policies and Procedures or Training for Users	10
Facilitating Conditions	Project Management	7
Facilitation Conditions	Security Requirements Management	6
Facilitation Conditions	Vendor Expert Resources for System Integration/Implementation	6
Performance Expectancy	Visibility and Oversight Using Dashboards for Periodic Health Monitoring of Third-Party Security	7

The qualitative inquiry research project explored why users are not fully accepting security solutions with experts working to secure banking/financial services organizations and their third parties. The researcher collected and analyzed data using the UTAUT framework to discuss effective approaches related to the users' full acceptance of technology for third-party security solutions. The theme categories were associated with the two areas of security for this research (data protection and access controls). Table 3 lists the relevant themes identified with the volunteer's supporting quotes. The volunteers in Table 3 and throughout the research are anonymized using an identifier P1 through P10.

Table 3. Project themes.

Project Themes Category and Theme	UTAUT Attribute	Supportive Quotes
Data protection transmission of data is secure from organizations to third-parties.	Performance Expectations	P1: "Data labeling is in place for all unstructured data… DLP is in place to catch any exfiltration of data."
	Performance Expectancy	P2: "There are processes in place that allow the release if the person who's sending it out has a legitimate reason to send it out and it would need to be protected with certain encryption algorithms… in order to protect this data."
	Performance Expectations	P4 stated: "ABA numbers routing numbers, bank account numbers, or data traversing our network is being monitored through the DLP solution."
	Performance Expectancy	P5 stated: "We have naming conventions or tagging for documents whether it's a confidential, restricted or personal and personal that could be PII."
	Facilitating Conditions	P6 stated: "The upfront training was significant for the members of my team. The supplier management team had a very intensive training for us."
	Facilitating Conditions	P8 mentioned in regards to behavioral heuristics usage over access controls: "To really fully take advantage of the product, there's multiple iterations of enabling certain settings (for DLP). Testing it out, make sure it doesn't break anything."
Access controls—third party access is secured using directory services from organizations to third-parties.	Effort Expectancy	P1: "Supplier access to data is managed via internal technology using our own directory service policies."
	Performance Expectancy	P2 mentioned: "The biggest control would be requiring single sign on because with single sign on, we get to control the supplier access."
	Performance Expectancy	P3: "We standardized. (Users) don't have don't have multiple different accounts with different passwords. All users use one account that account has access to applications or data that's required whether it is internal access or remote access, but once we got that, I would say that… it's pretty easy."
Access controls—third-party access is secured using security controls.	Performance Expectancy	P10 shared: "For third-party management, number one is the transmission or receiving of data. The 2-way pipe has to be protected especially for confidential data, payment systems like ACH and others. We really want that to be encrypted."
	Performance Expectancy	P3 mentioned: "We… deployed a password list solution which is more secure to log in to the banks environment. Users accessing the bank environment are no longer using (insecure) passwords. Users are also using a combination of a MFA device with biometric data."

Continued

Performance Expectancy	P8: "Certificates used to verify device used to authenticate devices to third-party access to systems and data. MFA soft tokens are used to authenticate third-party user access. Internal business users review third-party access to organizational data and systems."
Effort Expectancy	P10 noted: "Sailpoint solution is used to manage permissions and elevated privileges for third-parties."
Effort Expectancy	Per P9: "Configuration Management Databases (CMDB) used to identify and inventory systems and data internal to the organizational environment may take additional time for full acceptance due to the complexity of environment, legacy systems and emerging technologies in a real-time basis."
Effort Expectancy	P8 mentioned the following in regards to the use of 2FA (two factor authentication): "I remember we had 2FA two factor authentication, the RSA...It's gotten even easier to use over the years as they've upgraded things."

6. Answer Summary

The thematic and coding summaries from aggregated research data are adequate to address the research question. The question that directed the study was, "How do organizations improve the level of acceptance of security standards and technologies during implementation in banking and financial services industries to reduce IT security risks related to third-parties?". The analysis approach followed the plan documented in section 2.7. The primary data was collected related to improving the level of acceptance of security standards and technologies during the implementation in banking and financial service to reduce IT risks related to third parties. Throughout the literature review phase, there were many different solutions to measure the acceptance of security standards and technologies were identified. However, the research was limited in order to complete a deep investigation in order to conclude the study in a timely manner. The researcher selected the following information security areas in third-parties in banking and financial services: access controls and data protection, and third-party security assessments. The thematic analysis completed is listed in Table 3. The following sections provide a high-level overview of the answers for the three areas identified for improving the acceptance of security standards and technologies in banking and financial services and their third parties.

Data Protection. The theme for data protection involves the protection of non-public information. For the study, bank account information was concentrated on along with other PII (personally identifiable information). Several participants communicated that data exfiltration can occur though several avenues: application interfaces, direct network connections, email, and file transfers. Some of the participants discussed at their organization how data protection measures are a regulatory requirement for banking and financial services including NACHA, CPRA,

and also key to maintaining customers safe. Most of the participants' organizations used a DLP solution in order to secure internal communication to customers and external third parties such as customers, suppliers, and vendors. Delays to the acceptance of the DLP tool included false positives such as the sending of personal data (W-2) during tax season and blocking of data with non-public information with valid business requirements. Solutions to these technical problems include the deployment of solutions to manage personal tax forms and vendor portals for managing non-public data outside of the banking environment. Additionally, P7 mentioned there is a release process for bank data that is flagged by the DLP system that has a legitimate reason to be sent to external locations using the required encryption parameters of the organization. Several participants mentioned any false positives or impacts to the business will delay implementations and user acceptance of the DLP solutions.

Several of the participants mentioned several factors for a success implementation of a DLP system. Intensive training during the beginning stages of technological rollout solutions is very key to the success of IT solutions per P6. For DLP training, P1 and P5 mentioned training included the labelling, naming, tagging and categorization of data and files that may be sent externally to customers and third-party entities. P8 mentioned the successful user acceptance and implementation included multiple iterations of testing the DLP solution and other technologies in order to prevent any impact to the business.

Access Controls. The theme for access controls is regarding the organizational assignment of access via roles and permissions to authorized third-parties. Several participants mentioned that directory services to the organization are used to manage access to the organization whether the data be stored in the internal environment or externally hosted environment such as a cloud or SaaS (Software as a Service) solution. One of the key factors for the implementation and usage of the directory services solution is to be able to manage the third-party access via internal systems per P2. Additionally, P7 mentioned the standardization of several accounts into one Single Sign-On (SSO), which creates an environment that is much more user-friendly given the fact the user is able to only manage one secure login versus several usernames and passwords across several systems. Several participants mentioned another layer of authentication for internal and external users when signing into systems with non-public information including multifactor authentication that can be used through mobile devices or biometrics such as fingerprint scanning.

For high or critical risk levels of third-parties, security architects or security assessors may recommend several IT controls for securing the data and services provided to the banking and financial services organizations in alignment with social influence factor of the UTAUT. The controls may include private VPNs, dedicated network connections, and certificates for ensuring only authorized devices gain access or are accessed to and from the organization and a legitimate third-party. Additional security measure that worked as intended that were successfully

deployed included passwords lists and PAM (Privileged Access Management) solutions that were applied to both to manage both elevated organizational and third-party permissions per P10. Possible delays to the acceptance and use of third-party security solutions include the complexity and proper scoping of emerging and legacy technologies in the environment per P9.

Third-party Assessments. The themes for third-party assessments for banking and financial services organizations are based on the social influence theory. Several participants mentioned security assessments conducted by the organizations and threat intelligence tools to provide insight into possible breaches and vulnerabilities in the third-party environment. Per P7, any deviations from security standards must be rectified in order to continue to do business with the banking/financial services organization. Several participants attested that the use of both automated and manual assessments can be used to understand the security posture of third parties by providing insight into the externally facing services and intelligence feeds regarding security events, data disclosure, and possible risks to organizations. Per P10, the use of automated assessment tools may include the opportunity to create a workflow to establish a questionnaire to clarify details on any specific security events or vulnerabilities related to an organization and the related third party.

7. Contribution to Theory, the Literature, and the Practitioner Knowledge Base

The qualitative inquiry research was not used to create a new theory, but instead aggregated a vast range of professional and qualified opinions. The results of the project contributed to the information security practitioner's knowledge base by actual experience of successful factors to increase the level of user acceptance during the implementations of security solutions to reduce risks to banking and financial organizations and their third parties. By reviewing the real-life practices for increasing the level of user acceptance during implementation, practitioners can more efficiently and effectively implement security solutions for banking and financial services organizations. For example, intensive training in the earlier stages of implementation may allow for more the earlier adaptation and acceptance of security solutions in banking and financial services.

The information gathered from participants includes both best practices and details about potential barriers and key factors for successful implementation of solutions to reduce risks for third parties and associated banking and financial services organizations. The details provided by the participant assist in validating prior research regarding solutions and key factors for acceptance and usage of technology. Subsequently, the research findings assist in extending the literature.

8. Project Application and Recommendations

Due to the increasing number of security events related to banking and financial service organizations and related third parties, an investigation was initiated to

understand how to more effectively and efficiently implement IT solutions to reduce risk. Throughout the qualitative inquiry project, the researcher aggregated data from volunteer interviews, including actual factors for success and possible points of failure during implementation.

Third-party security issues remain significant throughout the banking and financial services industries. Data protection involves a layered approach by encrypting data, using secure network connections, and establishing a monitoring tool throughout the data in transit to its destination. Access controls can be used to secure third-party access to banking and financial services non-public information. Access controls can be used to validate authorized users and their devices using certificates, directory services, multifactor authentication, and privileged access management systems.

Overcoming implementation delays and significant issues is vital to the successful implementation and user acceptance of security systems. Before deploying IT solutions to organizations and third parties, training should be developed and disseminated early in the implementation phases of the project. Additionally, any complex and legacy technologies should be identified before the implementation phase to prevent delays to the implementation and user acceptance of the systems deployed. Finally, testing should have several iterations and exhaustive use cases to prevent any impacts on the business and end users. Security assessments should be established periodically to understand any deviances from security standards and require remediation to mitigate any related risks from the third-party.

For banking and financial services organizations to secure their environment in concert with their third-party, this qualitative research will assist in increasing successful implementations and user acceptance of IT security solutions. Due to the nature of this project, it was not feasible to explore all types of IT security solutions discovered in the literature review. The research concentrated on securing third-parties for banking and financial services: data protection, access controls, and security assessments. Further projects may investigate additional factors for the success or failure of IT solutions in banking and financial services, such as artificial intelligence and fourth parties. Another project may concentrate specifically on threat intelligence usage by organizations to monitor third-parties in the banking and financial services sector.

9. Conclusion

The research question was, "How do organizations improve the acceptance of security standards and technologies during implementation in banking and financial services industries to reduce IT security risks related to third-parties?". The research study covered data from all participants, including manual and automated assessments. Manual assessments include penetration testing, onsite assessments, and data flow diagrams to enumerate how the banking information may traverse securely through the banking and financial services organization to the third-parties before the implementation of new products and services and on an ongoing

basis. Requirements must be adequately translated into system configurations for the technology to perform as intended and meet requirements on the banking and financial services side for the third party. Practitioners may use automated assessments to identify vulnerabilities in third-party organizations. Assessments are vital to establishing requirements, translating requirements to technological configuration and deployment to meet users' expectations. The research presented solutions to improve the acceptance of security standards and technologies during implementation in banking and financial services and their third-parties in assessments, access controls, and data protection. Access controls include the extension of permissions management, multifactor authentication, and privileged access management. Data protection measures discussed encompassed APIs, DLP, and encryption. Critical factors for improving the acceptance of security solutions for banking and financial organizations and their third parties include executive sponsorship in the budgetary requirements, oversight of the implementation of solutions, requirements management, sufficient planning, and testing of technical solutions during implementation and on an ongoing basis.

Acknowledgements

Please allow me to thank the following for their support of the research and work: Stephen Roberts, Diane Adams, J. Brian Costello, James Schumacher, Dr. Carl Fong, Mac McKenna, Cantrell Harris, Arturo Dumindin, Anthony Enriquez, Eric Peoples, Francis Morelos, Kelly Gear, Kwame Fields, Faye Dixon-Harris, Paul Hanna, Ryan Young, Ryan Caasi, Joe Appel, Rob Harigel, Fred Gallegos, Dr. Brandon Brown, Dr. Ahmad Mostafa, Dr. Alex Lazo, Dr. Tony Lyons, and Edward J. Isaacs.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

AbuShanab, E., & Pearson, J. M. (2007). Internet Banking in Jordan: The Unified Theory of Acceptance and Use of Technology (UTAUT) Perspective. *Journal of Systems and Information Technology, 9,* 78-97. https://doi.org/10.1108/13287260710817700

Akdag, Y. (2017). *Cyber Deterrence against Cyberwar between the United States and China: A Power Transition Theory Perspective (Order No. 10640499).* ProQuest Central.

Alsowail, R. A., & Al-Shehari, T. (2022). Techniques and Countermeasures for Preventing Insider Threats. *PeerJ Computer Science*. https://doi.org/10.7717/peerj-cs.938

Anak Agung Bagus, A. W., & Gusti Made, A. S. (2019). IT Risk Management Based on ISO 31000 and OWASP Framework Using OSINT at the Information Gathering Stage (Generic Qualitative Inquiry: X Company). *International Journal of Computer Network and Information Security*, 11, 17-29. https://doi.org/10.5815/ijcnis.2019.12.03

Ashraf, S. A., Wu, S. L., Fon, S. O., & Deng, R. (2021). The Mediating Influence of the Unified Theory of Acceptance and Use of Technology on the Relationship between Internal Health Locus of Control and Mobile Health Adoption: Cross-Sectional Study. *Journal of Medical Internet Research*, **23**, e28086. https://doi.org/10.2196/28086

Barrett, B., & Newman, L. (2018). *The Facebook Security Meltdown Exposes Way More Sites than Facebook.* Wired. https://www.wired.com/story/facebook-security-breach-third-party-sites/

Boggavarapu, S. (2021). *The Effect of Third-Party Service Providers on Information Security Breaches at Financial Institutions.* Master's Thesis, University of the Cumberlands.

Bronson, H. E. (2022). *Five Common Shortcomings of Third-Party Management Programs in Financial Organizations and Recommended Risk Management Strategies.* Master's Thesis, Utica University.

Bryant, L. (2016). *Cybersecurity Regulations: Banking and Third-Party Providers (Order No. 10109630).* ProQuest Central.

Buker, H. N. (2021). *Financial Institutions Adapting to Cybersecurity Regulation Modifications: A Qualitative Multiple-Case Study (Order No. 28722239).* ProQuest Central.

Burton, J. (2018). *Cyber Deterrence: A Comprehensive Approach?* https://ccdcoe.org/uploads/2018/10/BURTON_Cyber_Deterrence_paper_April2018.pdf

Chitreddy, K., Anthony, A., Bandaru, C., & Abiona, O. (2024). Information Security in the Cloud: Emerging Trends and Challenges. *International Journal of Communications, Network and System Sciences, 17,* 69-80. https://doi.org/10.4236/ijcns.2024.175005

Cleary, S., & McLarney, C. (2019). Organizational Benefits of an Effective Vendor Management Strategy. *IUP Journal of Supply Chain Management, 16,* 50-67.

Colnago, J., Devlin, S., Oates, M., Swoopes, C., Bauer, L., Cranor, L., & Christin, N. (2018). It's Not Actually That Horrible: Exploring Adoption of Two-Factor Authentication at a University. In *CHI'18: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (pp. 1-11). Association for Computing Machinery. https://doi.org/10.1145/3173574.3174030

Cotton, W. G. (2022). *Best Practices to Improve Big Health Care Data Project Success in the US.* Master's Thesis, Capella University.

Crosman, P. (2017). *Scottrade Bank's Breach Underlines Third-Party Vendor Risk.* American Banker.

DeFleice, M. O. (2022). *Prevention and Mitigation against Cyberattacks: Bare Minimum (Order No. 28869362).* ProQuest Central.

Demetriou, S., Zhou, X. Y., Naveed, M., Lee, Y., Yuan, K., Wang, X., & Gunter, C. A. (2015). *What's in Your Dongle and Bank Account? Mandatory and Discretionary Protection of Android External Resources.* NDSS. https://doi.org/10.14722/ndss.2015.23098

Dhillon, G., Syed, R., & de Sá-Soares, F. (2017). Information Security Concerns in IT Outsourcing: Identifying (in) Congruence between Clients and Vendors. *Information & Management, 54,* 452-464. https://doi.org/10.1016/j.im.2016.10.002

Elzamly, A., Hussin, B., Abu-Naser, S. S., Shibutani, T., & Doheir, M. (2017). *Predicting Critical Cloud Computing Security Issues Using Artificial Neural Network (ANNs) Algorithms in Banking Organizations.*

Fielding, J. (2020). The People Problem: How Cyber Security's Weakest Link Can Become a Formidable Asset. *Computer Fraud & Security, 2020,* 6-9. https://doi.org/10.1016/S1361-3723(20)30006-3

Fujimori, R., Liu, K., Soeno, S., Naraba, H., Ogura, K., Hara, K., Sonoo, T., Ogura, T., Nakamura, K., & Goto, T. (2022). Acceptance, Barriers, and Facilitators to Implementing Artificial Intelligence-Based Decision Support Systems in Emergency Departments: Quantitative and Qualitative Evaluation. *JMIR Formative Research, 6,* e36501. https://doi.org/10.2196/36501

Ghelani, D., Hua, T. K., & Koduru, S. K. R. (2022). A Model-Driven Approach for Online Banking Application Using AngularJS Framework. *American Journal of Information Science and Technology, 6,* 52-63.

Harrison, S., & Jürjens, J. (2017). Information Security Management and the Human Aspect in Organizations. *Information and Computer Security, 25,* 494-534. https://doi.org/10.1108/ICS-07-2016-0054

Kellezi, D., Boegelund, C., & Meng, W. (2021). Securing Open Banking with Model-View-Controller Architecture and OWASP. *Wireless Communications & Mobile Computing (Online), 2021,* Article ID 8028073. https://doi.org/10.1155/2021/8028073

Knudson, J. (2021). *Top Bank Risks for 2021.* American Bankers Association.

Kolpakova, G., & Evdokimova, I. (2017). *The Financial Mechanism of Management as a Way of Organizing Financial Services and Financial Values.* Varazdin Development and Entrepreneurship Agency (VADEA).

Krell, E. (2022). *Payments Trends: Faster, Larger, and More Secure.* Treasury & Risk.

Legowo, M. B., Subanidja, S., & Sorongan, F. A. (2020). A Conceptual Framework of Technological Innovation for the Financial and Banking Industry in Indonesia. *International Journal of Information, Business and Management, 12,* 100-114.

Leung, R. (2018). *Cybersecurity Regulation in the Banking Sector: Global Emerging Themes.* Master's Thesis, The London School of Economics and Political Science.

Levtsov, V. (2017). *Cyberattacks Cost Financial Institutions US$1M Per Attack.* SMB World Asia (Online).

Li, Y. (2022). A Framework for Secure Online Bank System and Cloud Architecture. *Journal of Internet Banking and Commerce, 27,* 1-3.

Lusher, T. (2018). *Present and Future Solutions for the Lack of Cybersecurity Professionals (Order No. 10791221).* ProQuest Dissertations & Theses Global.

Ly, L. T., Maggi, F. M., Montali, M., Rinderle-Ma, S., & van der Aalst, M. P. (2015). Compliance Monitoring in Business Processes: Functionalities, Application, and Toolsupport. *Information Systems, 54,* 209-234. https://doi.org/10.1016/j.is.2015.02.007

Malik, M. (2020). Elements Influencing the Adoption of Electronic Banking in Pakistan an Investigation Carried Out by Using Unified Theory of Acceptance and Use Technology (UTAUT) Theory. *Journal of Internet Banking and Commerce, 25,* 1-18.

Mayur, S. (2018). *Govt to Banks: Speed Up Cards with NFC Tech [Times Business]: Security Concerns Delay Pay Channel's Adoption.* The Times of India.

McGinnis, J. O. (2020). Bitcoin's Nature and Its Future. *Harvard Journal of Law and Public Policy, 43,* 59-66.

Mest, E. (2019). *Financing Marriott Ends 2018 Ahead despite Data Breach, Strikes.* http://hdl.handle.net/10919/89076

Mohsen, F. (2016). *Exploring Varied Approaches for Countering the Privacy and Security Risks of Third-Party Mobile Applications.* ProQuest Dissertations Publishing.

NACHA (2021). *NACHA Supplemental Security Requirements.*

NACHA (2022). *NACHA Risk Management Portal.*

Naylor, L. (2016). Trading Fraud Liability for National Security: A Proposal to Amend the False Claims Act for Cybersecurity Contractors. *Public Contract Law Journal, 45,* 677-693.

News Bites (2020). *BearingPoint Generic Qualitative Inquiry: Hero Prepares for the Future with Digitally Harmonized Supply Chain.* News Bites—Private Companies.

Noble, S. M., Saville, J. D., & Foster, L. L. (2022). VR as a Choice: What Drives Learners'

Technology Acceptance? *International Journal of Educational Technology in Higher Education, 19,* Article No. 6. https://doi.org/10.1186/s41239-021-00310-w

Nunes, N., Adamo, G., Ribeiro, M., Gouveia, B. R., Elvio, R. G., Teixeira, P., & Nisi, V. (2022). Modeling Adoption, Security, and Privacy of COVID-19 Apps: Findings and Recommendations from an Empirical Study Using the Unified Theory of Acceptance and Use of Technology. *JMIR Human Factors, 9,* e35434. https://doi.org/10.2196/35434

O'Rourke, K. (2022). *Banks Must Respond to Digital Threats after Pandora's Box Moment.* FT.Com.

Ogudebe, O. I. (2022). *Challenges of Digital Privacy in Banking Organizations (Order No. 29258011).* ProQuest Central, ProQuest Central, ProQuest Dissertations & Theses Global.

PCI (2022). *Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures Version 3.2.1* https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1612157094225

Pennic, F. (2022). *Most Healthcare Facilities Lack Holistic Digital Identity Strategy, Report Finds.* Newstex.

Peters, A. (2015). *Faulty Access Controls Led to Morgan Stanley Data Breach: FTC.* Financial Planning (Online).

Plachkinova, M. (2018). Teaching Case: Security Breach at Target. *Journal of Information Systems Education, 29,* 11-20.

Pomerleau, P. (2019). *Countering the Cyber Threats Against Financial Institutions in Canada: A Qualitative Study of a Private and Public Partnership Approach to Critical Infrastructure Protection (Order No. 27540959).* ProQuest Central (2320957957).

Qazi, F. A. (2022). *Insecure Application Programming Interfaces (APIs) in Zero-Trust Networks (Order No. 28966153).* ProQuest Central (2638299306).

Savage, B. A. (2017). *A Qualitative Exploration of the Security Practices of Registered Nurses.* Master's Thesis, Walden University.

Scott, C. R. (2022). *Comparing Cybercrime in Banking and Healthcare Sectors (Order No. 29206127).* ProQuest Dissertations & Theses Global.

Sfoglia, P. (2019). *N.Y. Cyber Reg: A Third-Party Service Provider Compliance Framework.* ProQuest Dissertations Publishing.

Sloboda, L. Y., & Demianyk, O. M. (2020). Prospects and Risks of the Fintech Initiatives in a Global Banking Industry. *Problemy Ekonomiky, 1,* 275-282. https://doi.org/10.32983/2222-0712-2020-1-275-282

Stoppok, P., Teufel, M., Jahre, L., Rometsch, C., Müßgens, D., Bingel, U., Skoda, E., & Bäuerle, A. (2022). Determining the Influencing Factors on Acceptance of eHealth Pain Management Interventions among Patients with Chronic Pain Using the Unified Theory of Acceptance and Use of Technology: Cross-Sectional Study. *JMIR Formative Research, 6,* e37682. https://doi.org/10.2196/37682

Tanoh, C. N. (2022). *Effectiveness of Information Security Governance in the U.S. Banking Industry: Towards a Resilient Business Perspective (Order No. 29160858).* Dissertations & Theses @ Capella University; ProQuest Dissertations & Theses Global.

Tarlow, P. (2019). The Human Side of Cyber Security Breaches. *International Journal of Safety and Security in Tourism and Hospitality, No. 20,* 1-4.

Thomson, L. (2018). Third-Party Vendors Can Be a Weak Link: ABA Vendor Contracting Cybersecurity Checklist Focuses on the Procurement Process to Strengthen Security Protections. *SciTech Lawyer, 14,* 36-37.

Tissera, M., Thelijjagoda, S., & Goonathilake, J. (2017). User-Centric Privacy Preservation Solution to Control Third-Party Access in Digital Databases. *International Journal of Advances in Engineering & Technology, 10,* 30-45.

Turunen, M., & Kari, M. J. (2020). *Cyber Deterrence and Russia's Active Cyber Defense.* Academic Conferences International Limited.

Ula, M., Ismail, Z., & Sidek, Z. M. (2011). A Framework for the Governance of Information Security in Banking System. *Journal of Information Assurance & Cybersecurity, 2011,* Article ID: 726196. http://www.ibimapublishing.com/journals/JIACS/jiacs.html https://doi.org/10.5171/2011.726196

Unigwe, O. P. (2021). *Exploring Risk Management Strategies for Transitioning to Cloud within Financial Services Industry: A Grounded Theory Study (Order No. 29395857).* ProQuest Central.

Varma, P., Nijjer, S., Sood, K., Grima, S., & Rupeika-Apoga, R. (2022). Thematic Analysis of Financial Technology (Fintech) Influence on the Banking Industry. *Risks, 10,* Article 186. https://doi.org/10.3390/risks10100186

Weinstock, D. (2014). Is Your Practice at Risk for Medical Identity Theft? *The Journal of Medical Practice Management: MPM, 30,* 168-170.

Wewege, L., Lee, J., & Thomsett, M. C. (2020). Disruptions and Digital Banking Trends. *Journal of Applied Finance and Banking, 10,* 15-56.

Williams, R. T. (2021). *Banking and Cybersecurity Governance.* Master's Thesis, Utica College.

Yee Yen, Y. (2011). *User Acceptance of Internet Banking Services: A Comparative Study (Order No. 3498184).* ProQuest Central.

Appendix: Interview Questions

Interview Question(s)

The interviews will include the organizational third-party requirements in regards to the management of people, procedures, and technologies via phone call or teleconference (NACHA, 2021). The informational interview questions are listed below. The intent of the information questions is to gain a general understanding of the acceptance of technology related to information security IT solutions at banking and financial services organizations for related third-parties.

A) Interview Questions—Demographic Information

1) How many years in banking or financial services industries?

2) How many years in cyber security or information assurance?

B) Interview Questions—Research

1) Are automated or manual assessments done to evaluate the security around ACH data for third-parties?

Data Protection

2) What systems are in place to support policies and procedures to protect the confidentiality, integrity, and threats of Protected Information for your organization related to third-parties?

3) What are the capabilities and features of DLP, encryption, or similar systems in place to protect data for third-parties?

4) Please discuss the following regarding the technology used to facilitate data protection controls over third-parties:

Effort—How difficult/easy are the security systems over data protection to use?

Facilitating Conditions—Please provide details of present or missing training, resources, and ongoing support for the data protection security systems.

Performance—Please describe the effectiveness or areas of improvement of data protection systems that allow you to automate and monitor the data and prevent unauthorized disclosure of data. Do the data protection systems meet performance expectations?

Social Influence—Please provide organizational roles/titles of people of importance/leadership positions that support using the systems to protect data accessible to third-parties. How do professionals of importance support using systems to protect data from breaches involving third-parties?

Access Controls

5) What are systems and their capabilities to support policies and procedures to protect against unauthorized access/use of Protected Information by third-parties?

6) Please discuss the following regarding the technology used to facilitate access controls over third-parties:

Effort—Do you find the security systems over access control easy/difficult to use?

Facilitating Conditions—What are the strengths and weaknesses of training, resources, and ongoing support for the access control security systems?

Performance—What are the strengths and weaknesses of access control systems over third-parties in place that allow you to thoroughly monitor, prevent, and mitigate security events more efficiently and increase productivity? Do the access control systems over third-parties perform as expected?

Social Influence—Do people of importance/leadership positions support using the systems to establish access control for third-parties? What are the strengths and weaknesses of organizational support for systems in place for protecting access?

Additional Security Measures

7) Are any other continuous or real-time monitoring services or systems in place for access or data?

8) Please provide background on any automated or manual inventory and continuous monitoring of third-parties access controls and the amount of data that is available to third-parties.

9) Please provide any information regarding third-party security events and factors that may have contributed to the events.

10) Do you have any other access control or security challenges with securing third-parties?

If necessary, follow-up communication.

The clarifications will review any additional questions regarding experiences, frameworks, and emerging technologies or enrich and update the research data.

The researcher will collect data for thematic analysis and compose a presentation summarizing data evaluation. The presentation will include recurring themes and discussion points.