

# **BANKING CYBERSECURITY CULTURE INFLUENCES ON PHISHING SUSCEPTIBILITY**

---

A Dissertation Proposal  
Submitted to the  
Temple University Graduate School

---

In Partial Fulfillment  
of the Requirements for the Degree  
Executive Doctor of Business Administration

---

by  
Calvin Nobles  
Temple University, Fox School of Business  
May 2021

Anthony Vance, Ph.D., Advisory Chair, Fox Business School, MIS, Director, Cybersecurity Center  
Lynne Andersson, Ph.D., Committee Member, Fox Business School, Business, Society, and Ethics  
Jason Thatcher, Ph.D., Committee Member, Fox Business School, MIS  
Maurice Dawson, Ph.D., External Reviewer, Illinois Institute of Technology

---

©  
Copyright  
2021

by

Calvin Nobles  
All Rights Reserved

## ABSTRACT

The banking industry faces an unprecedented number of phishing attacks as cybercriminals circumvent security and technical countermeasures to deceive banking employees. There is a lack of scholarly research on the causes of phishing susceptibility in the U.S. banking sector. The literature review analysis highlighted the following gaps: (a) studies on information security and organizational culture failed to link theoretical underpinnings to information security results, (b) the lack of scholarly studies on the banking sector impedes academic perspective on the business problem, and (c) there is a need to investigate banking cybersecurity culture influence on phishing susceptibility.

This study consists of two qualitative inquiries; the initial study was an interpretive inquiry that resulted in a conceptual framework and highlighted a need for theory on banking cybersecurity culture influence on phishing susceptibility. The qualitative interpretive study only included interviews from security and technology executives. This study yielded the following three major themes: (a) continuous security awareness, (b) executive-driven security climate, and (c) human-centered security operations. From the inductive analysis, a reducing phishing susceptibility through executive influence and culture conceptual framework emerged. From this study, the basis of a grounded theory study was necessary to develop theory to address phishing in the banking sector.

The second inquiry was a grounded theory inquiry that expanded the initial study by interviewing (a) security and technology executives, (b) cybersecurity professionals, and (c) non-technical employees and executing a rigorous data analysis process. This study resulted in the following five major themes: (a) lack of executive coordination and support, (b) security awareness, (c) stronger security resiliency, (d) positive security behavior and environment

alignment, and (e) phishing strategy confusion. These findings derived from the data analysis resulted in the development of the Dynamic Phishing Susceptibility Reduction Theory, an organizational approach for solidifying phishing countermeasures through banking cybersecurity culture. The Dynamic Phishing Susceptibility Reduction Theory reinforces phishing countermeasures with a robust approach due to the hyperactive threat environment and constant changing of tactics.

**Keywords:** Banking, cybersecurity culture, phishing susceptibility, organizational culture

## TABLE OF CONTENTS

ABSTRACT.....	iii
LIST OF TABLES.....	4
LIST OF FIGURES.....	5
CHAPTER	
1. INTRODUCTION.....	6
2. LITERATURE REVIEW.....	9
Organizational Culture.....	9
Cybersecurity Culture.....	12
Banking Cybersecurity Culture.....	14
Phishing.....	17
Phishing Susceptibility.....	19
National Culture and Security Behavior.....	22
Studies on Phishing Susceptibility and National Culture.....	24
Gaps in Literature.....	26
3. STUDY 1.....	27
Research Method, Design, and Findings.....	27
The Role of the Researcher.....	28
Data Collection and Analysis.....	29
Research Study Participants.....	29
Research Methodology Applied to the Data Analysis.....	29
Presentation of Data and Results of the Analysis.....	32
Conceptual Framework.....	33
Continuous Security Awareness Training.....	34
Executive Influence.....	35
Human-centered Security Operations.....	36
Discussion.....	38
4. STUDY 2.....	43

Research Method, Design, and Findings .....	43
Overview of Research Methodology and Design .....	44
Research Methods .....	46
Instrumentation .....	47
Population Description.....	47
Sampling .....	48
Researcher Procedures .....	50
Reliability and Validity .....	56
Data Analysis .....	57
Analysis and Results .....	59
Data Analysis .....	59
Demographic Analysis .....	60
Study Participant Interview Data Analysis .....	62
Findings.....	65
Theory .....	76
Discussion.....	81
Security Awareness.....	83
Stronger Security Resiliency.....	83
Conclusion .....	84
5. CONCLUSION, LIMITATIONS, AND CONTRIBUTIONS .....	86
General Discussion .....	86
Other Findings .....	89
Significance of the Model.....	90
Limitations .....	90
Contributions to the Literature.....	92
Contributions to Practice.....	94
Application for Practice .....	94
Conclusions.....	95
REFERENCES .....	96
APPENDICES .....	114
A. IRB SUBMISSION.....	115

B. INTERVIEW QUESTION GUIDE ..... 116  
C. HUMAN SUBJECTS PARTICIPANT CONSENT ..... 117  
D. RECRUITMENT LETTER OR EMAIL ..... 119  
E. TABLE OF CODES, SOURCES, REFERENCES, AND SAMPLE EXCERPTS..... 120  
F. CONCEPTS, THEMES, and OVERARCHING DIMENSIONS..... 123  
G. FOUNDATION WORK AND DATA FOR OVERARCHING DIMENSIONS F..... 124

## LIST OF TABLES

Table	Page
1. Types of Phishing .....	14
2. Participant Study Date .....	24
3. Six Themes Emerging from the Data Analysis.....	27
4. Three Major Themes Emerging from the Data Analysis.....	28
5. Research Participant Groups, Definitions, and Phishing Functions .....	43
6. A Listing of Probability and Non-probability Sampling.....	44
7. Senior Security and Technology Executives Participants Study Data.....	56
8. Cybersecurity Professionals Participants Study Data.....	56
9. Non-technical Employees Participants Study Data.....	57

## LIST OF FIGURES

Figure	Page
1. High-level Depiction of Coding to Attain the Major Themes.....	25
2. Conceptual Framework: Reducing Phishing Susceptibility Through Executive Influence and Culture.....	29
3. Process for Constructivist Grounded Theory.....	47
4. Emergent concepts, themes, and overarching dimensions.....	60
5. The Dynamic Phishing Susceptibility Reduction Theory.....	72

## CHAPTER 1

### INTRODUCTION

*“A single spear-phishing e-mail carrying a slightly altered malware can bypass multi-million-dollar enterprise security solutions if an adversary deceives a cyber-hygienically apathetic employee into opening the attachment or clicking a malicious link and thereby compromising the entire network.”<sup>1</sup>*

— James Scott, Senior Fellow, Institute for Critical Infrastructure Technology

The banking sector faces relentless phishing attacks as cybercriminals circumvent technical and security countermeasures by targeting employees through phishing attacks. The Anti-Phishing Working Group (2016) reported that in 2014 that 75% of phishing attacks targeted the financial industry, retail services, and online payment systems. In 2018, U.S. businesses and organizations experienced a 40% increase in phishing attacks (Li et al., 2020). During the first quarter of 2020, the financial sector was the second most attacked industry, representing 19.3% of all phishing attacks (APWG, 2020). Cybercriminals are attracted to banks because of the collected data, sensitive information, and banking entities’ financial assets. The banking cybersecurity culture is worthy of exploring because U.S. banks are significant to the international and national markets, globalization, and personal financings. The purpose of this study is to explore a critical gap in scholarly research and address a pervasive business problem.

Banks are high-valued targets, and cybercriminals are always trying to access the information systems infrastructure, sensitive and private information, intellectual property, and financial assets by using various phishing techniques (see Table 1). Industry reports indicate that banks remain a high priority target in which phishing remains the primary attack vector (DBIR, 2020; ENISA, 2017). Phishing attacks enable a cybercriminal to illegally gain an employee’s login credentials to bypass technical countermeasures when accessing the network (William &

---

<sup>1</sup> See Scott, J. (2017, March). How to crush the health sector’s ransomware pandemic in references.

Joinson, 2020). Upon gaining access to the network, cybercriminals upgrade their credentials and entitlements to access sensitive data and critical areas of the network to exploit the bank's prized possessions.

Cybersecurity culture aims to drive positive security behavior through compliance with organizational security policies, increase cybersecurity awareness, institutional learning, and leadership (Huang & Pearlson, 2019; Reegård & Blackett, 2020). Huang and Pearlson (2019) identified (a) cultural leadership, (b) performance evaluation, (c) rewards and punishment, (d) institutional learning, (e) cybersecurity training, and (f) communications channel as organizational resources to influence cybersecurity culture. Influencing the behavior of employees is essential for averting phishing incidents by exercising positive security behavior. By leveraging cybersecurity culture, banks can adequately prepare employees to combat phishing attacks.

Phishing remains a primary vector for deceiving employees; thus, enabling nefarious actors to gain unauthorized access to the organization's corporate network (Benenson, Gassmann, & Landwirth, 2017; Sebescen & Vitak, 2017). The Anti-Phishing Working Group 4<sup>th</sup> quarter Phishing Activity Trends Report revealed that financial institutions, including banks, remain a top victim of phishing attacks (APWG, 2020a). Existing literature indicated that most large banks and financial institutions reported approximately 50,000 cyber intrusions daily (Fung, 2013; Vishwanath, Harrison, & Ng, 2018). Successful phishing attacks resulted in the theft of intellectual property, identities, financial fraud, espionage, and hacktivism, consequently contributing to unprecedented financial losses (Vishwanath, Harrison, & Ng, 2018). One issue impacting phishing susceptibility in the U.S. banking sector is the lack of scholarly research and theory contribution on cybersecurity culture influences on decreasing phishing susceptibility.

The qualitative interpretive inquiry results (the initial study) informed the basis of the second study, a grounded theory inquiry. The initial study results indicated a lack of theory and scholarly works on understanding banking cybersecurity culture influences on phishing susceptibility. The initial study produced a conceptual framework based on the data analysis; thus, revealing that a grounded theory study with three groups of study participants was necessary to develop a theory for addressing phishing susceptibility in the banking sector. This study is unique because it explores an understudied area and real-world business problem that affects the banking sector.

The following central research question guided the studies: *How does banking cybersecurity culture influence phishing susceptibility?* One the initial study, I interviewed security and technology executives and grasped the significance of expanding the study participants groups based on the initial study. I interviewed (a) security and technology executives, (b) cybersecurity professionals, and (c) non-technical employees to gain an in-depth understanding based on the study participants' experiences with phishing susceptibility in a banking environment.

This dissertation consists of the following chapters (a) Chapter 2 is the literature review, (b) Chapter 3 is Study 1, (c) Chapter 4 is Study 2, and (d) Chapter 5 is the conclusions, limitations, and contributions. The literature review and analysis include an in-depth perspective of organizational culture, cybersecurity culture, phishing, phishing susceptibility, and literature gaps. Both Chapters 3 (Study 1) and 4 (Study 2) include the research methodology and design, data collection, data analysis, and the findings.

## CHAPTER 2

### LITERATURE REVIEW

#### Organizational Culture

Organizational culture is essential to banks' overall success by providing an enterprise disposition on business operations in which cybersecurity culture is aligned as a subculture. The existing literature regarding organizational culture indicates the lack of consensus on a definition of organizational culture (Schneider, Ehrhart, & Macey, 2013; Spencer, 2019). Howard (1998) suggested that the lack of a homogeneous classification for organizational culture could impact an anthropologic concept where culture is still evolving and not defined.

The following definitions of organizational culture are from seminal organizational culture researchers. Schneider (1987) defined organizational culture as “when the people there share a common set of assumptions, values, and beliefs” (p. 448). Schein (1984) characterized organizational culture as “the pattern of basic assumptions that a given group has invented, discovered, or developed in learning to cope with its problems of external adaptation and internal integration, and that have worked well enough to be considered valid, and therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems” (p. 3). Denison (1996) described organizational culture as “the deep structure of organizations, which is rooted in the values, beliefs, and assumptions held by organizational members” (p. 624). Pettigrew (1979) defined organizational culture as “the system of such publicly and collectively accepted meanings operating for a given group at a given time” (p. 574). The abovementioned definitions are analogous; for that reason, any of the above characterizations adequately defines organizational behavior.

Schein (1996) defined organizational culture as a compelling and enduring capability. Organizational culture shapes institutional behavior through shared and similar assumptions, values, and artifacts (Howard, 1998). Researchers suggested that organizational culture is a complicated social materialization entailing widespread principles, morals, customs, and actions shared by organizational members (Hartnell, Ou, & Kinicki, 2011). Ivancevich, Konopaske, and Matteson (2014) noted that organizational culture is an indistinguishable influence; however, its presence can be perceived through organizational members' attitudes and behaviors.

Denison, Nieminen, and Kotrba (2014) emphasized that the presence of multiple cultures within a single organization, which is described as subcultures, is a recognized reality. An organization's subcultures could implement additional principles that are based on employees' profession or position. Schein (2015) contended that organizations struggle to recognize the significance of subcultures and the associated compatibility driven by occupational cultures within the subculture communities. Researchers indicated that security culture is an integral factor in establishing robust security compliance (D'Arcy & Green, 2014). According to Da Veiga and Martins (2015), instituting a security subculture is necessary to facilitate a positive environment for integrating cybersecurity and information security principles that align with the organizational culture. Cybersecurity culture is a subculture of the organizational culture in the banking sector.

Chang and Lin (2006) posited that social scientists adopted different perspectives, definitions, and types of organizational culture. Douglas (1985) stressed that organizational culture is the evolving outcome of the ongoing compromises concerning principles, values, and proprieties between organizational stakeholders. Quinn and Spreitzer (1991) advanced the concept of categorizing elements such as internal and external orientation and flexible and

control orientation to develop a grouping for classifying organizational culture into the following four types: (a) group culture, (b) developmental culture, (c) hierarchical culture, and (d) rationale culture. It is typical for organizations to demonstrate each type of culture (Quinn & Spreitzer, 1991).

Boggs (2004) continued advancing Quinn's and Spreitzer's theoretical viewpoints by creating the four following organizational cultures: (a) clan culture, (b) hierarchy culture, (c) adhocracy culture, and (d) market culture. Boggs' research was based on evaluating the integration of total quality management. Denison, Haaland, and Goelzer (2004) established four types of organizational culture, which are (a) mission, (b) consistency, (c) adaptability, and (d) involvement. The researchers deliberately expanded the body of knowledge on organizational culture to support principles for effectiveness (Denison, Haaland, & Goelzer, 2004). The research on the different types of organizational cultures reflects the latitude needed by businesses to change the culture, such as accounting for cybersecurity.

Tang and Zhang (2016) conducted a multi-stage qualitative case study on the impacts of organizational culture on information security culture by interviewing 12 study participants working in China's garment industry using various interviewing techniques at different stages. Tang and Zhang (2016) used Hofstede's organizational culture framework and the information security model's dimensions to explore the influences. The findings concluded that organizational culture directly influences information security culture (Tang & Zhang, 2016).

Hu, Dinev, and Cook (2012) investigated how top management can influence employee compliance with information security policies through a quantitative study using survey data and structural equation modeling. This study used a framework consisting of top management, organizational culture, and theory of planned behavior to tested the hypotheses on senior

management relationship participation, organizational culture, and critical factors of workers' compliance with information security policies (Hu, Dinev, & Cook, 2012). I used a framework consisting of top management, organizational culture, and planned behavior theory. The study participants consisted of MIS and MBA alumni from a large university. The study revealed a complementary relationship between organizational culture and top management in cultivating a climate of employee compliance to information security policies (Hu, Dinev, & Cook, 2012). Another finding was that perceived top management involvement directly influences organizational culture rule orientation and goal orientation by senior management, impacting the perceived cultural values (Hu, Dinev, & Cook, 2012).

### Cybersecurity Culture

In cybersecurity culture, researchers noted that computer systems and networks are standardized to a certain degree; however, the end-users are not; research indicates that human behavior is shaped and formed by cultural values (Sample, Cowley, Hutchinson, & Bakdash, 2017). From a business perspective, the cybersecurity domain is an interdisciplinary realm based on the practices of existing fields such as information technology, computer science, information security, accounting, marketing, strategy, finance, and risk management. Given the inclusion of preexisting practices and behavior into cybersecurity, according to Sample et al. (2017), the recent appreciation for behavioral sciences will enable business stakeholders to attain a more profound comprehension of phenomena such as phishing susceptibility. Fiske and Taylor (2013) alluded that the inclusion of cross-domain research potentially creates the risk of researchers interjecting their cultural viewpoints into the analysis.

A prominent university study explored cybersecurity culture by making everyone's responsibility, executive engagement and influence, active notices, a team approach, metrics, and

accountability (Madnick, 2018). The executives are responsible for fostering a cybersecurity culture to shape employees' security actions as worker behavior is essential for reducing cyber vulnerabilities (Huang & Pearlson, 2019). Existing literature highlighted a leading practice by organizations is investing in technologies while reluctant to increase spending on people (Huang & Pearlson, 2019). Disproportionate investing in employees reduces security resiliency and makes businesses more prone to cyber threats (Huang & Pearlson, 2019), such as phishing. Bauer and Bernroider (2015) indicated that information security awareness is a principal factor in illustrating compliance intention for enhancing positive security behavior.

In a study conducted by Da Veiga (2016), cybersecurity culture was deemed a critical factor in developing mitigating practices and security controls to increase protection and understand risk exposure. Da Veiga (2016) designed the cybersecurity culture research methodology (CSeCRM) to provide organizations with a standardized process for measuring cybersecurity culture integrated into the information security risk framework and assessment for documenting and evaluating the organization's cybersecurity culture. Madnick (2018) corroborated Da Viega's finding of needing to measure the effectiveness of cybersecurity culture.

The increasing number of cybersecurity attacks coupled with the mounting cost of data breaches, ransomware attacks, reputation damage (Ioannou, Stavrou, & Bada, 2019), insider threats, and human errors (Gaumer, Mortier, & Moutaib, 2016) adversely impede banks from developing robust security programs. Cybercriminals increasingly target banks as their motives continue to expand, including greed and ideology; even in an extensive regulated domain, banks struggle to keep pace with the changing cybersecurity threat landscape (Crosman, 2016). Tang

and Zhang (2016) noted that organizational culture impacts the security culture, given that culture is the most significant determining in whether a business succeeds or fails.

A gap in cybersecurity culture is the lack of scholarly research on its effectiveness in reducing phishing susceptibility in the U.S. banking sector. According to Abdelhamid (2020), “in 2019, about 30% of phishing e-mails still bypassed security detection measures. Phishing volume increased by approximately 41% in 2018, and the success rate of attacks has also increased” (p. 2). Another gap regarding cybersecurity culture is the implications of banking regulations on employee security behavior. This study will explore banking cybersecurity culture and its influences on reducing phishing susceptibility.

### Banking Cybersecurity Culture

The banking sector faces a constant barrage of cyber-attacks; thus, making cybersecurity a top concern for most banking institutions (Grasshoff et al., 2018). Security attacks against banks have increased by 80% since 2015, accompanied by the financial sector experiencing mounting organized and multi-vector attacks (Camillo, 2017) while undergoing digitalization, increasing risk by 70% (Aguayo & Ślusarczyk, 2020). Existing research indicates that banks struggle with cybersecurity culture and mitigating security risks because cyber remains siloed, a distant strategic requirement (Aguayo & Ślusarczyk, 2020; Grasshoff et al., 2018).

As banks leverage technologies, integrate new customer services, expand online platforms, implement remote working, and struggle to treat cybersecurity as a strategic risk, cybercriminals continue to outwit banks’ intelligent systems and capabilities (Aguayo & Ślusarczyk, 2020; Camillo, 2017; Grasshoff et al., 2018). Cybercriminals can gain access to a bank’s infrastructure and remain undetected for an average of 200 days (Grasshoff et al., 2018). Existing literature highlights the frailty of the banking sector’s cybersecurity resiliency (Aguayo

& Ślusarczyk, 2020; Grasshoff et al., 2018; Camillo, 2017), even with the banks' significant investments in cybersecurity, the institution remains vulnerable.

Researchers noted that the banking culture is hierarchical, bureaucratic, and slow to change while banks grapple with internal pressures from investors, competitors, and resistance to change (Kam, Katerattanakul, & Gogolin, 2013). Fagade and Tryfonas (2017) stated that banking and financial institutions function in a dynamic and complex landscape where risk management is an imperative and continuous interplay between malicious threats, information security readiness, and compliance. In the banking sector, it is essential to note that cybersecurity risk is a part of the holistic management of operational risk (Fagade & Tryfonas, 2017). Unmitigated threats and vulnerabilities could result in profit losses, unplanned time-consuming endeavors, brand damage, and operational setbacks.

External and insider threats continue to trouble the banking sector; however, customers' demands and expectations for mobile banking and easy access increase risk (Damenu & Beaumont, 2017). Despite the regulatory mandates (Kam, Katerattanakul, & Gogolin, 2013), banks are compelled to remain competitive by introducing new services while simultaneously increasing attack surfaces and security risks (Damenu & Beaumont, 2017). A study by Ula, Ismail, and Sidek (2011), concluded that banks must provide easily accessible and secure network connections and services to capitalize on new market opportunities.

The rapid development of technologies accompanied by technological deterministic thinking continues to mount pressure on banks to remain competitive. Existing research highlights that the banks should not be complacent as "societies are on the verge of deep transformation due to IT developments in social networks, communications, artificial intelligence, and big data analytics" (Jakšič & Marinč, 2019, p. 1). Aral, Dellarocas, and Godes

(2013) posited that the ongoing economic challenges are changing the banking industry with the (a) demand for hyperconnectivity, (b) widespread use of social networks, (c) the internet of things, (d) artificial intelligence, and (e) big data analytics are challenging existing banking and managerial practices.

As the business environment evolves, institutions must have a cybersecurity culture that responds to emerging technologies and threats (Aiken, 2019). Johnson (2019) avowed that banks are held accountable for cyber-attacks by financial regulators. Therefore, having a resilient cybersecurity culture is necessary to counter emerging threats and vulnerabilities. Marotta and Pearlson (2019) contend that as banks expand digital services such as internet banking and online applications, the number of threats targeting customers' personally identifiable information and financial assets increases. Senior leaders play a pivotal role in reducing threats by implementing and advocating for a cybersecurity culture (Marotta & Pearlson, 2019).

The literature underscores that certain banking operations contribute to the institution's vulnerability and inherent risk to cyber-attacks, such as cloud computing, third-party vendors, mobile banking applications, automated teller machines, and certain access points connections (Johnson, 2016). Despite banks continuously working to combat or mitigate emerging threats that evolve, a 2015 report by the Homeland Security Research Corporation indicated that the U.S. financial industry cybersecurity market reached \$9B, claiming the largest non-governmental market. Another side-effect of the growing concerns for cyber-attacks has led to some banks having extensive or unrestricted budgets to maintain a robust cybersecurity readiness (Johnson, 2016).

A prominent consulting firm indicated that banks suffered from a shortage of cybersecurity talent, issues with third-party management, and the absence of culture, which

prevents banks from reducing risks and building security resiliency (Grasshoff et al., 2018). Another problem that banks suffer from is integrating technology and human capital without increasing unnecessary risks (Grasshoff et al., 2018). Corradini (2020) declared that cybersecurity is no longer solely an information technology problem; cybersecurity threats and vulnerabilities are business problems and warrant budgeting and strategy support from the executive management team.

### Phishing

Phishing was coined in the 1990s as malicious actors used e-mail and instant messages as a fishing hook to attain sensitive customer information, login credentials, and billing data (Rekouche, 2011). Phishing attacks ascended in the mid-1990s, with cybercriminals leveraging American Online (AOL) to embezzle users' login credentials and sensitive information (Iuga, Nurse, & Erola, 2016). Gupta, Arachchilage, and Psannis (2018) corroborated the mounting phishing attacks in the 1990s as hackers tried to attack the Department of Defense in 1995. The mid-1990s marked an era in which phishing-related activities gained significant momentum, and early forms of discourse began to highlight the deceitfulness in stealing AOL customers' billing and login credentials (Rekouche, 2011; Gupta, Arachchilage, and Psannis, 2018).

Phishing events' sophistication continued to evolve through the 2000s as hackers spoofed websites to phish consumer information, conduct man-in-the-middle attacks, and deceptive messages (Rekouche, 2011; Alsayed & Bilgrami, 2017; Gupta, Arachchilage, and Psannis, 2018). Iuga, Nurse, and Erola (2016) purported that the advancement of technological solutions coupled with anti-phishing training and awareness has not slowed the continuous uptick in phishing attacks. Over the past decade, cybercriminals evolved and adapted new phishing tactics while employees remain increasingly susceptible to manipulation.

Phishing attacks predominantly use multiple phishing forms (see Table 1) during execution, such as using social engineering to survey a potential target to send an e-mail with a malicious link or attachment (VDBIR, 2020). Verizon's 2017 Data Breach Investigations Report indicated that successful phishing attacks in 2016 included malware installation on 66% of incidents (VDBIR, 2017). Banks are attractive targets for phishing attacks because these institutions create, process, and store extensive amounts of sensitive and confidential information and financial data (Kleitman, Law, & Kay, 2018). Existing literature reveals that humans' inability to detect online phishing attacks resulted in 90% of people becoming phishing victims (Kleitman, Law, & Kay, 2018). Researchers emphasized that technical solutions alone are insufficient to counter and mitigate increasingly sophisticated threats to the cybersecurity infrastructures (Conway et al., 2017). Table 1 lists the different types of phishing attacks that malicious threat agents use for phishing.

Table 1. *Types of Phishing*

<b>Type</b>	<b>Definition</b>	<b>Source</b>
Deceptive Phishing	The most used method to defraud account owners through deceptively claiming the need to verify account information, system failures, false charges, or free services to sign on to malicious links to enter login credentials so that cybercriminals can steal the end-user's login credentials.	Banu & Banu (2013); Chaturvedi & Mena (2016); Sukanva (2016)
Man-in-the-Middle Phishing	In this attack, the malicious threat agent places himself/herself between the user's system, phone, or device and the internet connection to collect a person's sensitive information or credentials to sell or use later.	Banu & Banu (2013); Chaturvedi & Mena (2016); Sukanva (2016)
DNS-based Phishing or Pharming	Pharming is an attack targeting to redirect website traffic to another phony site.	Banu & Banu (2013); Chaturvedi & Mena (2016); Sukanva (2016)
Keyloggers and Screen loggers	This attack uses malware forms that trace keyboard input in the backdoor and send important information to the malicious threat agent via the Internet.	Banu & Banu (2013); Chaturvedi & Mena (2016); Sukanva (2016)
Malware-based Phishing	This deception pertains to activating malicious software on a person's computer, smartphone, or devices. The malware is typically sent via an e-mail attachment as an executable file from a website for an issue for small and medium businesses (SMBs) who are challenged to keep their software applications current.	Banu & Banu (2013); Chaturvedi & Mena (2016); Sukanva (2016)
Session Hijacking	This is a phishing attack in which users' actions are observed until signing into an account compromising legitimate credentials. The threat agent uses malware to take over and execute unauthorized activities like transferring money without the account owner's permission.	Banu & Banu (2013); Chaturvedi & Mena (2016); Sukanva (2016)
Web Trojan	An attack in which a popup operates unbeknown to the computer user. Upon login, the threat agent steals the end-user's credentials during the phishing evolution.	Banu & Banu (2013); Chaturvedi & Mena (2016); Sukanva (2016)
Host File Poisoning	Entails modifying the operating system's host files that include the IP addresses corresponding to the websites.	Banu & Banu (2013); Chaturvedi & Mena (2016); Sukanva (2016)
Content-injection Phishing	In this type of attack, hackers will change the primary content with the counterfeit substance on the website, which misuses the user to give their confidential information.	Banu & Banu (2013); Chaturvedi & Mena (2016); Sukanva (2016)
Data Theft	This attack involves using malware to compromise the computer user's credentials and private and sensitive data such as credential card data and social security numbers.	Banu & Banu (2013); Chaturvedi & Mena (2016); Sukanva (2016)
Search Engine Phishing	Phishers establish fake websites and products to deceive consumers into providing their login credentials, addresses, and credit card data.	Banu & Banu (2013); Chaturvedi & Mena (2016); Sukanva (2016)

### Phishing Susceptibility

Phishing susceptibility is primarily an essential antecedent for measuring an organization's or individual's susceptibility to phishing attacks. Chen, Gaia, and Gaon (2020)

defined phishing susceptibility as the likelihood that a computer user would fall prey to a deceitful or illicit scam. Sommestad and Karlzén (2019) defined phishing susceptibility as the probability that an individual executes an action requested in a deceptive message. Dodge, Coronges, and Rovira (2012) classified phishing susceptibility as an indication that a person clicked on a suspicious link due to failure to identify the fraudulent scam, while Kleitman, Law, and Kay (2018) defined phishing susceptibility as the failure to identify a phishing e-mail. Phishing susceptibility is currently scarcely defined in scholarly research, even though there is a litany of studies investigating and exploring phishing susceptibility.

In an earlier study, Dhamija, Tygar, and Hearst (2006) denoted that people are susceptible to phishing attacks due to devaluing the significance of browser indications. Downs, Holbrook, and Cranor (2006) conducted a study that corroborated similar findings as Dhamija, Tygar, and Hearst. End-users revealed sensitive information via phishing e-mails that were perceived as coming from trusted stakeholders (Dhamija, Tygar, & Hearst, 2006). Sheng, Holbrook, Kumaraguru, Cranor, and Downs (2010) conducted extensive studies investigating phishing susceptibility and demographics, concluding that women are more susceptible to men regarding phishing attacks, given that women tend to be less knowledgeable on phishing. The researchers concluded that participants in the age range 18-25 have higher susceptibility rates of all groups due to less training and lower understanding of the phishing threat. Alsharnouby, Alaca, and Chiasson (2015) conducted a phishing susceptibility study, which indicated that end-users only identified 53% of phishing websites. I acknowledged that users disregarded security indicators and relied primarily on website content when evaluating websites' legitimacy (Alsharnouby, Alaca, & Chiasson, 2015).

Anawar, Kunasegaran, Mas'ud, and Zakaria (2019) indicated that understanding employees' phishing behavior is essential for developing countermeasures. Earlier research suggested that some employee characteristics could present a security threat to the enterprise (Anawar et al., 2019). Potential phishers can analyze an employee's e-mail interests and habits, enabled the prediction of e-mail activities for targeting, which increases the likelihood of phishing susceptibility (Zaki, Uddin, Hasan, & Islam, 2017). Existing literature indicates that phishing susceptibility fluctuates with workers' demographic variables, which in age and gender are the central factors that influence phishing susceptibility (Anawar et al., 2019). Sebescen and Vitak (2017) revealed that young employees are the most vulnerable and susceptible to phishing attacks. The longer employees stay at a job, the phishing susceptibility increases (Sebescen & Vitak, 2017), which corroborated Bandi's (2016) findings that younger individuals have riskier online security behavior than older people, and some literature indicated that women are more susceptible than men. Darwish et al. (2012) argued it could be that women have more congenial personalities and demeanor, while Sheng et al. (2010) contended that it was due to women having lower technical proficiency and skills than men.

Current literature consists of a litany of studies on personality traits and phishing susceptibility and the interrelatedness to different theoretical viewpoints (Anawar et al., 2019). Abdelhamid (2020) contends that research studies on personality-based factors and linkage to actions, attitudes, and intentions have been examined in many situations (Abdelhamid, 2018; Hansen, Saridakis, & Benson, 2018; Wang, Ngamsiriudom, & Hsieh, 2015). Bandi (2016) leveraged the Big Five Personality Model to investigate the connection between personalities and online security behavior that influence organizational culture security, such as password creation and device protection. Bandi (2016) concluded that conscientiousness, extraversion, and risk

avoidance are significantly linked to online security behavior. However, no study on personality-based factors has been conducted on banking employees in the U.S.

### National Culture and Security Behavior

Existing research indicates that national culture plays a substantial role in influencing security behavior and organizational culture (Hofstede, 2001; Connolly, Lang, & Tygar, 2015). It is important to note that some banks in the U.S. operate internationally; therefore, the interplay between international and national cultures is essential. The intersectionality between international and national culture could impact the organization's information security culture. Ali and Brooks (2008) lamented that national culture is commonly accepted foundational values, customs, and traditions that shape people's security behavior within that society. Karahanna, Evaristo, and Srite (2003) postulated that the management information system domain cross-cultural suffers from (a) the lack of theory, (b) inclusion of culture as an antecedent, and (c) ameliorating methodologies. These implications impeded the advancing of empirical research on phishing susceptibility in the U.S. banking sector. Limited research revealed that cross-cultural differences resulted in increased phishing susceptibility (Flores, Holm, Nohlberg, & Ekstedt, 2015; Gcaza, von Solms, & van Vuuren, 2015; Huang & Pearlson, 2019; Tembe et al., 2014). Pavlou and Chai (2002) echoed similar sentiments of scarce research regarding cross-cultural dimensions accompanied by an urgent demand to increase empirical research in this area.

The research highlighted that factors such as (a) human capital, (b) literacy rates, and (c) domestic income levels were critical in shaping national cultures and the influence on information security (Gregorio, Kassicieh, & Neto, 2005). Researchers emphasized that national culture influences organizational learning (Kim & McLean, 2014), resulting in increased innovation and growth. Marquardt, Berger, and Loan (2004) argued that national culture

influenced learning because countries strongly advocate for (a) language integration, (b) mass media, (c) regulations, (d) academia, (e) political affairs, (f) athletics, and (g) the economy. National culture is stymied because lower-level employees are attracted and influenced by the personal culture rather than the corporate culture (Govender, Kritzinger, & Loock, 2016).

Existing literature indicated that national culture is vital for businesses to maximize information security and privacy, especially for norms and values (Björck & Jiang, 2006; Chen, Medlin, & Shaw, 2008; Schmidt et al., 2008; Ifinedo, 2014). Björck and Jiang (2006) studied discovered that cultural attributes impacted the evaluations of information security implementations. Researchers determined that evaluating American and Chinese cultures revealed disparities in awareness of information security threats (Schmidt et al., 2008). Dinev et al. (2009) disclosed that national-level culture deviations helped determine user behavior regarding cybersecurity protective technologies in the U.S. and South Korea. Johnston, Warkentin, and Luo (2009) found that national culture to be a critical factor for comprehending privacy matters and organizational obligation.

Some researchers oppose that national culture is not an essential factor for information security-related matters. Ifinedo (2008) revealed that financial institutions are prone to increased influences from interior and industry matters rather than from national culture regarding security and privacy concerns. The study suggested no statistical disparities of information security and privacy issues across different world regions when examined by contextual factors such as socio-economic and national culture (Ifinedo, 2008). The lack of statistical disparities indicates that financial service institutions implement analogous security practices (Ifinedo, 2008). Milberg, Smith, and Burke (2000) conducted a study on approximately 900 study participants and

discovered no security and privacy disparities when investigating three national cultural dimensions.

Cross-cultural factors are examined primarily using three models by Hofstede (2001), Schwartz (2006), and GLOBE (2004); consequently, there was extensive controversy regarding the objectivity and content of each model even though there was overlap in the models (Govender, Kritzing, & Loock, 2016). Hofstede (2014) is the predominantly used cross-cultural framework, which investigated the five following dimensions: (a) power distance, (b) individualism versus collectivism, (c) masculinity versus femininity, (d) uncertainty avoidance, and (ee) pragmatism and indulgence. Researchers noted that it is impossible to test for all possible cultural dimensions and relationships when investigating national cultures and information security (Flores et al., 2015).

#### Studies on Phishing Susceptibility and National Culture

Even though national culture implications on phishing susceptibility are underexplored, a few studies highlight the phenomenon. An empirical survey by Tembe et al. (2013) investigated the cross-cultural dimensions of national culture between Americans and Indians. The investigation disclosed that Indians were successfully phished more than Americans and that Indians indicated questionable online security behavior. Americans recognized secure websites while Indians struggle to emphasize privacy and destroy documents containing sensitive data. According to Tembe et al. (2013) revealed that Indians struggled with maintaining positive security behavior online compared to Americans.

In a quantitative survey, Tembe et al. (2014) investigated American, Chinese, and Indian phishing susceptibility based on national culture. The study revealed that a difference in internet behaviors and comprehension of phishing amongst the three groups. The findings indicated that

Indians are more susceptible to phishing than the Americans and Chinese; however, Americans were more cautious about phishing attacks than the Chinese and Indians. The findings suggested that the Chinese and Indians were not sensitized to the potential harms of phishing. At the same time, Americans were more mindful of privacy and recognizing secure websites than the Chinese and Indians. The Americans and Chinese practiced destroying documents containing sensitive information while the Indians were not attuned to this security practice. Overall, the study highlighted that Americans were more aware of the phishing phenomenon than the Chinese and Indians, thus, highlighting cross-cultural differences.

Flores et al. (2015) conducted a study on employee resistance to phishing between Americans, Indians, and Swedish study participants, which indicated a difference between the groups. The results suggested that the Swedish employees' general information security awareness and intention were significantly correlated to behavior while non-significant for the Americans and Indian employees. The Swedish and American samples had a significant correlation between formal training and phishing resistance, with the American population being the strongest while the Indian sample was non-significant. The researchers annotated the above cumulative outcome as a result of the following cultural dimensions: (a) individualism, (b) masculinity, (c) uncertainty, (d) uncertainty avoidance, (e) pragmatism, and (f) indulgence (Flores et al., 2015). The authors noted that the difference is because U.S. senior security managers customarily leverage formal training to maximize information security, which is not the case for Swedish and Indian entities (Flores et al., 2015). In summary, the results revealed that national culture affects phishing determinants, and the workers' observed phishing behavior varies between Swedish, American, and Indian employees in 6 out of 15 incidents.

## Gaps in Literature

After several decades, phishing susceptibility remains an aggressive threat to U.S. banks. According to Hu, Hart, and Cooke (2012), there are research gaps associated with information security culture and executives. First, even though there are numerous studies on information security and organizational culture, the studies failed to illustrate the linkage of organizational culture's theoretical underpinnings to information security results (Hu, Hart, & Cooke, 2012). Second, the lack of scholarly data on the banking sector makes it difficult to understand the industry from an academic perspective. Third, there is a need to investigate banking employees, cybersecurity culture, and the factors for reducing phishing susceptibility to deeper understand the banking sector. Currently, researchers do not have a clear comprehension of phishing susceptibility in the U.S. banking sector.

## CHAPTER 3

### STUDY 1

#### Research Method, Design, and Findings

The purpose of this qualitative interpretive study is to explore banking cybersecurity culture's influence on phishing susceptibility. The interpretive qualitative approach is used in many domains and disciplines. Creswell (2007) proclaimed that interpretive quality research is used to explore problems by understanding a phenomenon's meanings or a social or human-related issue experienced by an individual or a group. The interpretive approach provides profound awareness into the complicated world of lived experiences from the study participants' points of view (Díaz Andrade, 2009). Interpretive research is designed to educate and inform through inductive, hypothesis, or theory-building processes instead of a deductive approach (Merriam, 2009).

Qualitative interpretive research is a vehicle in which the researcher helps the study participants construct social reality through social interaction between the researcher and the participants (Díaz Andrade, 2009). The researcher's role is critical for interpreting and enhancing the subjectivity with quality arguments rather than statistical accuracy (Mingers, 2001). The basis of qualitative interpretive research is "that our knowledge of reality is gained only through social constructions such as language, consciousness, shared meanings, documents, tools, and other artifacts" (Klein & Myers, 1999, p. 69), in which the researcher acts as a "passionate participant" (Guba & Lincoln, 1994, p. 115). Merriam (2009) posited that the purpose of interpretive research is making sense of a situation, how people interpret experiences, and how individuals construct their worlds based on the interpretation of experiences.

Ferranto (2013) stated that interpretive constructionist researchers set out to explore the common meanings by realizing that each person interprets their experiences distinctively due to individual interpretation of life experiences and socio-cultural influences. In interpretive research, the individuals' interpretations stem from their everyday experiences, which provide the meanings. The meanings from the interpretations are based on the participants' experiences and making sense of the experiences rather than discovering the interpretations. Merriam (2002) contended that the researcher's role is not to uncover the meanings of the participants' experiences; instead, the researcher helps clarify the interpretations derived from research participants.

The researcher explored the study participants' experiences of how the banking information security culture decreased phishing susceptibility. The study participants in this interpretive qualitative study provided specific and thick descriptions of their habits, internal perspectives, and meanings. Given the exclusivity of the banking environment, the study participants' experiences with how banking information security culture decreases the susceptibility to phishing coupled with time and geographical constraints preclude the use of other qualitative designs; therefore, the interpretive qualitative approach is the most suitable.

#### The Role of the Researcher

A qualitative interpretive inquiry relies upon the research participants' information and the researcher's meaning from the study participants' ascribed experiences. I played a critical role in analyzing and interpreting the meaning of the information throughout the data collection and data analysis phases. My expertise as a cybersecurity professional who is employed in the banking sector aided in interpreting the meaning of the information. Given that this is an interpretive study, I purposely interjected my professional assessment when necessary to

determine the information’s meaning. With first-hand experience of the phenomenon, phishing susceptibility, I provided in-depth explanations and further clarifications as necessary but without detracting from the participants’ thick descriptions.

### Data Collection and Analysis

#### Research Study Participants

Seven security and technology executives were recruited using purposeful and snowballing sampling techniques to find senior leaders currently employed in the banking industry. The security and technology executives were given a pseudonym to maintain their privacy. Table 4 provides a complete list of the research participants used for this study. I provided minimum data on the research participants to protect their privacy.

Table 2. *Participant Study Data*

Participant ID	Title	Interview Length	Sex	Experience in Years
EXC-1	V.P. InfoSec	68:17	M	17
EXC-2	Sr. Dir, Cybersecurity	51:29	M	28
EXC-3	V.P. Sec Architecture	62:32	F	15
EXC-4	Chief InfoSec Officer	53:41	M	25
EXC-5	SVP, Info Tech	48:54	F	22
EXC-6	SVP, Cyber Engineer	43:22	M	30
EXC-7	Group CIO	57:08	M	33

#### Research Methodology Applied to the Data Analysis

The qualitative interpretive methodology was the research design used to frame this study. Data was collected through semi-structured interviews with demographics and open-ended questions. All interviews were recorded using Zoom online video or audio for face-to-face interviews. Subsequently, all interviews were uploaded to Trint, an online automated

transcription service in which I checked the transcript for accuracy and forwarded it to the research participant for approval. Next, I manually conducted data analysis on the transcripts using qualitative content analysis. I reviewed and coded each transcript three times, including coding, to identify the categories, groups, and major themes. I used documents, notes on body language, and interviews in the data analysis to arrive at the three major themes.

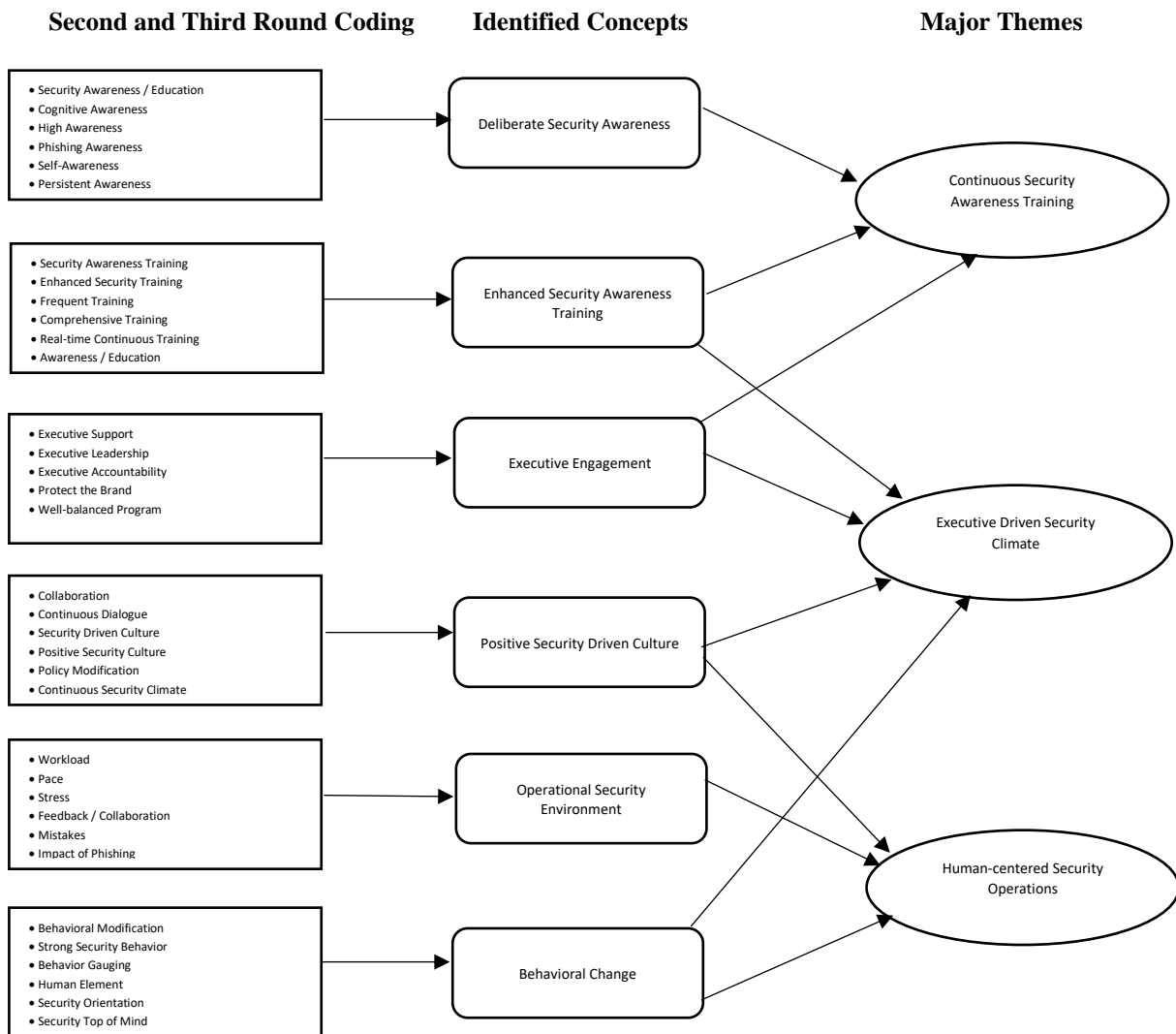


Figure 1. High-level Depiction of Coding to Attain the Major Themes

I read each transcript three times before commencing the coding evolution. I interpreted the transcript information's meaning related to the research question into high-level themes into categories during the initial coding. The coding was documented in the right margin. During the second coding evolution, I tested the coding scheme on three interviews by analyzing how the categories and concepts answered the research question and evaluating the coding for consistency. Figure 1 depicts the first and second rounds of coding and the identified concepts, which is the third round of coding. Next, I finalized the major themes and used lines to connect and illustrate how the identified concepts aligned to the themes (see Figure 2). Table 5 provides descriptions of the identified themes and representative quotes to define and understand the identified themes. The purpose of Table 5 is to assist in connecting the qualitative content analysis process with the presentation and reporting of the major themes. The three themes that emerged from the data analysis are (a) continuous security awareness training, (b) executive-driven security climate, and (c) human-centered security operations.

Table 3. *Six Themes Emerging from the Data Analysis*

Identified Theme	Description of Emerging Theme	Representative Quotes
Deliberate Security Awareness	Heightened alertness to security climate and environment to prevent malicious activity in the physical and logical spaces	<i>Phishing is a top threat to banking (EXC-4)</i> <i>Employees must fight the urge to click (EXC-7)</i> <i>We must expect that every e-mail is bad (EXC-2)</i>
Enhanced Security Awareness Training	A comprehensive awareness training program aimed at increasing situational understanding of security threats	<i>Adaptive training to reflect the climate (EXC-1)</i> <i>More frequent and real-world training (EXC-3)</i> <i>Increased simulated phishing attacks (EXC-4)</i>
Executive Engagement	Senior managers leading, resourcing, and actively setting and participating in the security culture	<i>Executives need to set the example (EXC-3)</i> <i>Executives are in charge of the culture (EXC-6)</i> <i>Executives provide required resources (EXC-5)</i>
Positive Security Culture	A climate of reinforced security practices that align with security policies and the organizational culture	<i>We must adhere to security practices (EXC-7)</i> <i>A security-driven culture is critical (EXC-7)</i> <i>Security increases collaboration (EXC-3)</i>
Operational Security Environment	The environment where the physical and logical components connect during cybersecurity operations	<i>The security pace is fast/unforgiving (EXC-5)</i> <i>Phishing attempts are always occurring (EXC-1)</i> <i>The threats are endless/unpredictable (EXC-2)</i>
Behavioral Change	The mental state of employees in the security environment and the ability to be flexible and compliant	<i>Employees adapt to the environment (EXC-3)</i> <i>Emotional intelligence is necessary (EXC-2)</i> <i>Punishing employees is not the answer (EXC-5)</i>

### Presentation of Data and Results of the Analysis

Five demographics type questions preceded the seven interview questions, which were used to answer the central research question: How does banking cybersecurity culture decrease phishing susceptibility? From the data analysis, the following themes emerged: (a) continuous security awareness training, (b) executive-driven security climate, and (c) human-centered security operations. Table 4 provides insight into understanding the three major themes emerging from the data analysis, description of the topics, and representative quotes that tie directly to the theme.

Table 4. *Three Major Themes Emerging from the Data Analysis*

Major Theme	Description of Major Theme	Representative Quotes
Continuous Security Awareness Training	A sustained level of training geared towards increasing employees' situational insight through heightened cognitive abilities by mastering phishing training objectives	<i>Interactive training on a routine basis (EXC-6)</i> <i>Awareness increased through training (EXC-5)</i> <i>Cyber readiness is vital for banks (EXC-4)</i>
Executive Driven Security Climate	A cybersecurity culture is driven by executives and meticulously resourced to ensure employees are trained and aware of the physical and logical environment related to mitigating phishing.	<i>Executives need to be held accountable (EXC-2)</i> <i>The culture is set from the top down (EXC-3)</i> <i>Executives own the threats (EXC-7)</i>
Human-centered Security Operations Center	A deliberate approach to account for human weakness by placing people at the center of cyber operations and building processes and policies to drive behavioral and attitudinal adjustments to lessen phishing susceptibility	<i>There needs to be more focus on people (EXC-6)</i> <i>Behavioral modification is paramount (EXC-1)</i> <i>Employees need emotional intelligence (EXC-1)</i>

### Conceptual Framework

The conceptual model below depicts the major themes as antecedents and propositions. The conceptual model describes that executives can positively influence banking cybersecurity culture, which drives continuous security awareness and training and human-centered security operations to reduce phishing susceptibility. The linkage between executive influence and banking cybersecurity culture indicates dual interplay, given that executives are responsible for establishing the culture and can initiate changes to the culture as necessary to reduce phishing susceptibility. These changes directed by the executives can directly influence continuous security awareness and training and human-centered security operations. As depicted, continuous security awareness training and human-centered security operations can result in reduced phishing susceptibility. The linkage between reduced phishing susceptibility and executive indicates a feedback loop or mechanisms for executive leaders to implement changes to ameliorate the cybersecurity culture. Without this linkage, the bank could potentially miss the

opportunity to make adjustments to the banking cybersecurity culture, especially with the cyber threat landscape being hyperactive and unpredictable.

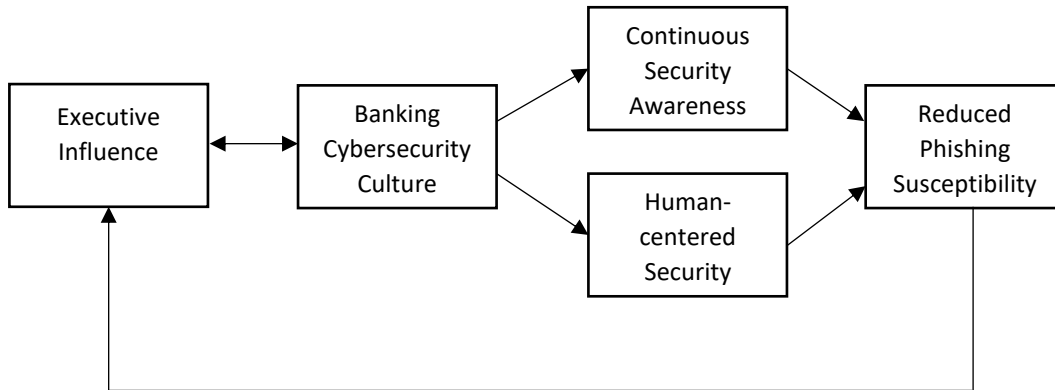


Figure 2. Conceptual Framework: Reducing Phishing Susceptibility Through Executive Influence and Culture

### Continuous Security Awareness Training

A key theme that emerged from the data analysis was the importance of continuous security awareness training in reducing phishing susceptibility. Every research participant commented on how banking cybersecurity culture makes it mandatory to undergo numerous security training sessions throughout the year. Participant EXC-1 stated, “Train your employees and let them contribute to the security culture and do not make the employees dependent but rather as change agents to expand the importance of having a security-minded approach.” Participant EXC-1 further expounded that phishing is wreaking havoc on banks, so we have implemented simulated phishing campaigns and training programs. Participant EXC-2 stated, “The only way to reduce phishing attacks is to establish a security-driven culture with rigorous security awareness and training requirements that are enforced through continuous dialogue and increased frequency levels of training.” Participant EXC-6 asserted, “Phishing susceptibility is reduced through continuous learning, adaptive and interactive training, real-time training events,

and positive security culture.” Participant EXC-7 stated, “we should simulate phishing attacks until we get it right to enhance security awareness, accountability,.....employees that handle sensitive information should undergo more stringent security training.....train all employees on the impact of a phishing attack on the bank”.

All the research participants indicated high regard for security awareness training and a high level of awareness, given the sophistication of phishing attacks. It is assessed that continuous security awareness training increases bank employees’ security awareness, aiming to reduce phishing susceptibility.

#### Executive Influence

Another important theme that emerged from the data analysis is executive driven security culture, which the study participants deemed critical in reducing phishing susceptibility. Participant EXC-7 stated, “As executives, we just unintentionally clicked on things just because we are moving so quickly that is not until like two minutes later, we are surprised about clicking on a malicious link.” Participant EXC-4 indicated that “Leadership plays a critical role in increasing the bank’s phishing awareness, especially since e-mail remains a primary attack vector for targeting executives.” Participant EXC-4 avowed that “Executives are responsible for policy development to drive the behavioral modification and compliance that is necessary to reduce phishing.” Participant EXC-3 stated, “It is not enough for executives to just drive the culture senior managers need to lead security training sessions and show the visible involvement in increasing awareness through security training.” Participant EXC-7 mentioned that the executives are directly responsible for protecting the brand; therefore, in the case of phishing, it means allocating resources, providing oversight, and staying engaged in helping establish a

security culture to prevent phishing attacks. Participant EXC-4 stated a similar comment “Phishing incidents are too costly and damage our brand and interrupt banking operations.”

Participant EXC-5 stated, “Since I have been at the bank, I have observed a constant improvement in the culture and executive engagement in establishing the culture; however, the next hurdle for executives is increasing transparency about cyber threats throughout the banks.” Participant EXC-7 declared that “The bank is very siloed, which in turn hurt the transparent culture we are trying to establish.” Participant EXC-1, an information security executive, stated, “Banks are a pretty private group. We do not like bad information getting out; we believe in defense of secrecy. The less you know about my organization and how it operates, the less likely you are to break into it.” Regarding establishing a resilient cultural approach to phishing, Participant EXC-4, a Chief Information Security Officer, stated, “Every month, during a meeting, we discuss here is what we got going. Here is what we see out on the web. We are continually attacked. This open collaboration keeps it at the forefront of people’s minds.

Executive-driven security culture is a fundamental capability for reducing phishing susceptibility through cultivating a strong and positive climate to protect the brand and the bank from the constant barrage of phishing and cyber threats.

### Human-centered Security Operations

Another theme that emerged from the data analysis is human-centered security operations, given that humans are considered as the weakest resource in cybersecurity. Participant EXC-3 proclaimed that “From a human behavior perspective, I think people can be aware of information security policy until they actually have to make a choice about it. It is convenient or not.” Participant EXC-2 stated, “I think we focus too much on just the technical side and not enough on the people's side. We miss that the message is not clear. This is why I

think the phishing numbers continue to increase.” Participant EXC-6 confirmed, “The human element is really what it is. The human element is what makes us susceptible. So our mind is an intriguing mine, and we also have a defending mind so we can protect ourselves.” Participants EXC-6 and EXC-7 called the human inclination to click on malicious sites even after undergoing training as a low-level of emotional intelligence. Participant EXC-7 stated, “The sense that our schedules are so hectic, and we are always trying to keep up with the pace makes us more susceptible to phishing due to having a fast pace schedule and operational tempo.” Participant EXC-2 replied that “We do not educate our team members or employees the way we need to. People just by habit, they will click things so quick things and will not think about it until it is too late.”

Several of the participants raised the issue of neglecting the human element in cybersecurity because there is too much emphasis on the technical aspects, while the employees continue to suffer. Several participants alluded to banks being quick to terminate employees for making a mistake instead of implementing an effective training program. Participant EXC-6 stated, “It is human nature to be intrigued. But we do not touch the stove because it is hot. You just must pause. You know what to do. We are just intrigued and want to do differently.” Participant EXC-2 asserted, “We operate from a fear-based perspective, and most of the time when bad things happen, we are quick to terminate rather than try to train the employees.” Participant EXC-3 stated, “If companies can develop a culture of training and partnering in the cybersecurity training, I think they will be more successful than using the fear culture method.”

Some security policies implemented by banks adversely impact cyber operations. Participant EXC-5 stated, “So as an example, last week we had to do presentations, and we wanted to make exceptional products, but we were prohibited from importing MP4 files, so it

impacted the quality of our work.” Regarding policies, Participant EXC-3 stated, “If bank employees can get away with not maintaining policy compliance, they will risk it to get the job done..... I am talking about the non-malicious user who is prioritizing work over information security.” Participant EXC-1 commented that “Security policies often fail to modify bank employees’ behavior and result in policy non-compliance and sidestepping.” This theme highlights the significance of human-centered security operations, emphasizing placing bank employees at the center of the cyber operations and safeguarding through effective policies and security controls.

## Discussion

This qualitative interpretive study aimed to explore cybersecurity culture and its influences on phishing susceptibility in the banking industry. There is a lack of empirical research on banking cybersecurity culture and its influences on phishing susceptibility; therefore, I intended to increase discourse around this pertinent topic and produce scholarly work towards reducing the research gap. This study aimed to facilitate the understanding of cybersecurity culture and its effects on phishing susceptibility. This study revealed some practical findings related to banking cybersecurity culture and its influences on reducing phishing susceptibility. The study findings indicated that (a) executive influence, (b) continuous security awareness training, and (c) human-centered security operations are essential practices for reducing phishing susceptibility in the banking sector through cybersecurity culture.

### Executive Influence

A previous study determined that a complementary relationship exists between organizational culture and top management in cultivating a climate of employee compliance to information security policies (Hu, Dinev, & Cook, 2012). This study revealed that banking executives are responsible for establishing and maintaining a culture of cyber readiness to

increase diligence; maintain a high level of awareness and readiness because the threat is continuous. Executives are the direct target of phishing tactics (spear-phishing/whaling); therefore, executives are the lead agents for influencing cyber hygiene.

Earlier research highlighted two essential features (a) organizational culture influences the attitudes and behavior of employees through values to ascertain commitment and (b) that corporate leadership is vital in cultivating the business culture through manipulation by the senior management (Smircich, 1983). Executive leaders influence the cybersecurity culture by marketing the need for continuous and increased awareness of contemporary phishing tactics. Executive engagement ensures adequate resources to develop an effective phishing program that mandates continuous phishing training and awareness. Providing comprehensive phishing awareness and training is not enough; executives need to ensure that employees understand the impact and ramifications of a successful phishing attack on the business. Executives have to ensure that the security culture is transparent, non-siloed, mandates leadership accountability, and prioritizes security requirements.

This study revealed that executive leadership, accountability, presence, and constant engagement are essential for establishing a positive security culture and reducing phishing susceptibility and setting a supportive tone from the top.

### Banking Cybersecurity Culture

In a study conducted by Da Veiga (2016), cybersecurity culture was deemed a critical factor in developing mitigating practices and security controls to increase protection and understand risk exposure. Banking cybersecurity culture capitalizes on heightened regulatory requirements in the banking sector to solidify critical assets protection. Banking cybersecurity culture is everyone's responsibility, from the top executives to the newest employee, proliferated through a mutual sense of accountability. Researchers noted that the banking culture is

hierarchical, bureaucratic, and slow to change while banks grapple with internal pressures from investors, competitors, and resistance to change (Kam, Katerattanakul, & Gogolin, 2013).

Banking cybersecurity culture aligns with the organizational culture and instills shared values increased awareness, regulatory and policy compliance, and positive security behavior as a mechanism to reduce phishing susceptibility.

This study revealed three negative aspects of the banking cybersecurity culture; first, there is too much focus on phishing attack methodologies and not enough attention to continuously training employees. Second, banking cybersecurity culture supports the use of scare tactics to curtail poor security behavior. Third, the banking cybersecurity culture is not driving a climate of continuous learning; hence, making employees susceptible to phishing

#### Continuous Security Awareness Training

Research indicated that most people are prone to phishing attacks, even the most experienced professionals (Dhamija, Tygar, and Hearst, 2006). Given that the banking sector's threat landscape is constantly under attack from phishing attempts, continuous security awareness and training are necessary to reinforce positive security behavior and enhanced alertness to combat phishing attacks. For security awareness and training to achieve high-level effectiveness, banks need to provide various training and simulated phishing attacks based on real-world threats. Phishing awareness and training should vary based on the employee's risk profile, individual security training weakness, and organizational trend data. Phishing awareness and training need to occur continuously, including real-world examples that are practical, relatable and tailored to the banking environment. The training needs to address phishing's impact to enhance bank employees' understanding of the financial, operational, and social fallout. Achieving a high state of continuous awareness should be commensurate with the phishing threat level and led by executives to highlight the significance.

## Human-centered Security Operations

Existing research indicates that men and women have various weaknesses that make each gender prone to phishing susceptibility (Downs, 2010). Banking executives need to address the importance of emotional intelligence and the impact on the employees' psyche. The operational pace, stress, and constant phishing attacks on banks can adversely impact employees.

Unaddressed stress could result in banking employees having reduced cognitive awareness; consequently, increasing phishing susceptibility. The banking environment needs to improve efforts to account for the human element in cybersecurity operations because the lack of prioritization, constant stress and continual policy and technology changes makes employees vulnerable, not just to phishing attacks but all forms of security attacks. The banking security environment is intense and demanding; however, employees are prone to phishing susceptibility and human error without countermeasures to lessen the impact. Considering the complexity of banking operations, failure to implement human-focused security operations could result in operational stress, fatigue, poor security practices, and increased phishing susceptibility.

Even though this study provides insights into the phishing susceptibility phenomenon, what is unknown is the perspectives of cybersecurity professionals and non-technical employees in the banking sector on organizational culture, cybersecurity culture, training, and phishing susceptibility. An additional qualitative study using the same interview questions will further expand the scope of the study. This study only captured the views of technology and security executives. Exploring the viewpoints of cybersecurity professionals and non-technical employees might provide different findings than the executives. Investigating phishing susceptibility and cybersecurity culture from small banks, mid-size banks, and large banks are worth investigating to determine the differences by leveraging a mixed-method approach. A large-scale mixed-method study exploring and examining the Conceptual Framework (Figure 3) is worthwhile for

determining the reliability or modify the framework based on the study's findings. More studies using a larger sample size of banking employees are needed to understand banking cybersecurity influences on phishing susceptibility.

## CHAPTER 4

### STUDY 2

#### Research Method, Design, and Findings

The purpose of this grounded theory study stemmed from the qualitative interpretive inquiry as a need to develop theory based on the lived experiences of the study participants. Study 1 emphasized the need for theory to understand phishing susceptibility in the banking sector. I expanded the study participants to include security and technology executives, cybersecurity professionals, and non-technical employees to gain a holistic understanding of the phenomenon. As reported by the APWG (2020, 2020a), the banking sector remains a highly attacked industry for phishing; consequently, the banking sector needs theory to reduce the theory and practice gap.

According to Creswell (2014), there are multiple methodologies to execute research. The research methodology was based on the research questions asked (Bryant, 2003). This qualitative research study explored the study participants' experiences of how cybersecurity culture decreased phishing susceptibility using a grounded theory methodology (GTM). This chapter discussed the research methodology and design for this research inquiry. This chapter included how I employed the research methodology, the research instrument, population, sample size, data collection, and data analysis.

Creswell (2014) postulated that constructivists direct comprehensive questions that persuade study participants to offer enriched answers, which create meaning for a particular situation. The responses provided by the study participants must be riched in facts to support a comprehensive exploration of banking cybersecurity culture influences on phishing susceptibility. According to Corbin and Strauss (2015) noted, qualitative research encourages

investigation into the lived experiences of study participants to reveal the variables involved and derive meaning from their experiences. The information gathered during the data collection was necessary to explore the effects of banking cybersecurity culture and its impacts on the employees' phishing susceptibility. Merriam and Tisdell (2016) underscored that the foundation of qualitative research rests with "the belief that knowledge is constructed by people in an ongoing fashion as they engage in and make meaning of an activity, experience, or phenomenon" (p. 23). This study primarily explored interrelationships and constructed meaning based on the 34 study participants' responses where variables were unknown and no understanding of the themes that emerged through the adopted qualitative approach.

### Overview of Research Methodology and Design

Prominent scholars indicate that researchers should classify their worldview as a central element of all research inquires (Creswell & Creswell, 2018). Creswell and Creswell (2018) acknowledged four different worldviews: (a) postpositivism, (b) constructivism, (c) transformative, and (d) pragmatism. The constructivist worldview is typically used with qualitative research inquiries because this paradigm is based on developing or generating theory based on observations rather than starting with theory (Creswell & Creswell, 2018). For this inquiry, based on the above suppositions, I used the constructivist worldview.

Glaser and Strauss (1967) were the first scholars to purport GTM; consequently, the researchers took on different approaches after a public disagreement regarding practical issues of GTM (Urguhart, Lehmann, & Myers, 2009). Some researchers refer to the two distinct approaches as the "classic" and "evolved" progression of GTM (Matavire & Brown, 2017). Contemporary researchers classified work by Charmaz and other GTM contributing scholars as aligning to the "evolved" group (Matavire & Brown, 2017); hence, the methods used for this inquiry. According to Charmaz (1995), GTM is applicable for qualitative and quantitative

research approaches (data). An essential element of GTM is the strong emphasis on theory development and enabling researchers to seek different levels of theory throughout the data collection process (Denzin & Lincoln, 1994). By employing GTM, researchers can find concepts substantiated in collected data and determine their fundamental sources (Corbin & Strauss, 1990). Glaser and Strauss (1967) contended that GTM is applicable for developing new theory by concentrating on the disparities between day-to-day experiences of activities and how those actions and experiences are translated through the lived experiences (Suddaby, 2006). Urquhart and Fernández (2013) postulated that GTM could manufacture high-level theories that are generalizable and practical. There is currently a dearth of theory regarding phishing susceptibility in the U.S. banking sector and a paucity of theory on how cybersecurity culture influences the reduction of phishing attacks. The use of a GTM provided a mechanism for answering the research questions for this inquiry.

This research aimed to explore the influences of banking cybersecurity culture on reducing phishing susceptibility to discover meaning and facilitate explanations for phishing instances occurring in the U.S. banking industry. The research was not intended to discover an outright reality, alter a particular condition, or indicate a solution to the situation.

Inductive reasoning was used to describe situations revealed through data analysis accumulated from study participants (Creswell, 2014). Inductive reasoning entails examining data or evidence to build meaning, which can help clarify situations that have the likelihood of being true (Feeney & Heit, 2007). Constructing meaning from data attained from the study participants' replies and understanding why a specific situation exists is aligned with a constructivist worldview.

## Research Methods

I used the constructivist grounded theory to develop a practical theory through an iterative process of collecting, coding, and contrasting data based on my interpretation (Charmaz, 2014). The constructivist grounded theory manifested upon the tenets of constant comparative methods and theoretical sampling (Bloomberg & Volpe, 2012; Charmaz, 2014).

Constant comparative methods. The constant comparative method consisted of iterative and synchronized procedures for data collection and analysis (Cho & Lee, 2014; Glaser & Strauss, 1999). In this inquiry, constant comparative analysis was performed during all phases of coding and involved comparing data to data, data to codes, codes to codes, codes to concepts, concepts to concepts, concepts to categories, and categories to categories to detect similarities and variances which enabled the emergence of themes (Birks & Mills, 2011; Saldana, 2016).

Theoretical sampling. The targeted population for selecting study participants comprised of current banking employees in the U.S. and in a position to respond accurately to questions about banking cybersecurity culture and phishing susceptibility in the banking sector. Theoretical sampling entails the practice of gathering data from participants who lived experience with the phenomena being explored or an individual with a different attribute to be explored (Cho & Lee, 2014; Glaser & Strauss, 1999). Theoretical sampling was achieved by interviewing study participants who possessed varying security and technology executives, cybersecurity professionals, and non-technical employees actively employed in the banking industry. The theoretical sampling premises was to confirm areas that needed additional data collection so concepts already discovered through comparative methods could fully evolve (Charmaz, 2014). Theoretical sampling consisted of purposefully sampling study participants to obtain further information pertinent to the researched concepts (Corbin and Strauss, 2015). Purposeful sampling was conducted with the targeted

population. Demographics data were used to ascertain a diverse sample population to ensure categories would contain a broader number of viewpoints.

#### Instrumentation

I used an Interview Question Guide (Appendix B), which consisted of demographic questions and interview questions specifically aimed to gather data on the study participants' lived experiences of the phenomenon. The interview questionnaire provided some structure to start the semi-structured interviews and provide alignment with corresponding responses to the research questions. The Interview Question Guide consisted of six interview questions and one follow-on to give a course during the interviews; however, I asked probing and follow-up questions to gain deeper insights into the participants' lived experiences throughout the interviews.

#### Population Description

The sample population for this study consisted of individuals who were currently employed in the banking sector. The population sample consisted of three groups (a) technology and security executives, (b) cybersecurity professionals, and (c) non-technical employees, as depicted in *Table 5*. Additionally, the population needed sufficient experience in the bank's phishing countermeasures, security awareness, security training, and phishing policies. For this purpose, I inquired about the study participant's experience with the bank's anti-phishing program.

Table 5. *Research Participant Groups, Definitions, and Phishing Functions*

<b>Research Participant Group</b>	<b>Definition of the Group</b>	<b>Phishing Responsibility</b>
Technology and Security Executives	Executives of U.S. Banks that direct security and technology functions	Responsible for creating strategies and resourcing the security and technology functions
Cybersecurity Professionals	Security and technology professionals employed at U.S. banks	Responsible for managing and executing the cybersecurity program to protect the business
Non-technical Employees	Non-technical employees in the U.S. banks	Responsible for executing non-technical functions of the business while maintaining a high level of phishing awareness

### Sampling

Researchers emphasized that sampling is a critical element of qualitative studies because it pertains to clarifying the groups’ or communities’ characteristics that will participate in the interviews (Naderifar, Goli, & Ghaljaie, 2017). The significance of sampling is selecting a small population to represent the group (Naderifar et al., 2017). The most common sampling form includes probability and non-probability sampling (Etikan, Musa, & Alkassim, 2016). Probability sampling refers to having the distinctive attributes that each component in the populace has a chance of being included in the sample population (Etikan et al., 2016). The non-probability sampling technique indicates that all group participants do not have an equal opportunity to be selected (Etikan et al., 2016). For this study, I used non-probability sampling to target security and technology executives, cybersecurity professionals, and non-technical employees in the U.S. banking sector as study participants.

Naderifar et al. (2017) noted that non-probability sampling includes various methods, such as (a) convenience, (b) purposeful, and (c) quota sampling. The researchers also indicated that probability sampling is standard in quantitative studies, whereas, in qualitative inquiries, non-probability sampling is typical (Naderifar et al., 2017). Table 6 lists probability and non-probability sampling techniques. I selected to pursue non-probability sampling to capitalize on the latitude and take a proactive role in selecting the participants.

Table 6. *A Listing of Probability and Non-probability Sampling (Sharma, 2017)*

<b>Probability Sampling</b>	<b>Non-probability Sampling</b>
Simple Random Sampling	Quota Sampling
Systematic Sampling	Purposive Sampling
Stratified Sampling	Self-selection Sampling
Cluster Sampling	Snowball Sampling

Purposive, snowballing, and self-selection sampling techniques were used to select study participants based on the researcher’s judgment and expertise (Sharma, 2017) to explore the phenomenon. One negative aspect of purposive sampling was researcher bias (Sharma, 2017), in which I practiced bracketing personal biases from affecting the study. Another negative consequence was convincing the audience that subjectivity and the study participants’ selection were generalizable, meaning selecting different participants from the population produced the same results (Sharma, 2017).

I mitigated subjectivity and generalizability concerns by bracketing personal biases and selecting study participants through a fair and open process. Snowball sampling’s negative effect is the study’s lack of inclusivity by identifying potential study participants with similar affiliations with previous participants (Sharma, 2017). An issue with self-selection is that the volunteering study participant could have biases or ulterior motives for participating in the study (Sharma, 2017). I countered the negative aspects of non-probability sampling by bracketing, suppressing personal biases, thoroughly pre-interviewing the potential study participants, and examining the collected data with exhaustive data analysis.

Purposive, snowballing, and self-selection sampling techniques ensure I garnered enough study participants to reach data saturation. These techniques of targeting potential study participants were necessary to gain contact with challenging to reach individuals through self-

selection or acquaintances of individuals with similar experiences (Naderifar, Goli, & Ghaljaie, 2017). Cybersecurity could be regarded as a sensitive subject, resulting in potential research potentials to abstain from participating in the study. An expert sampling was essential due to the complexity of phishing susceptibility in the banking industry (Apostolopoulos & Liargovas, 2016).

Qualitative researcher experts indicated that the number of study participants required for a qualitative inquiry varies (Vasileiou, Barnett, Thorpe, & Young, 2018). Research emphasizes that qualitative inquiry sample sizes are small to support exploring the cases in-depth to gain textual rich data (Vasileiou et al., 2018). I interviewed 34 research participants for this qualitative inquiry; however, the number of research participants depended on reaching data saturation. Data saturation occurred when the research participants no longer introduced new discoveries, data, or themes on the phenomenon (Bungay, Oliffe, & Atchison, 2016; Guetterman, 2015); at this point, I concluded the interviewing.

#### Researcher Procedures

Charmaz (2004) noted that the practices of constructivist grounded theory consisted of (a) theoretical sampling, (b) data collection, (c) data coding and analysis, and (d) theory emergence. Figure 3 listed the methods and procedures to execute the constructivist grounded theory for this study. The GTM is not a linear process, as illustrated in Figure 3, meaning preceding activities were not entirely completed before ensuing processes started. In the GTM, data collection and coding processes were simultaneously performed, which enabled theoretical sampling and data collection to pursue while earlier collected data was compared, analyzed, and coded.

Nassiff (2012) completed an investigation of 25 grounded theory scholarly articles published between 1993 and 2011 and noticed that 52 of the studies contained between 2 and

159 participants. Grounded theory studies typically achieved theoretical saturation between 20 and 30 samples (Creswell, 2014). I did not use a predetermined number of study participants, which was deemed impractical for this study and could have adversely impacted theoretical saturation. Due to the time constraints limitations, I implemented two conditions to ensure the process could produce a result and not continue indefinitely. If theoretical saturation was reached or the time allotted for study participant interviews was depleted, theoretical sampling and ensuing data collection would cease.

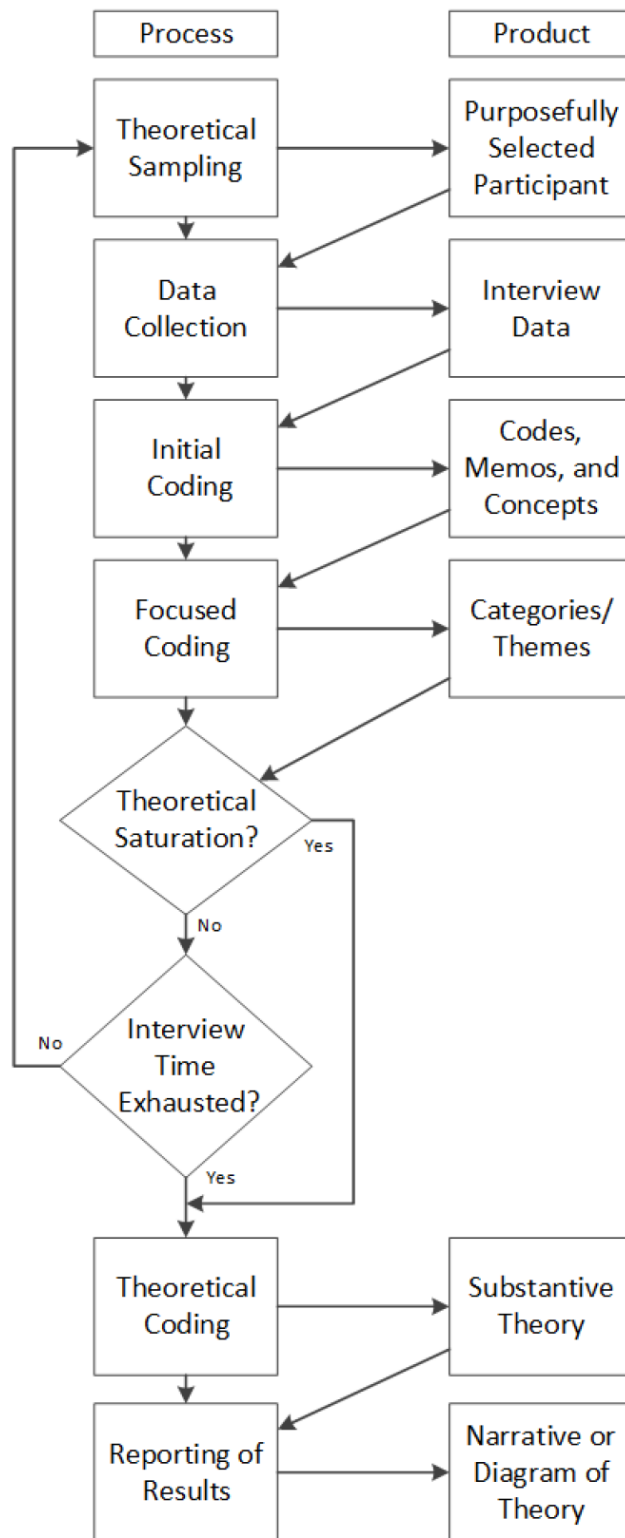


Figure 3. Process for Constructivist Grounded Theory. (Charmaz, 2014 and Nassiff, 2012)

Data collection. Data for studies can derive from many sources such as (a) interviews, (b) surveys, (c) journals, (d) autobiographies, or (e) formerly analyzed data (Corbin & Strauss, 2015; Jansen, 2010). I used semi-structured interviews to purposely secure the information reflecting the study participants' lived experiences of the phenomenon. As Corbin and Strauss (2015), indicated data collection was inspired by comparative analysis in a paralleling process. I used comparative analysis information to enrich the questions asked in subsequent interviews to capture new and different information.

The data collection process consisted of interviewing a total of 34 study participants (11 security and technology executives, 9 cybersecurity professionals, and 14 non-technical employees) that were actively employed in the U.S. banking sector. I identified a total of 43 individuals as potential research participants. The study participants were asked to partake in the research, in which 38 study participants agreed to participate in the research inquiry. I explained the purpose of the inquiry and the study participants' rights (Appendix B) while participating in the study; upon receiving written consent, the interview was conducted. After obtaining informed consent from the study participants, I attained permission to record the Zoom sessions. The interviews lasted between 28-62 minutes and were conducted between September 2020 and February 2021. Due to the pandemic and health and safety reasons, the interviews were conducted and recorded via Zoom, an online collaboration platform.

After each interview, I uploaded the Zoom video into Trint, an advanced automated transcription service, to produce the interview transcript. Each study participant and I reviewed his or her transcript for accuracy. I checked the transcripts for accuracy and allowed the respondent to do the same. After confirmation, I loaded the transcript into ATLAS.ti, a qualitative data analysis software application. The benefit of using ATLAS.ti was because it

enabled the coding, sorting, and exploring of the data to identify the themes, categories, and relationships.

I interviewed a total of 34 respondents to include 3 study participants (included in actual studies). The first three interviews were part of the pilot study to ensure the study data collection and data analysis were accomplishable and met the study objectives. I forwarded the pilot study transcripts to a seasoned academic researcher for validation that the research questions were addressed.

The demographics information collected during the interview was used to enable purposeful sampling. Due to the pandemic, study participants were interviewed electronically in which each interview was recorded for playback. Initially, I had planned to record the interviews face-to-face; however, many cities had instituted a no-movement policy, which prevented face-to-face interviews. The interviews were digitally recorded and transcribed automatically using an advanced transcription capability before conducting data analysis.

The data collection period covered six months with study participants from every primary geographical area in the U.S.

**Initial coding.** In the GTM process, coding occurred between data collection and the advent of practical theory. Throughout the coding process, a bottom-up approach ensued, analytical acumen and data interpretation led to the development of codes, memos, concepts, categories, and substantive theory (Charmaz, 2014). Saldana (2016) referred to the initial coding process as separating the collected data into independently coded portions. Initial coding involved examining each sentence (line) for data or events that emerged in the data (Charmaz, 2014). Initial coding creates additional questions and concepts that generate more in-depth data collection (Charmaz, 2014). Codes identify the importance of the concepts that emerge and recognize the meaning within blocks of data (Corbin & Strauss, 2015).

In this inquiry, initial coding was used to extrapolate meaning from each sentence and label the data to preserve its significance. I capitalized on using in vivo and process coding during initial coding. During the first repetition, I went sentence-by-sentence using in vivo codes to obtain the real meaning of a sentence using the study participant's own words (Saldana, 2016). During the second repetition, I employed process coding, which used deponent phrases to capture each sentence's action (Saldana, 2016). I then compared the in vivo codes and the process codes to the original line of data using comparative analysis to ensure an exact interpretation of the extrapolated data. Initial coding persisted until each data section was coded, and memos were used to explain the (a) data context, (b) emerging concepts, and (c) discovered questions (Charmaz, 2014).

Focused coding. Focused coding encompasses identifying the more prevalent codes to produce salient categories (Saldana, 2016). The purpose of focused coding helped identify initial codes that have importance and created categories to incorporate numerous initial codes and concepts (Charmaz, 2014). Subsequently, focused coding processes larger portions of data are analyzed and abstracted. Saldana (2016) emphasized that identifying and using overarching categories to organize data from the initial coding process can facilitate the structure of meaning.

I used focused coding to uncover categories that were incorporated for multiple process codes and concepts and created abstract connotations representative of the original data. Some categories were revealed through continuous analyzing and comparing process codes and concepts against each other (Saldana, 2016). The revelation of new categories representing higher levels of concepts allowed many codes and suggestions to be incorporated under a single label. The in vivo codes were used to make certain categories accurately subsumed process codes

and concepts. Focused coding was used continuously until all initial codes and concepts categorized in an analogous group.

Theoretical coding. According to Saldana (2016), the theoretical coding process combines the groupings created within the focused coding process, which the theoretical coding will result in an overarching code that can incorporate all codes and categories formulated during the inquiry (Saldana, 2013). An adequately comprehensive and conceptual main or fundamental category will appear through the means of theoretical coding and encapsulate the primary theme of the study (Corbin & Strauss, 2015).

This study's salient theoretical coding objective was to uncover the central theme intertwined through the categories, concepts, codes, and data. Comparative analysis was identifiable, which led to a single umbrella code. All previously generated categories, concepts, and codes led to the dominant theme through umbrella code categorizing.

Reporting results. A critical facet of conducting an inquiry is reporting the results to enable others to benefit from the study's knowledge and findings (Corbin & Strauss, 2015). GTM scholars recommended a comprehensive outline to document the study's results (Corbin & Strauss, 2015). Reporting commenced upon the completion of theoretical coding. Applicable memos, coding frameworks, and theoretical structures created throughout the coding processes were used to produce the findings.

### Reliability and Validity

Leveraging a recognizable approach that is duplicable and repeatable within multiple research projects can help achieve qualitative reliability (Creswell, 2014). I used the constructivist grounded theory, a proven methodology, and regularly used to build theory to pursue this qualitative inquiry (Charmaz, 2014; Glaser & Strauss, 1999). A requirement for qualitative reliability is to provide adequate details throughout the study that demonstrates the results are reliable (Merriam &

Tisdell, 2016). I made widespread use of the study participants' responses to derive rich and thick descriptions and analyses for enhancing the reliability and the methods used.

The purpose of this qualitative study was not to reject personal biases but more accurately acknowledge the existence of individual predispositions and lessen its influences on the inquiry (Maxwell, 2013). Entirely eradicating researcher prejudice while ensuing a qualitative investigation is challenging. The constructivist grounded theory acknowledges the subjective aspect of coding and promotes researchers to codify situations and bases for specified actions in the memos (Charmaz, 2014). Throughout the study, I minimized personal biases through bracketing predispositions, which were identified and minimized (Creswell, 2014).

A generally recognized method for attaining qualitative validity and lessening researcher bias is triangulation (Cho & Lee, 2014; Creswell, 2014). Triangulation is attainable by assembling data from various sources or choosing study participants with different experience levels or distinct environments (Creswell, 2014). This study used triangulation of sources to gather data through face-to-face interviews conducted on security and technology executives, cybersecurity professionals, and non-technical employees who possessed diverging perspectives.

### Data Analysis

Data analysis should adhere to acceptable principles (Pratt, 2009; Romano, Donovan, Chen, & Nunamaker Jr., 2003; Venkatesh et al., 2013). Creswell and Creswell (2018) postulated that qualitative data's richness should yield five to seven distinct themes. Given the complexity of working with qualitative data, researchers recommended using qualitative software to ease the burden of managing contextual information (Bringer, Johnston, & Brackenridge, 2006; Creswell & Creswell, 2018; Peters & Wester, 2007; Romano et al., 2003). Bringer et al. (2006) noted that qualitative software applications are essential in managing and manipulating data for the GTM. Researchers summarized a five-step procedure for analyzing qualitative data that includes the

subsequent steps: (a) organizing and preparing information for data analysis, (b) evaluating the data, (c) coding the data, (d) creating a description of themes, (e) characterizing the description and themes (Creswell & Creswell, 2018).

I electronically recorded the interviews via Zoom and uploaded the recorded session in Trint to produce transcripts as a measure to increase validity. I addressed trustworthiness and authenticity by having the research participants review the transcripts for accuracy. After the transcripts were examined for accuracy, I imported the transcripts into ATLAS.ti, a qualitative data software tool.

Charmaz (2006) indicated that coding occurs in the following three phases: (a) initial coding, (b) focused coding, and (c) theoretical coding. Charmaz (2006) conceded that axial coding is a part of the Strauss and Corbin model of GTM is optional. Coding is an indiscriminate process in GTM in which researchers have the flexibility to leverage different coding methods are necessary (Thornberg & Charmaz, 2012). Coding was a significant step of the data analysis, which enabled the researchers to comprehend what the data was reflecting (Charmaz, 2006).

During the initial coding process, I began to use labels to classify the data. Researchers use initial coding to progressively evaluate and decipher the study participants' thick descriptions relating to the problem being explored (Thornberg & Charmaz, 2012). Charmaz (1995) acclaimed that focused coding is the method of capturing codes generated in the initial coding process to filter through large amounts of data. Theoretical coding enabled researchers to underline potential connections between codes established during the focused coding phase to reveal the theoretical narrative (Charmaz, 2006).

Initially, I coded all the transcripts. The initial codes divulged fundamental concepts that I collected and evaluated to address the repetitive and similar concepts. To address validity and

reliability concerns, I reviewed each transcript three times, documented the fundamental concepts, and then narrowed the list of concepts.

After the initial coding of the interviews was completed, I transitioned to focused coding to create themes that symbolized a common thread or idea. Next, I employed theoretical coding to create the primary dimensions to develop the theoretical model.

### Analysis and Results

This section discusses the results of data analysis and findings for this inquiry. This section illustrates the analysis method followed. Subsequently, this section deliberates the demographic analysis that was conducted. A discussion of the detailed results of the findings follows next. Finally, this segment closes with a summary of the results.

### Data Analysis

I performed data analysis on the study participants' interview data and interview data coding. I leveraged the GTM to derive concepts and themes that emerged from the data, which enabled the discovery of overarching dimensions. The finding of the overarching dimensions resulted in a theoretical model to articulate the results.

Data analysis began upon starting with the initial coding process, as expounded by Charmaz (2006). I performed initial data coding of each interview immediately after creating the transcripts using an online transcript service (Trint). The study participants reviewed the transcripts for accuracy and addressed any concerns that pertained to validity and reliability. Undertaking this method permitted me to explore the data using GTM and code the transcripts to discover germane concepts, themes, and overarching dimensions. Throughout the GTM process, interviews and initial coding coincided as I continually engaged the collected data while also performing initial data analysis. This interconnection was vital, as it enabled me to identify

significant concepts more swiftly and determine when data saturation materialized. Coding occurred in three stages, as explained by Charmaz (2006): (a) initial coding, (b) focused coding, and (c) theoretical coding.

The breakthrough of the overarching dimensions presented in the data led to the development of the Dynamic Phishing Susceptibility Reduction Theory that researchers and practitioners can use to leverage banking cybersecurity culture to reduce phishing susceptibility in the banking sector.

### Demographic Analysis

During the interview process, demographic information was collected as the Interview Question Guide (Appendix B) as demographic-based during the initial portion of the interviews. The research participants for three groups are listed below in Tables 7, 8, and 9. The study participants included three banking employees as detailed in Figure 1: (a) security and technology executives, (b) cybersecurity professionals, and (c) non-technical employees.

Table 7. *Senior Security and Technology Executives Participants Study Data*

Participant ID	Title	Interview Length	Sex	Banking Experience (Years)
STE-1	Chief Info Security Officer	57:41	M	8
STE-2	Managing Dir, CISO	52:58	M	3
STE-3	Senior Vice President, Cybersecurity	47:23	M	16
STE-4	Executive Vice President, CIO	31:29	F	17
STE-5	Senior Vice President, Enterprise Sec	38:27	F	11
STE-6	Vice President, CISO	44:53	M	2
STE-7	Senior Director, Enterprise Cloud	36:37	M	20
STE-8	Exec Vice President, Chief Data Off	33:09	F	6
STE-9	Group CIO	41:34	M	10
STE-10	Chief Info Security Officer	46:19	M	14
STE-11	Divisional CTO	54:48	F	15

N=11

Table 8. *Cybersecurity Professionals Participants Study Data*

Participant ID	Title	Interview Length	Sex	Experience in Years
CYP-1	Information Security Eng	45:18	F	7
CYP-2	Cloud Security Architecture	37:43	M	4
CYP-3	Cybersecurity Manager	51:22	F	11
CYP-4	Technology Risk Consultant	32:49	F	9
CYP-5	Network Engineer	31:36	M	14
CYP-6	Penetration Tester	47:11	M	10
CYP-7	Senior Risk Analyst	39:48	F	12
CYP-8	Compliance Tech Business Analyst	52:39	M	8
CYP-9	Operations Risk Manager	63:54	M	5

N=9

Table 9. *Non-technical Employees Participants Study Data*

Participant ID	Title	Interview Length	Sex	Experience in Years
NTE-1	Human Resources Manager	53:11	M	12
NTE-2	Digital Consultant	50:49	F	8
NTE-3	Leadership and Development Analyst	37:55	M	5
NTE-4	Program Manager	31:27	M	9
NTE-5	Account Executive	45:42	M	6
NTE-6	Crisis Management Manager	33:21	F	8
NTE-7	Product Manager	47:38	M	13
NTE-8	Customer Solution Analyst	42:24	F	2
NTE-9	Credit Risk Analyst	54:44	M	10
NTE-10	Project Manager	56:36	M	9
NTE-11	Human Resources Consultant	30:59	F	8
NTE-12	User Experience Designer	39:18	F	6
NTE-13	Financial Analysis	34:29	M	3
NTE-14	Administrative Assistant	42:47	F	7

N=14

For the security and technology executive group, 37% of the study participants were females; the banking sector’s average experience for this group was 11 years, which the respondents ranged in various security and technology executive positions in the banking industry. In the cybersecurity professional group, females accounted for 44% of the respondents interviewed, and the study participants in this group averaged 8.8 years in the banking sector. In the non-technical group, 43% of the participants were females, and the average experience in the group’s banking sector was 7.6 years. Given the complexity and difficulty in gaining access to banking employees regarding phishing susceptibility, I focused extensively on reaching data saturation more than attaining race, educational levels, or demographic representation information based on industry specifics.

#### Study Participant Interview Data Analysis

I used ATLAS.ti for data analysis and conducted initial coding on interviews directly after transcribing the interview. As Charmaz (2006) stated, initial coding permitted me to gather

data into categories and identify any processes that surfaced in the data. While executing the initial coding process, the researcher used the constant comparative methods, as defined by Charmaz (2006). By employing the constant comparative process, I started to notify dissimilarities in the data, which enabled the at each coding level (Charmaz, 2006).

I recruited and used a subject matter expert to review and analyze each interview transcript during the initial coding phase to enhance the coding results' validity and reliability. The subject matter expert analyzed four transcripts while I conducted interviews and passed off the transcripts for initial coding. I shared the results of the initial coding with the subject matter expert. A significant requirement for qualitative research is to attain agreement amongst the coders (McDonald et al., 2019; Wiesche et al., 2017). According to MacPhail (2015), the researcher and subject matter expert collaboration provided a repetitious process for resolving the coding differences to increase reliability.

The subject matter expert and I often collaborated via Zoom or telephone to discuss the disparity and reach an agreement. During the three rounds of interview coding, coding conflicts ensued, resulting in 207 minutes of collaborative discussions in multiple meetings. This inquiry consisted of three distinct research groups, which resulted in over 350 initial codes discovered during the initial coding phase, as depicted in Appendix E.

Creswell and Creswell (2018) noted that researchers could quantify intercoder agreement by employing reliability process checking tools in qualitative data analysis applications. By using ATLAS.ti, I was able to conduct the reliability process checking, specifically Krippendorff's alpha. The Krippendorff alpha coefficient represents a statistical value indicating agreement in repetitions of qualitative and visual data (Krippendorff, 2017). Krippendorff (2004) stated that an alpha coefficient of .800 or greater is sufficient to emphasize minimal agreement

amongst coders. The subject matter expert and I calculated the Krippendorff alpha score of .837 after the initial coding and disagreement resolution process to ensure the intercoder agreement during the initial coding process.

Next, I transitioned to focused coding of the data. Focused coding enabled me to initiate data synthesis and comprehending larger portions of the data (Charmaz, 2006). The collating of data to data enabled the formation of focused codes (Charmaz, 2006). The ensuing output of focused codes enabled me to distinguish themes that embodied the initial coding process's concepts.

I transitioned to theoretical coding analysis upon completing the focused coding. Theoretical codes illustrate the potential connections between the themes identified during the focused coding process (Charmaz, 2006). The subsequent theoretical code analysis enabled discovering the overarching dimensions in the data, which developed into the Dynamic Phishing Susceptibility Reduction Theory. Using GTM, I derived the concepts, themes, and overarching dimensions from the data collection and analysis process, as depicted in Figure 4.

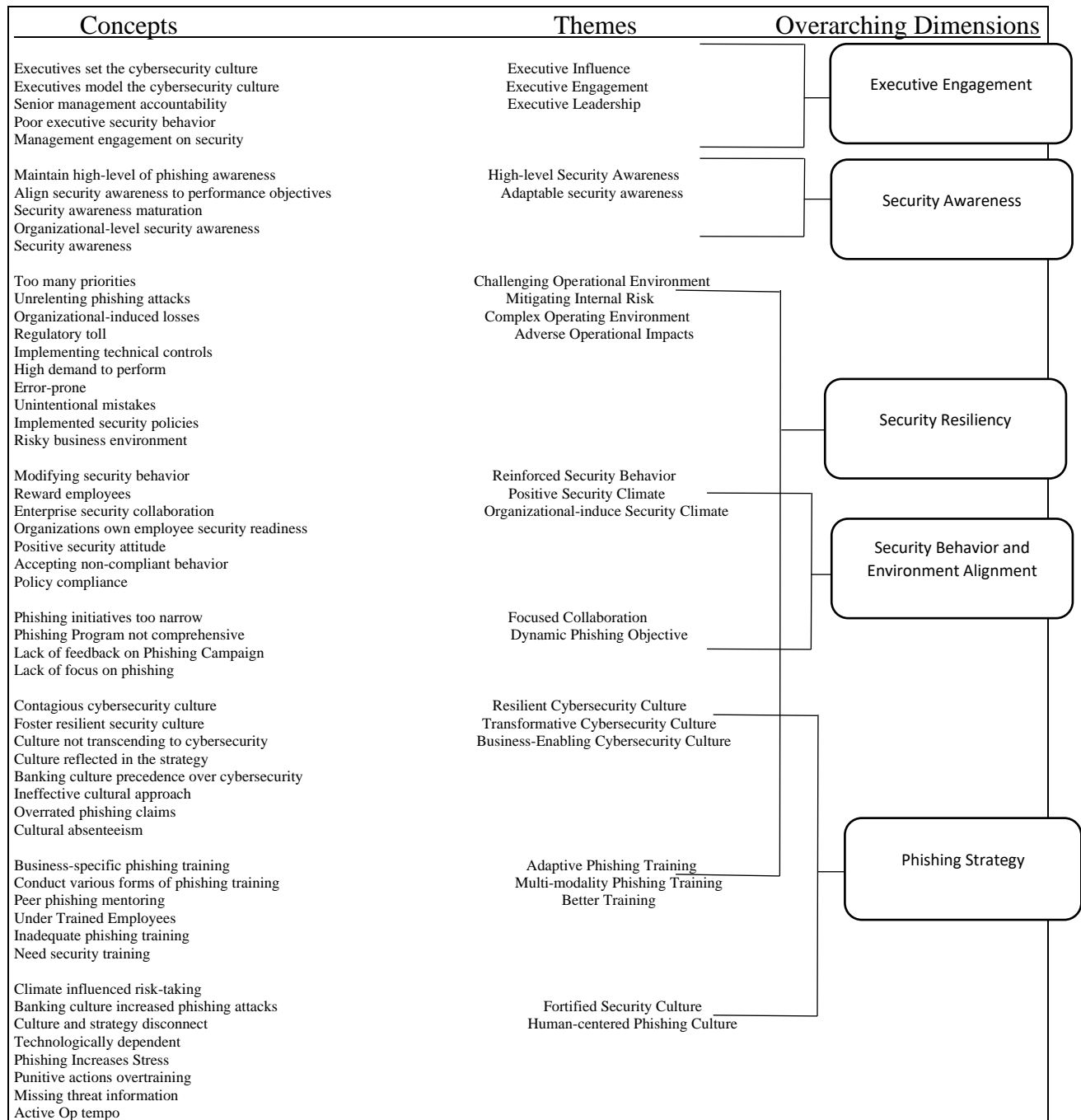


Figure 4. Emergent concepts, themes, and overarching dimensions

### Findings

Five significant findings directly supported the theory development that emerged from the inquiry.

These findings are:

1. Lack of executive coordination and support – An overwhelmingly major of the study participants (24/34 or 71%) indicated having issues with executive leaders supporting anti-phishing efforts.
2. Reinforced security awareness – An overwhelmingly major of the study participants (27/34 or 79%) reported that security awareness is essential for preventing phishing attacks. Interesting is that 21% of the bank employees did not list security awareness as critical resources for averting phishing.
3. Stronger security resiliency – The majority of the study participants (18/34 or 53%) responded to needing better security resiliency to prevent phishing attacks from affecting banking operations.
4. Positive security behavior and environment alignment – Some study participants (16/34 or 47%) postulated that banking employees lacked the training and awareness to recognize various phishing attacks in different environments (SMS, email, telephony, physical, or whaling).
5. Phishing strategy confusion – A majority of the study participants (22/34 or 65%) alluded to not having or understanding the phishing strategic initiatives, which increased phishing susceptibility.

The following consists of data supporting the findings. The research methodology employed intensive interviews from the study participants' lived experiences with the phenomenon. Quotations from the study participants are used to illustrate the findings. I used quotes from the study participants to highlight and support the findings.

Finding 1: Lack of executive coordination and support

I discovered that the lack of executive coordination and support included executive influence, executive engagement, and executive leadership. These themes and representative data are illustrated in Appendix F.

#### Executive Influence

Extant literature indicated that the top management team's executive influence specifically on the company's performance and strategy given that senior executives are responsible for organizational decisions, operations, and risk factors that impact the business (Elenkov, Judge, & Wright, 2005; Helfat, Harris & Wolfson, 2006; Yukl, 2008). Top executive management involvement is an essential factor for strongly influencing the organizational culture and the employees' attitudes concerning compliance towards the information security program (Hu et al., 2012). A study by Hu et al. (2012) indicated that top management influences in creating phishing awareness only improved to a certain degree, which is why phishing remains a top security risk for organizations. As participant STE-3 noted, "an important element of the cybersecurity program is executive influence.....governance....and the ability to make vital culture and strategy changes as directed by the volatile cyber threat environment". CYP-4 noted, "it is difficult to praise the executive leadership when the quality of the training and other security resources are never provided".

#### Executive Engagement

According to Verizon, phishing is a primary vector for data breaches, as evident by 22% of breaches due to phishing (DBIR, 2020). Reports by the APWG highlighted similar phishing results (APWG, 2020a). CYP-9 stated, "our bank is too slow to make changes to mitigate different phishing techniques.....while we implement the latest technology.....our training and practices are too archaic". Executive engagement is essential for posturing banks to combat

phishing attacks, especially as cybercriminals routinely change their tactics and techniques to deceive banking employees for sensitive and private information.

#### Executive Leadership

Yukl (2008) declared that organizations need executive leaders that are adaptive and flexible in today's tumultuous and ambiguous environments. Top executives should be amenable to changing formal programs and structures to meet organizational objectives (Yukl, 2008).

Participant STE-10 declared that "executives are responsible for positioning the banks for success to include phishing.....any other form of adverse risk that affronts the bank". Banking executives need to implement new measures and adaptively increase training standards to enable employees to outwit phishing attacks.

#### Finding 2: Security Awareness

I discovered that security awareness includes high-level security awareness and adaptable security awareness, as depicted in Appendix F.

#### High-level Security Awareness

A renowned leader in security awareness articulated the following points regarding security awareness (Carpenter, 2019): (a) because someone is aware it does not mean he or she cares, (b) working against human nature will result in failure, (c) the behavior of people is more important than what they say. Researchers acknowledged that technical solutions to mitigate against phishing attacks are not enough to safeguard employees and their company's (Al-Daeef et al., 2017). Non-technical solutions, used predominantly for human vulnerabilities, should increase employees' security awareness of phishing attacks; consequently, resulting in better utilization of technical solutions against phishing attempts (Al-Daeef et al., 2017; Kirlappos & Sasse, 2011; Wilson & Argles, 2011). Researchers emphasized the importance of the embedded training concept to increase employees' security awareness by incorporating real-world training

activities into the workers' environment rather than a traditional classroom or computer-based training (Al-Daeef et al., 2017). For example, phishing simulation that provided in-depth training scenarios to the worker is a proven way to increase security awareness (Al-Daeef et al., 2017). Study participant NTE-2 stated, "worrying about phishing attacks is stressful; we need training that increases our security awareness, so we are not taken advantage of....my security awareness is low because I am not properly trained....I need a higher level of security awareness to be safe". STE-7 stated, "the level of security awareness is a reflection of the organizational culture and executive guidance in building a banking team that protects our assets.....we need to place more emphasis on security awareness". Banks can capitalize on employees with a high level of security awareness to protect against phishing attacks and reduce risk to banking operations.

#### Adaptable Security Awareness

A critical element of software security systems is the engineering aspects of matching protection levels against risks, threats, and vulnerabilities to ensure adequate protection is sustained (Salehie, Pasquale, Omoronyia, Ali, & Nuseibeh, 2012). In cybersecurity, employees need to adapt to the security situation to prevent phishing via emails, attachments, text messages, or telephonically. NTE-13 noted, "my knowledge on the direct types of phishing and all the different technical need improvements.....I am a risk to the bank". STE-1 said, "banking employees deserve the training and awareness to recognize phishing attacks through and the many avenues and tactics that cybercriminals employ". Phishing techniques that banking employees face are evolving; therefore, training is necessary so workers can adapt and adequately defend against phishing attacks.

#### Finding 3: Stronger Security Resiliency

I discovered that stronger security resiliency consists of challenging operating environments, mitigating controls, adaptive phishing training, multi-modality training, high-level security awareness, and continuous training, as depicted in Appendix F.

#### Challenging Operating Environment

Phishing is a persistent and sustained issue in the business world, as indicated by 80% of organizations experiencing a phishing attack, resulting in significant financial losses (Derouet, 2016) as phishing attacks continue to increase annually (Greenwald, 2016). According to Soceanu, Vasylenko, and Gradinaru (2017), the increasing number of cyber-attacks are due to the complexity of information technology and organizational vulnerabilities executed by cybercriminals with expert-level skills. STE-3 stated that “the cybersecurity threats are complex and challenge the existing cultural approaches to phishing and other cybersecurity threats”. CYP-1 indicated that “Senior managers focus primarily on production and not information security because the bank is about making money at the risk of phishing attacks”. Banks need to focus on security resiliency to counter the increasing complexity of security and banking operations because the ultimate goal is to safeguard the firm’s assets.

#### Mitigating Internal Controls

For organizations to effectively combat phishing attacks, a combination of technical controls and humans as the first and last line of defense are necessary (Frauenstein, 2013). Mitigating controls are used to prevent human error or human-initiated losses (Frauenstein, 2013); the objective is to avert cybersecurity incidents such as phishing attacks from materializing to less damaging events in banks. STE-7 noted that “one way of reducing risk in the organization is to implement security controls and restrict employees access to the network”. CYP-9 remarked that “most organizations have implemented two-factor authentication as a

technical control to restrict access and prevent unauthorized users from getting on our network”. Banks leverage internal controls as measures for risk management to prevent phishing attacks from degrading banking operations.

#### Adaptive Phishing Training

A meticulous and comprehensive phishing training program can decrease information security compromise resulting from malicious emails and enhance the overall cybersecurity posture (Miranda, 2018). The National Institute of Standards and Technology stressed that organizations fail to maximize cybersecurity awareness because employees are not thoroughly trained using phishing training exercises due to the lack of a comprehensive approach that captures the phishing awareness training lifecycle completely (Miranda, 2018). NTE-11 stated, “banking employees are poorly trained....we receive training once a year .....banking will continue to face phishing attacks until better training goes into effect”. For banks to maximize phishing training opportunities, more adaptive and comprehensive methods should be implemented to reduce the static nature of existing phishing training modules.

#### Multi-modality Phishing Training

Wash and Cooper (2018) indicated that phishing is a primary vector for exploiting human weaknesses; therefore, training end-users to recognize cybercriminals’ deployed traps is essential. Using various methods to train end-users on phishing provides a multi-modality approach to expanding the trainees’ security awareness (Wash & Cooper, 2018). NTE-8 noted that “we always have training on the computer or phishing simulation emails....I do not learn that way”. CYP-7 stated, “I prefer face-to-face training so I can ask questions, but I only take computer-based training because that is what is offered”. Given the versatility and sophistication

of phishing schemes used today, banking employees require exposure to many phishing tactics to advance their security awareness.

### Continuous Training

Extant literature emphasized that security training remains ineffective and results in employees being vulnerable to a multitude of cybersecurity threats (Wash & Cooper, 2018). Researchers highlighted that embedded training, especially the instant remediation training once clicking on a simulated link, is one of the most effective training modalities by using comic rather than conventional formats (Kumaraguru et al., 2010). NTE-13 stated, “we do not stand a chance against phishing attacks because the training is a waste of time”. NTE-4 acclaimed, “I can only fight against phishing based on the training I receive....the banks owe me better and more time to train consistently”. Implementing continuous phishing training using different teaching modalities can enhance banking employees’ phishing security awareness.

### Finding 4: Positive Security Behavior and Environment Alignment

I discovered that positive security behavior and environment alignment include reinforced security behavior, positive security climate, and focused collaboration, as depicted in Appendix F.

### Reinforced Security Behavior

Researchers highlighted that self-efficacy is an essential trait for security behavior because it enables one to cope with required tasks and conquer the things that impact one’s life (Blythe, Coventry, & Little, 2015). Blythe, Coventry, and Little (2015) contended that having self-efficacy provides employees with the security acumen and determination to comply with the directed security behavior. Companies can reinforce security behavior through transparency on what is expected for security behavior (Blythe, Coventry, & Little, 2015). STE-1 stated,

“demanding positive security behavior is imperative for countering phishing attacks.....this behavior is set from the top”. NTE-8 noted that “training and security awareness is not enough.....banks need to design ways to build stronger security behaviors creatively”. Banks can reinforce security behavior by improving employees’ self-efficacy through security awareness and fortifying the proper security behavior through its culture and executives modeling the culture.

### Positive Security Climate

The organization’s senior managers are critical in establishing a positive security climate because the firm’s environment directly influences the employee’s motivation toward policy compliance (Dong, Ali, Dominic, & Ali, 2021). STE-5 proclaimed that “setting the organization’s climate is an executive function, and we continue to struggle with cybersecurity culture because most view security as a business impediment.....especially other executives who are concerned with profits and losses....security climate often clashes with the banking culture”. STE-9 emphasized, “until we accept phishing as an equivalent risk to poor liquidity practices.....most banking employees will remain oblivious to phishing attacks.....our climate is skewed to fail”. Banking executives are responsible for establishing a positive security climate to enable employees to excel and demonstrate the security behavior required.

### Focused Collaboration

An associated issue of relegating information security as a technical concern is the lack of communications experts involved in the information security process (Hallas, 2018). Employees are overwhelmed with large volumes of information security content with information that the workforce deems useless (Hallas, 2018). NTE-9 noted, “our phishing initiatives lack feedback and follow-up.....we do not see the data on any simulated phishing attacks”. CYP-6 stated, “most

phishing programs are one way....they are not open to partnering with security teams”. Hallas (2018) emphasized that information content should be designed purposely for specified audiences for information security to attain a maximum impact because employees have different learning styles.

#### Finding 5: Phishing Strategy Confusion

I discovered that phishing strategy confusion includes transformational culture, business-enabling cybersecurity culture, fortified security culture, and human-centered phishing culture, as depicted in Appendix F.

#### Transformational Culture

Carpenter (2019) recommended the five following factors to transform an enterprise’s culture: (a) develop an unobstructed view of what good looks like for your organization, (b) examine awareness through the security culture lens, (c) use behavior management practices to cultivate good security hygiene, (d) identify the different personalities, learning styles, and enablers in the organization, and (e) develop realistic short-term objectives and remain optimistic on long-term goals. STE-5 stated, “we need a transformative cybersecurity culture that provides extensive training on anti-phishing methods....as leaders, the onus is on us to change the culture to be more effective in the cybersecurity realm”. STE-8 stated, “our actions and behavior should be reflected in the culture and set the example for banking employees to follow....the culture and strategy can not contradict or be misaligned”. Banks can achieve a transformational cybersecurity culture by leveraging Carpenter’s recommendations, which will enhance the banking anti-phishing efforts.

#### Business-enabling Cybersecurity Culture

Extant research indicated that information security programs lack a cultural foundation, which is counterproductive to the organizational culture efforts of driving business performance to include safeguarding information assets (McKeown, 2019). According to Blum (2020), the security culture is a part of the business culture. McKeown (2019) emphasized that information security culture is neglected because security is evolving and tends to be based on beliefs and values rather than standards and data. NTE-14 declared, “my manager encourages our team to leave the cybersecurity business to the IT folks....My manager does not discuss cybersecurity at all; he focuses only on our direct business”. STE-2 noted, “a growing practice in most banks is to embed information security experts with the different businesses across the bank....this ensures the businesses are integrating information security practices in the day-to-day business efforts”.

#### Fortified Security Culture

Security leaders can fortify security culture by leveraging various methods to advance secure behavior, including policy integration, awareness initiatives, and other resources to avert insecure behavior (Blum, 2020). STE-4 noted, “it is time for executives to get off our asses and out in the spaces to talk cybersecurity and build partnerships with the CFOs, CMOs, and the COOs.....we have been fighting this battle too long by ourselves....a culture change is long overdue”. STE-3 noted, “I believe a strong culture is based on executives setting the pace.....getting feedback from our direct reports....implementing changes to make the bank stronger in every aspect”. Through security culture fortification, banks can reduce employees’ phishing susceptibility and increase their overall security awareness.

#### Human-centered Phishing Culture

Blum (2020) stressed that human error and poor security behavior contribute to most data breaches or outages; the primary vector that causes the security incident is a phishing attack. CYP-9 noted that “people are the weakest link because....leadership do not invest in its people”. STE-5 noted, “employees make mistakes at work because there are too many things on their plates....this is a normal practice in a bank.....it does not mean it is right”. Leveraging human-centered practices such as role-based awareness and training can reduce human vulnerabilities through phishing attack attempts.

### Theory

Study 2 generated the Dynamic Phishing Susceptibility Reduction Theory (model) grounded in evidence from the data analysis results. The Dynamic Phishing Susceptibility Reduction Theory (Figure 5) aligns to and reveals the overarching dimensions that present a framework for reducing phishing susceptibility in the banking sector. The study participants indicated that phishing efforts lacked robustness and responsiveness, hence the theory’s naming nomenclature.

The naming nomenclature for the theory (model) requires further explanation. I decided that phishing attacks in the banking sector are sustained and disruptive to banking operations, as indicated by the APWG’s (2020; 2020a) two most recent reports. During the COVID-19 pandemic, phishing attacks have increased by over 700%, while organizations struggle to protect remote workers (Shi, 2020). Existing literature highlighted that workers are overconfident in their abilities to identify phishing attacks (Shi, 2020). As noted by the APWG, banks remain a target of choice by cybercriminals. Banks need a dynamic and reinforced approach to reduced phishing susceptibility; hence, the theoretical model’s name is derived from this inquiry, which is grounded in the study’s findings.

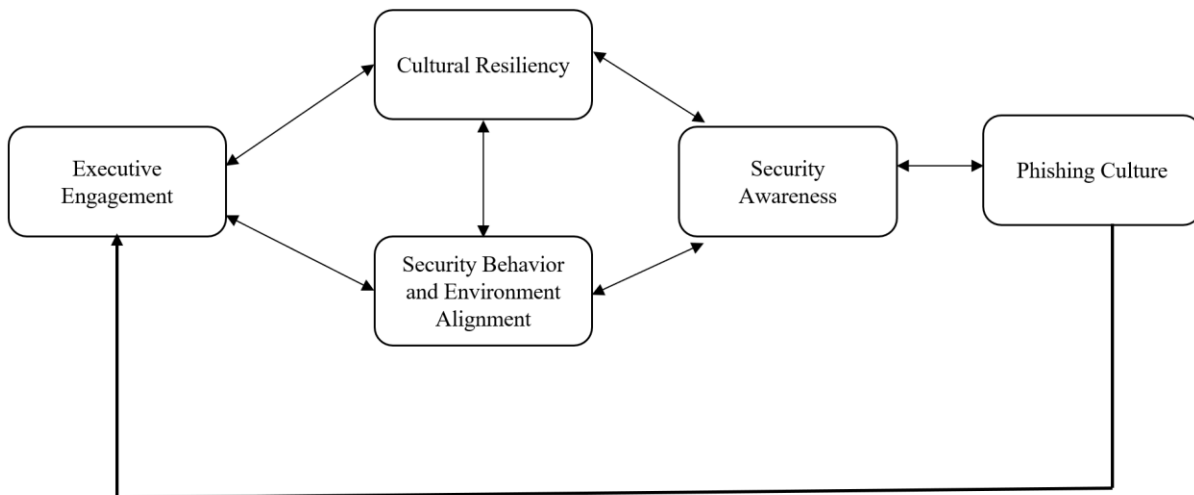


Figure 5. The Dynamic Phishing Susceptibility Reduction Theory (DPSRT)

Next, it is essential to explain the constructions and order relationships in the DPSRT model. The order of the model is derived from the study’s data analysis. Based on data analysis, most study participants indicated that executive involvement and direction were vital for the cybersecurity culture and combatting phishing attacks in the banking sector. I constructed the model to reflect that senior executives (top management) are ultimately responsible for cybersecurity to include phishing. It is essential to start with executive engagement since senior executives are responsible for the organizational culture and the cybersecurity culture, and the bank’s security behavior based on the current cybersecurity threat landscape. Given the multitude of cybersecurity threats, banks have to adjust and remain resilient to defend against phishing attacks and other malicious security incidents.

The model reflects that executive engagement, cultural resiliency, and security behavior and environment alignment are directly influenced and managed by the senior executives. The arrows connecting executive engagement, cultural resiliency, and security behavior and environment alignment indicate the constant interplay based on the threat environment, resource

allocation to prevent phishing, and feedback from the phishing strategy. Strong cultural resiliency and security behavior and environment alignment should increase the workforce's security awareness. Based on evaluating the organization's security awareness, the arrows between cultural resiliency, security behavior and environmental alignment, and security awareness illustrate the constant interplay and adjustments made by the senior executives to solidify the bank employees' security awareness. The connection of security awareness to the phishing culture derived from the study participants indicating a lack of understanding and confusion regarding the phishing culture. Senior executives must establish a phishing culture within the cybersecurity culture, given that phishing is a primary attack vector used by cybercriminals. The model illustrates that security awareness enables bank employees to impact the phishing culture directly, and the phishing culture enhances the workforce security awareness. The line linking the phishing culture to executive engagement indicates a feedback loop, enabling senior executives to make adjustments based on the current threat and risk condition and employee preparation.

According to Zahra, Sapienza, and Davidsson (2006), when the environment is volatile and unpredicted, firms have to transform their operational routines and practices. Specifically, the extant literature highlighted the following three criteria for extensive evolving areas: (a) the capacity to resolve a problem (substantive ability), (b) the existence of quickly changing issues (an environmental characteristic), and (c) the capacity to change the way firms solve problems (a higher-order dynamic capability to amend capabilities) (Zahra et al., 2006). Given the continuous deceitful phishing practices and the cost associated with phishing attacks, accompanied by the lack of phishing susceptibility theory in banking, a dynamic-based theory is appropriate based on data analysis and urgent demand to reduce phishing in the banking sector.

## Executive Engagement

The study participants' data analysis of information led to discovering this overarching dimension and finding the three following themes: executive influence, executive engagement, and executive leadership. The finding of these themes is substantiated in data provided by study participants during their interviews. The study participants provided experiences of situations that highlighted the need for executive engagement in directing cybersecurity functions and countermeasures to mitigate phishing attacks in the banking sector. Study participants emphasized the importance of robust executive engagement to expedite and sustain the bank's preparedness in combatting phishing attacks because phishing is a significant disruptor to the cybersecurity culture.

## Security Awareness

The study participants' data analysis of information led to discovering this overarching dimension and finding the three following themes: high-level security awareness and adaptable security awareness. The finding of these themes is substantiated in data provided by study participants during their interviews. The study participants' comments indicated that some banking employees are unprepared to thwart phishing attacks due to substandard security awareness and security training. Study participants repeatedly suggested and requested improved security awareness to prevent from becoming a phishing attack victim.

## Security Resiliency

The data analysis led to discovering this overarching dimension and finding the six following themes: challenging operating environment, mitigating controls, adaptive phishing training, multi-modality training, high-level security awareness, and continuous training. The finding of these themes is substantiated in data derived from the interviews. A common

implication was senior managers' focusing more on the business while disregarding the importance of information security. The study participants raised several points to increase security resiliency, such as leveraging technical countermeasures and implementing internal controls to restrict access. The study participants consistently asked for better training and security awareness to improve security resiliency, indicating a widespread issue that impacts phishing preparedness.

#### Security Behavior and Environment Alignment

The data analysis led to discovering this overarching dimension and finding the three following themes: reinforced security behavior, positive security climate, and focused collaboration. The finding of these themes is substantiated in data derived from the interviews. The study participants' comments highlighted that security awareness and security training are not enough; consequently, indicating that banks need to focus on behavior and strengthening the security climate. The remarks noted that banks' phishing initiatives lack focused collaboration in a hyperactive cybersecurity threat environment accompanied by a need to reinforce the cybersecurity climate.

#### Phishing Culture

The data analysis led to discovering this overarching dimension and finding the five following themes: transformational culture, business-enabling cybersecurity culture, fortified security culture, and human-centered phishing culture. The finding of these themes is substantiated in data derived from the interviews. The remarks indicated that senior executives held themselves accountable for the culture by exhibiting and modeling the proper security behavior. Integrating senior information security professionals with the different directorates in

the bank is a practice to reduce phishing attacks, increase security awareness, and address human-centered problems that increase the probability of being phished.

## Summary

This chapter provided a thorough synopsis of the methodological framework, data coding, analysis, and interpretation employed in this study. Five overarching dimensions were identified through data analysis: *Dynamic Executive Engagement*, *Dynamic Security Awareness*, *Dynamic Security Resiliency*, *Dynamic Security Behavior and Environment Alignment*, and *Dynamic Phishing Strategy*. The study participants' excerpts were related to their assertions in each of the five overarching dimensions. This chapter discussed the study's findings and illustrated how the study participants' data were grouped into themes, eventually leading to the overarching dimensions. Lastly, this chapter produced the five overarching dimensions of the dynamic phishing susceptibility reduction theoretical model that answered the research question for this study.

## Discussion

This grounded theory inquiry aimed to explore banking cybersecurity culture influences on phishing susceptibility. There is a lack of empirical research on banking cybersecurity culture influences on phishing susceptibility; therefore, my intent for this study was to produce theory, increase discourse around this important topic, and produce scholarly work towards reducing the research gap.

I leveraged information from other critical sources to strengthen my data analysis and collected data from three different groups for triangulation. Guion, Diehl, and McDonald (2011) suggested that one can attain a diverse perspective on the phenomenon by interviewing different stakeholder groups. By interviewing security and technology executives, cybersecurity

professionals, and non-technical employees, I gained a deeper understanding of how banking cybersecurity culture influences phishing susceptibility. Another form of triangulation used was investigator triangulation, which was achieved through intercoder agreement by having another subject matter expert conduct data analysis and demonstrate similar results (Guion, Diehl, & McDonald, 2011). Data triangulation was achieved by using different data sources and information to inform the data analysis. Using the grounded theory approach, I was able to modify interview questions based on document analysis to gain in-depth perspectives on the phenomenon.

Given that I could not observe the study participants in the field, I paid close attention to their body language during the interviews and when reviewing the recorded sessions. On several instances, the study participants' body language provided clues on more profound personal convictions with a particular question, which I explored with follow-up questions. Following up on the body language gestures enabled me to take notes on which questions presented discomfort or struck a sensitive or troubled area and resulted in additional exploration.

This study revealed some practical findings related to banking cybersecurity culture and its influences on reducing phishing susceptibility. The study findings indicated that (a) lack of executive coordination and support, (b) security awareness, (c) stronger security resiliency, (d) positive security behavior and environment alignment, and (e) phishing strategy confusion are direct implications of banking cybersecurity culture influences on phishing susceptibility.

#### Lack of Executive Coordination and Support

The first finding of the study is the lack of executive coordination and support. Banking security and technology executives need better engagement and coordination with the employees to reduce phishing susceptibility. Cybercriminals are modifying their phishing tactics, and

banking employees lack the security awareness and the wherewithal to identify phishing scams due to a lack of adequate security training, awareness, and resources. Dynamic executive engagement is necessary to provide a foundation and resources to reduce employee phishing susceptibility.

### Security Awareness

The second finding of the study is that security awareness is a bedrock for reducing phishing susceptibility in the banking sector. Security awareness is vital that banking employees must exercise consistently in hyperactive cybersecurity threat environments to reduce phishing susceptibility. Many factors influence a bank employee's security awareness, such as substandard training, the lack of different training modalities, workload, fatigue, and the cybersecurity culture. Banking executives must cultivate a security climate with effective security awareness and training to keep employees and the banks safe from phishing.

### Stronger Security Resiliency

The third finding of the study is the need for stronger security resiliency, which is challenging with the uptick of phishing attacks directed at the banking sector. Phishing is a top attack vector used by cybercriminals; therefore, banks have to increase security resiliency by better preparing and equipping employees with awareness and proficiency to thwart phishing attacks. Failure to strengthen bank employee's security awareness and phishing proficiency increases phishing susceptibility.

### Positive Security Behavior and Environment Alignment

The fourth finding of the study is positive security behavior and environment alignment; banking employees are required to maintain positive security behavior in all environments because of the different variants of phishing. Banks remain an attractive target for

cybercriminals, consequently implementing new tactics and strategies to deceive employees in non-banking environments. By maintaining and practicing a positive security behavior, bank employees can prevent phishing attacks in non-banking environments through security training and awareness on new tactics, techniques, and procedures employed by cybercriminals.

### Phishing Strategy Confusion

The fifth finding of the study is phishing strategy confusion, whereas employees struggle to identify phishing strategies, resulting in increased phishing susceptibility. Many factors such as human error, workload, bad decision-making, and organizational culture can complicate initiatives to reduce phishing susceptibility. Unclear phishing strategies reflect the lack of alignment between executive engagement, the cybersecurity culture, and positive security behavior. The phishing strategy should align with the cybersecurity strategy with clear objectives for preventing phishing attacks on banking employees.

### Conclusion

This study illustrates that the existing practices to prevent phishing attacks require drastic and dynamic changes to reduce banking employees' phishing susceptibility. Executive engagement, security awareness, positive security behavior, security resiliency, and a decisive and communicated phishing strategy are measures to advance banking security postures for combatting phishing attacks. Phishing is a significant threat to banks; consequently, challenging employees' security awareness and phishing attentiveness through a continuous barrage of new phishing tactics and technique. Reducing phishing susceptibility in the banking sector is imperative due to the 700% increase in phishing attacks, which cybercriminals capitalize on remote workers (Shi, 2020). The Dynamic Phishing Susceptibility Reduction Theory, based on

data analysis findings, provides banks with a holistic model to strengthen and advance their phishing mitigation measures.

## CHAPTER 5

### CONCLUSION, LIMITATIONS, AND CONTRIBUTIONS

#### General Discussion

This section aims to compare the findings between Study 1 and Study 2 because each study had a different qualitative research design, and Study 2 included three groups of study participants. Both studies set out to explore banking cybersecurity culture's influence on phishing susceptibility. Study 1 informed Study 2 based on the lack of theory on phishing susceptibility and scholarly works on banking cybersecurity culture in the U.S.

#### Similar Findings

Both studies indicated that executive leadership and engagement are necessary to reduce phishing susceptibility in the banking sector. Study participants in both inquiries stressed the importance of executive leadership, such as developing policies to drive behavior modification (EXC-4), the governance of cybersecurity programs (STE-3), and positioning the banks for success (STE-10). Hu et al. (2012) emphasized the significance of senior executives in establishing a culture to address phishing awareness; today, such efforts yielded limited progress towards mitigating phishing attempts. Expanding the research participant groups to cybersecurity professionals and non-technical employees in Study 2 resulted in the capturing of ineffective executive leadership, which failed to reduce phishing susceptibility. The initial study did not yield similar results because the study participants only included security and technology executives.

Both inquiries listed security awareness as a vital element for reducing phishing susceptibility. Research participants stressed the need for increased security awareness (NTE-2) because properly trained banking employees with high-security awareness levels can reduce phishing susceptibility (EXC-1). A high degree of security awareness is attainable through a

continuous awareness program by ensuring security knowledge and education exceed the annual awareness requirement (Scholl, Leiner, & Fuhrmann, 2017). Effective security awareness results in employees practicing positive security behavior due to reinforced training that enables workers to exhibit the targeted behavior (Scholl, Leiner, & Fuhrmann, 2017). Both studies corroborated existing literature that security awareness is an essential factor for establishing positive security behavior.

The operational security environment was a significant concern in both inquiries. The research participants indicated that human errors played a critical factor in successful phishing attacks. Study 2 revealed that the security environment is complicated and compounded by organizational factors and human errors. Snyder (2016) emphasized Kurt Lewin's formula, which indicates behavior is a function of both the individual and the environment. To influence change, modifying one's behavior or changing the environment is necessary for materializing the transformation (Shoda, 2004). Cybercriminals are active agents in shaping the cybersecurity threat landscape. Banks are forced to implement information security defenses according to the threats; consequently, based on Shoda's (2004) point, the only variable to change is banking employees' behavior. The human element in cybersecurity remains an underexplored topic; therefore, preventing organizations from holistically understanding human behavior in information security. Banks struggle with lessening the operational security environment impacts on employees, so both studies addressed the conceptual framework and the theory development.

A correlated finding revealed in both studies is the human factor element associated with phishing. Both inquiries determined that human-based risk factors such as human errors, mistakes, inaction, bad decision-making, and being undertrained aided malicious actors in successful phishing attacks. Existing literature indicates silos within cybersecurity operations

(Wynn, 2021) and increasing work demands on employees, which result in distractions and the overextension of human performance abilities (Axelrod, 2021). The perpetuation of human-based risk factors is due to tactical approaches rather than leveraging comprehensive practices such as human system engineering (Winkler, 2021). The human system engineering process manifests on a layered methodology with countermeasures to prevent cybersecurity incidents such as phishing attacks (Winkler, 2021). Current security practices are layered; however, most do not account for the human element; hence, there is a need for a dynamic approach to prevent phishing attacks and reduce phishing susceptibility.

In both studies, security training was considered a significant factor for reducing phishing susceptibility; however, the study participants' lived experiences revealed that security training did not adequately prepare employees to prevent phishing attacks. Bank employees are poorly trained, in most cases, receiving security training annually (NTE-11). Our training consists of computer-based training or simulated phishing attacks; this is not enough to make use proficient (NTE-8). The ineffectiveness of security training was raised in both studies due to the limited nature of the training modalities and the training scenarios not based on real-world scenarios or failed to include the latest tactics and procedures used by malicious agents to deceive banking employees through phishing. According to the NIST, there is a difference between security awareness and security training (Hash & Wilson, 2012). Security awareness aims to modify security behavior and emphasize positive security practices while security training targets building skills and competencies through teaching (Hash & Wilson, 2012). In Study 1, the conceptual framework depicts the need for continuous security awareness and training, while in Study 2, the Dynamic Phishing Susceptibility Reduction Theory indicates the need for robust

security awareness. Based on the above suppositions, security training was deemed a vital element of reducing phishing susceptibility.

#### Other Findings

The limitations of Study 1 were due to only interviewing security and technology executives. In contrast, Study 2 included an expanded research participant group comprised of security and technology executives, cybersecurity professionals, and non-technical employees. Study 1 provided an executive-level perspective that lacked the urgency of preventing phishing attacks. Hence, the conceptual frame derived from Study 1 is based on reducing phishing susceptibility through executive influence and culture, whereas Study 2 resulted in a theory to address the dynamic necessity of reducing phishing attacks in the banking sector.

The second inquiry provides a more in-depth picture of phishing susceptibility based on the study participants' lived experiences, which resulted in the creation of the dynamic phishing susceptibility reduction theory. The data analysis reflects a lack of a dynamic approach from executives regarding phishing susceptibility. The Dynamic Phishing Susceptibility Reduction Theory is based on data analysis to increase attention and drive security posturing resiliency to prevent phishing attacks. The APWG (2020a) denotes that the banking sector remains a top targeted domain for phishing. Study 2 data analysis produced a theoretical model for creating a robust approach to safeguarding banks from phishing attacks. Phishing attacks in the banking sector are sustained threats. According to the study participants, banks fail to take aggressive actions to thwart phishing attacks; hence, creating the Dynamic Phishing Susceptibility Reduction Theory.

## Significance of the Model

The APWG (2020, 2020a) third and fourth quarter reports indicated that phishing attacks in the banking sector are sustained, as evident by banking representing close to 20% of phishing attacks. The Dynamic Phishing Susceptibility Reduction Theory (model) is indicative of a robust and assertive framework for countering phishing in the banking sector. The current approaches to phishing are not practical and require banking executives to rethink how to avert phishing attacks effectively. The study participants provided details of disconnects that made banks more vulnerable to phishing attacks, such as inadequate security awareness, substandard executive engagement, and the lack of cultural robustness. The significance of the model is to provide a framework for increasing executive engagement to drive a holistic phishing culture that aligns with the regulated nature of the banking sector.

Other fields struggling with phishing can leverage this framework to improve their phishing culture through executive engagement. The increasing number of phishing attacks (Shi, 2020) is indicative of unprepared organizations. Through executive engagement, organizations can capitalize on raising phishing issues to top management's attention to leverage an enterprise approach that is dynamic enough to counter phishing attacks.

## Limitations

A limitation of both studies was that I conducted all the interviews via Zoom, an online video platform. Typically, when conducting qualitative studies, the interviews are conducted face-to-face, when logistically feasible. Due to COVID-19, I conducted the interviews via Zoom and recorded each interview.

Another limitation was that I restricted the study to security and technology executives. In the banking sector, there are many types of executives working in various areas across the

bank. The research purposely targeted security and technology executives because this group of senior managers is typically the executive cadre's subject matter experts with an in-depth understanding of phishing and the accompanying oversight responsibility. I interviewed security and executives in small, medium, and large banks throughout the U.S. to gain a deeper understanding of the phenomenon based on the senior managers' lived experiences.

Researchers emphasized three areas that need validating for qualitative inquires. Sikolia, Biros, Mason, and Weiser (2013) acknowledged that (a) having the study participants review the transcripts for accuracy, (b) allowing the study participants to lead the direction of the interview, and (c) including study participants' responses in the emerging theory. I trusted that the research participants provided factual information, which I challenged the responses and used follow-up questions to validate the responses.

#### Limitations of Industry

One bounding of the study's findings is refuting the findings by indicating that cybersecurity in the banking sector is a risk area that is still maturing. Given that cybersecurity is a cost center rather than a profit and loss line of business, the return on investment remains a challenging outcome based on traditional business estimates. Taking a traditional business approach, some senior executives might view phishing as a risk factor rather than a pervasive malicious cyber practice used to gain access to sensitive information, credential, and financial assets. The banking culture is known for taking excessive risks, so the findings of this study might be perceived as impeding banks from capitalizing on financial gains by overinvesting in phishing. Organizations need to adapt and embrace the practice that cybersecurity is an enterprise-level initiative, and information security threats can be crippling without proper executive engagement.

## Contributions to the Literature

Currently, there is a shortage of scholarly research on banking cybersecurity culture influences the reduction of phishing susceptibility. The studies offer insight into banking cybersecurity culture and its impact on phishing susceptibility. One finding from this study is that executive influence is a critical factor for developing influential cybersecurity culture by ensuring the security program is adequately resourced to reduced phishing susceptibility. Executives' influence is a constant element for cultivating a banking security culture that leverages training and heightened awareness throughout the bank to reduce phishing susceptibility. The research indicated that banks could sustain enhanced awareness to reduce phishing susceptibility through continuous phishing training that is relatable to real-world problems. The security operations pace, unprioritized efforts, and constant changes within the banking ecosystem adversely impact cognitive awareness and make employees prone to phishing susceptibility. Banks need to increase their focus on the human element of phishing awareness by removing operational stressors that make employees prone to phishing susceptibility. Phishing susceptibility in the banking industry will remain a persistent challenge until addressing continuous phishing awareness and training, eliminating operational stressors, and the scare tactic.

The banking industry benefits from these studies by developing a holistic understanding of phishing susceptibility through a strong banking cybersecurity culture, continuous phishing awareness training, and a dynamic phishing approach. Academia and the banking sector can benefit from this study by forming partnerships and conducting mixed-method studies to investigate phishing susceptibility comprehensively. The psychology and human factor communities can benefit from this study by exploring and examining banking cybersecurity

culture influences on phishing susceptibility. Corporate executives can use this study to evaluate executive engagement's significance for reducing phishing susceptibility through strong cybersecurity culture and training.

Both studies contribute to the existing body of literature by capturing the viewpoints and experiences of banking employees on phishing susceptibility. This research provides scholarly work on phishing susceptibility in the banking sector, an area that suffers from the lack of research. The dynamic phishing susceptibility reduction theory (Study 2) and the conceptual framework developed (Study 1) assist in advancing phishing susceptibility theory. The academic community can leverage these inquiries to highlight the value of scholarly works to solve business problems and potentially form partnerships with banks similar to the relationships they have with consulting firms. The studies contribute to the human factors community by providing insight into the proper behavior necessary to counter phishing attacks. Given that cybersecurity is a multidisciplinary domain that banks are struggling to safeguard, this study contributes to various stakeholders.

Both studies contribute to the existing body of literature by capturing the viewpoints and experiences of banking employees on how culture influences phishing susceptibility. The five findings and the Dynamic Phishing Susceptibility Reduction Theory adds to the existing body of knowledge. The Dynamic Phishing Susceptibility Reduction Theory offers banks a model to advance their phishing initiatives and security protection. At issue is the lack of scholarly research on phishing susceptibility in the banking sector. This study provides finding and a theoretical model for reducing phishing susceptibility in the banking sector. The research adds to organizational culture and cybersecurity culture theories, specifically how banks can leverage culture to reduce phishing susceptibility. More importantly, the findings help lessen the theory-

to-practice gap regarding phishing susceptibility and culture in the banking industry. Both inquiries' findings are essential to contributing to foundational scholarly works and bank employees' susceptibility to phishing attacks, leading to actionable practices to reduce phishing attacks in the banking sector.

### Contributions to Practice

The banking sector can benefit from these studies, offering a deeper understanding of phishing susceptibility related to security and technology executives, cybersecurity professionals, and non-technical employees. Academia and the banking sector benefit from these studies by forming partnerships and conducting mixed-method studies to investigate phishing susceptibility comprehensively. The psychology and human factor communities can benefit from this study by exploring and examining banking cybersecurity culture influences on phishing susceptibility. Corporate executives can use this study to evaluate executive engagement's significance for reducing phishing susceptibility through strong cybersecurity culture and training.

### Application for Practice

The Dynamic Phishing Susceptibility Reduction Theory offers a theoretical-supported and practical approach to reduce phishing susceptibility in the banking sector. Given that there is a shortage of practical applications on phishing susceptibility, the banking sector needs models and methods that are actionable and can increase its cybersecurity posture. The Dynamic Phishing Susceptibility Reduction Theory applies to other industries that are challenged with reducing phishing attacks. This study provides insight into banking cybersecurity culture and its impact on phishing susceptibility. Corporate executives can use this study to evaluate executive engagement's significance for reducing phishing susceptibility through strong cybersecurity culture and training.

## Conclusions

These studies illustrate that cybersecurity culture is vital for countering phishing susceptibility by banks placing continuous security awareness training, executive-drive security climate, human-centered security operations, dynamic approach for countering phishing attacks. Banks face increasing threats and challenges every day, and by leveraging a continuous security awareness training campaign, employees can counter phishing attempts with greater certainty and preparation. The unrelenting banking climate can be unforgiving on employees, so executive engagement is paramount to drive an adequately resourced organization, awareness, and sufficiently trained employees. Cybersecurity is about people, and employees should be at the forefront of developing dynamic anti-phishing capabilities.

## REFERENCES

- (2016). Cybersecurity: Enhancing coordination to protect the financial sector: Hearing before the Committee on Banking, Housing, and Urban Affairs, United States Senate, One Hundred Thirteenth Congress, Second Session.
- Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, 33(3), 237-248.
- Abdelhamid, M. (2018). Greater patient health information control to improve the sustainability of health information exchanges. *J Biomed Inform*, 83,150-158.  
doi: 10.1016/j.jbi.2018.06.002
- Abdelhamid, M. (2020). The role of health concerns in phishing susceptibility: Survey design study. *Journal of Medical Internet Research*, 22(5), e18394.
- Aguayo, F. Z., & Ślusarczyk, B. (2020). Risks of banking services' digitalization: The practice of diversification and sustainable development goals. *Sustainability*, 12(10), 4040.
- Al-Daeef, M. M., Basir, N., & Saudi, M. M. (2017, July). Security awareness training: A review. In *Proceedings of the World Congress on Engineering* (Vol. 1, pp. 5-7).
- AlHogail, A., & Mirza, A. (2014, January). Information security culture: a definition and a literature review. In *2014 World Congress on Computer Applications and Information Systems (WCCAIS)* (pp. 1-7). IEEE.
- AlHogail, A., & Mirza, A. (2015). Organizational information security culture assessment. In *Proceedings of the International Conference on Security and Management (SAM)* (p. 286). The Steering Committee of The World Congress in Computer Science, Computer Engineering, and Applied Computing (WorldComp).
- Ali, M., & Brooks, L. (2008). Culture and I.S.: National cultural dimensions within I.S. discipline. In: *Proceedings of the 13th Annual Conference of the U.K. Academy for Systems*, pp. 1–14 (2009)
- Alsayed, A., & Bilgrami, A. (2017). E-banking security: internet hacking, phishing attacks, analysis, and prevention of fraudulent activities. *Int. J. Emerg. Technol. Adv. Eng*, 7(1), 110.
- Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies*, 82, 69-82.
- Anawar, S., Kunasegaran, D. L., Mas'ud, M. & Zakaria, N. A. (2019). Analysis of phishing susceptibility in a workplace: A big five personality perspectives. *Journal of Engineering Science and Technology*, 14(5), 2865-2882.

- Anti-Phishing Working Group [APWG]. (2016). Anti-phishing Activity Trends Report, 2nd Quarter, 2016. Retrieved from <http://www.antiphishing.org>
- Anti-Phishing Working Group [APWG]. (2020). Anti-phishing Activity Trends Report, 1st Quarter 2020. Retrieved from [https://docs.apwg.org/reports/apwg\\_trends\\_report\\_q1\\_2020.pdf](https://docs.apwg.org/reports/apwg_trends_report_q1_2020.pdf)
- Anti-Phishing Working Group [APWG]. (2020a). Anti-phishing Activity Trends Report, 4th Quarter 2020. Retrieved from <https://apwg.org/trendsreports/>
- Apostolopoulos, N. & Liargovas, P. (2016). Regional parameters and solar energy enterprises. *International Journal of Energy Sector Management*, 10(1), 19–37. doi:<http://dx.doi.org/10.1108/IJESM-11-2014-0009>
- Astakhova, L. V. (2014). The concept of the information security culture. *Scientific and Technical Information Processing*, 41(1), 22-28.
- Axelrod, G. (2021). Human psychology toward cybersecurity can build value as a business enabler. *United States Cybersecurity Magazine*.
- Bacivarov, I. (2017). RAISA and IJISC–5 years in the service of cybersecurity culture dissemination. *International Journal of Information Security and Cybercrime (IJISC)*, 6(1), 9-12.
- Bahoo, S. (2020). Corruption in banks: A bibliometric review and agenda. *Finance Research Letters*, 101499.
- Bandi, S. (2016). *An empirical assessment of user online security behavior: Evidence from a university*. Master Thesis. University of Maryland, College Park, United States of America.
- Banu, M. N., & Banu, S. M. (2013). A comprehensive study of phishing attacks. *International Journal of Computer Science and Information Technologies*, 4(6), 783-786.
- Bauer, S., & Bernroider, E. W. (2015, August). The effects of awareness programs on information security in banks: the roles of protection motivation and monitoring. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 154-164). Springer, Cham.
- Benardo, M. & Weatherby, K. (2015). A framework for cybersecurity. FDIC.gov. Supervisory Insights. Retrieved from [https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin15/si\\_winter2015-article01.pdf](https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin15/si_winter2015-article01.pdf)
- Benenson, Z., Gassmann, F., & Landwirth, R. (2017, April). Unpacking spear phishing

- susceptibility. In *International Conference on Financial Cryptography and Data Security* (pp. 610-627). Springer, Cham.
- Birks, M. & Mills, J. (2015). *Grounded theory: A practical guide* (2nd ed.). Thousand Oaks, CA: SAGE Publications Inc.
- Björck, J. & Jiang, K. W. B. (2006). Information security and national culture: Comparison between ERP system security implementations in Singapore and Sweden. *Master Degree Thesis Submitted at the Royal Institute of Technology, Sweden*.
- Bloomberg, L. D., & Volpe, M. (2012). *Completing your qualitative dissertation: A road map from beginning to end* (2nd ed.). Thousand Oaks, CA: SAGE Publications Inc.
- Blum, D. (2020). Strengthen security culture through communications and awareness programs. In *Rational Cybersecurity for Business* (pp. 91-122). Apress, Berkeley, CA.
- Blythe, J. M., Coventry, L., & Little, L. (2015). Unpacking security policy compliance: The motivators and barriers of employees' security behaviors. In *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)* (pp. 103-122).
- Boggs, W.B. (2004). TQM and organizational culture: A case study. *The Quality Management Journal*, Vol. 11 No. 2, pp. 42-52.
- Bringer, J. D., Johnston, L. H., & Brackenridge, C. H. (2006). Using computer-assisted qualitative data analysis software to develop a grounded theory project. *Field Methods*, 18(3), 245-266.
- Bryant, M. T. (2003). *The portable dissertation advisor*: Corwin Press.
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523-548.
- Bungay, V., Oliffe, J., & Atchison, C. (2016). Addressing underrepresentation in sex work research: Reflections on designing a purposeful sampling strategy. *Qualitative Health Research*, 26(7), 966-978.
- Camillo, M. (2017). Cybersecurity: Risks and management of risks for global banks and financial institutions. *Journal of Risk Management in Financial Institutions*, 10(2), 196-200.
- Carpenter, P. (2019). *Transformational Security Awareness: What Neuroscientists, Storytellers, and Marketers Can Teach Us About Driving Secure Behaviors*. John Wiley & Sons.
- Carter, W.A. (2017). Forces shaping the cyber threat landscape for financial institutions: SWIFT

- Institute Working Paper No. 2016-004, October 2, 2017. Retrieved from [https://csis-prod.s3.amazonaws.com/s3fs-public/171006\\_Cyber\\_Threat\\_Landscape%20\\_Carter.pdf](https://csis-prod.s3.amazonaws.com/s3fs-public/171006_Cyber_Threat_Landscape%20_Carter.pdf).
- Ceesay, E. N., Myers, K., & Watters, P. A. (2018). Human-centered strategies for cyber-physical systems security. *EAI Endorsed Transactions on Security and Safety*, 4(14).
- Chang, S. E., & Lin, C. S. (2007). Exploring organizational culture for information security management. *Industrial management & data systems*.
- Charmaz, K. (1995). Grounded theory. In J. A. Smith, R. Harre & L. Van Langenhove(Eds.), *Rethinking methods in psychology*. London, United Kingdom: Sage Publishing.
- Charmaz, K. (2006). *Constructing grounded theory: A practical guide through qualitative analysis*. Thousand Oaks, CA: Sage Publishing.
- Chen, C. C., Medlin, B. D. & Shaw, R. S. (2008). A cross-cultural investigation of situational information security awareness programs. *Information Management & Computer Security*, 16(4), 360-376.
- Chen, Y. A. N., Ramamurthy, K. R. A. M., & Wen, K. W. (2015). Impacts of comprehensive information security programs on information security culture. *Journal of Computer Information Systems*, 55(3), 11-19.
- Chen, R., Gaia, J., & Rao, H. R. (2020). An examination of the effect of recent phishing encounters on phishing susceptibility. *Decision Support Systems*, 113287. <https://doi.org/10.1016/j.dss.2020.113287>
- Cho, J. Y., & Lee, E. H. (2014). Reducing confusion about grounded theory and qualitative content analysis: Similarities and differences. *The Qualitative Report 2014*, 19(64), 1-20.
- Choo, K. K. R. (2011). Cyber threat landscape faced by financial and insurance industry. *Trends and Issues in Crime and Criminal Justice*, (408), 1.
- Cohn, A., Fehr, E., & Maréchal, M. A. (2014). Business culture and dishonesty in the banking industry. *Nature*, 516(7529), 86-89.
- Connolly, L., Lang, M., & Tygar, J. D. (2015, May). Investigation of employee security behaviour: A grounded theory approach. In *IFIP International Information Security and Privacy Conference* (pp. 283-296). Springer, Cham.
- Conway, D., Taib, R., Harris, M., Yu, K., Berkovsky, S., & Chen, F. (2017). A qualitative investigation of bank employee experiences of information security and phishing. In *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)* (pp. 115-129).
- Corbin, J. M., & Strauss, A. (1990). Grounded theory research: Procedures, canons, and evaluative criteria. *Qualitative Sociology*, 13(1), 3-21. doi:10.1007/bf00988593

- Corbin, J. M., & Strauss, A. (2015). *Basics of qualitative research: Techniques and procedures for developing grounded theory* (4th ed.). Thousand Oaks, CA: SAGE Publications Inc.
- Corradini, I. (2020). Building a cybersecurity culture in organizations. *Series: Advances in Intelligent Systems and Computing*, 1210, 102. doi: 10.1007/978-3-030-52581-1\_14
- Craigien, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, 4(10), 13-21. Retrieved from <http://libproxy.temple.edu/login?url=https://search-proquest-com.libproxy.temple.edu/docview/1638205509?accountid=14270>
- Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (4th ed.). Los Angeles, CA: SAGE Publications Inc.
- Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (Fifth ed.): SAGE Publications, Inc.
- Crosman, P. (2016, April 27). Where banks are most vulnerable to cyberattacks now. *American Banker*, 1(80).
- D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security*, 22(5), 474-489.
- Darwish, A.; El Zarka, A.; and Aloul, F. (2012). Towards understanding phishing victims' profile. *Proceedings of International Conference on Computer Systems and Industrial Informatics (ICCSII)*. Sharjah, United Arab Emirates, 1-5.
- Da Veiga, A., & Martins, N. (2015). Information security culture and information protection culture: A validated assessment instrument. *Computer Law & Security Review*, 31(2), 243-256.
- Da Veiga, A. (2016, July). A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. In the *2016 SAI Computing Conference (SAI)*, 1006-1015. IEEE.
- Denison, D.R., Haaland, S., and Goelzer, P., (2004). Corporate culture and organizational effectiveness: is Asia different from the rest of the world? *Organizational Dynamics*, Vol. 29(33)1, pp. 98-109.
- Denison, D., Nieminen, L., & Kotrba, L. (2014). Diagnosing organizational cultures: A conceptual and empirical review of culture effectiveness surveys. *European Journal of Work and Organizational Psychology*, 23(1), 145-161.
- Denzin, N. K., & Lincoln, Y. S. (1994). *Handbook of qualitative research*. Thousand Oaks: Sage Publications.

- Derouet, E. (2016). Fighting phishing and securing data with email authentication. *Computer Fraud & Security*, 2016(10), 5-8.
- Dhamija, R., Tygar, J.D., and Hearst, M.A. (2006). Why phishing works. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (Quebec, Apr. 24–27). ACM Press, New York, 2006, 581–590; <http://portal.acm.org/citation.cfm?id=1124861>
- Dinev, T., Goo, J., Hu, Q. and Nam, K. (2009). User behavior towards protective information technologies: The role of national cultural differences. *Information Systems Journal*, 19(4), 391-412.
- Dodge, R., Coronges, K., & Rovira, E. (2012, June). Empirical benefits of training to phishing susceptibility. In *IFIP International Information Security Conference* (pp. 457-464). Springer, Berlin, Heidelberg.
- Donaldson, S., Siegel, S., Williams, C. K., & Aslam, A. (2015). *Enterprise cybersecurity: how to build a successful cyber defense program against advanced threats*. Apress.
- c). The effect of organizational information security climate on information security policy compliance: The mediating effect of social bonding towards healthcare nurses. *Sustainability*, 13.
- Douglas, M. (1985). *Measuring culture: A paradigm for the analysis of social organization*. Columbia University Press, New York.
- Downs, J. S., Holbrook, M. B., and Cranor, L. F. (2006). Decision strategies and susceptibility to phishing. In *Proceedings of the SOUPS Symposium on Usable Privacy and Security* (Pittsburgh, July 12–14). ACM Press, New York, 2006.
- Elenkov, D. S., Judge, W., & Wright, P. (2005). Strategic leadership and executive innovation influence: an international multi-cluster comparative study. *Strategic Management Journal*, 26(7), 665-682.
- Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics*, 5(1), 1–4.
- Ertan, A., Crossland, G., Heath, C., Denny, D., & Jensen, R. (2020). Cyber security behaviour in organisations. *arXiv preprint arXiv:2004.11768*.
- European Union Agency for Network and Information Security (2017, November). *Cyber Security Culture in Organizations*. Retrieved from [https://www.enisa.europa.eu/publications#c5=2008&c5=2018&c5=false&c2=publicationDate&reversed=on&b\\_start=0](https://www.enisa.europa.eu/publications#c5=2008&c5=2018&c5=false&c2=publicationDate&reversed=on&b_start=0)
- Fagade, T., & Tryfonas, T. (2017). Hacking a bridge: An exploratory study of compliance-

- based information security management in banking organizations. In *Proceedings of the 21st World Multi-Conference on Systemics, Cybernetics, and Informatics (WMSCI 2017)* (Vol. 2, pp. 94-99).
- Feeney, A., & Heit, E. (2007). *Inductive reasoning: Experimental, developmental and computational approaches*. New York, NY: Cambridge University Press.
- Fiske, S. T., & Taylor, S. E. (2013). *Social cognition: From brains to culture*. Thousand Oaks, CA: Sage.
- Flores, W. R., Holm, H., Nohlberg, M., & Ekstedt, M. (2015). Investigating personal determinants of phishing and the effect of national culture. *Information & Computer Security*.
- Flores, W. R., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security*, 59, 26-44.
- Frauenstein, E. D. (2013). *A Framework to Mitigate Phishing Threats* (Doctoral dissertation, Nelson Mandela Metropolitan University).
- Fung, J. (2013). *How many cyber attacks hit the United States last year*. Retrieved from <http://www.nextgov.com/cybersecurity/2013/03/how-many-cyberattacks-hit-united-states-lastyear/61775/>
- Gaumer, Q., Mortier, S., & Moutaib, A. (2016). Financial institutions and cyber crime between vulnerability and security. *FSR Financial*, 45.
- Gcaza, N., Solms, R. Von, & Vuuren, J. Van. (2015). An ontology for a national cyber-security culture environment. In *Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015)* (1-10).
- Gcaza, N., & von Solms, R. (2017, May). Cybersecurity culture: An ill-defined problem. In *IFIP World Conference on Information Security Education* (pp. 98-109). Springer, Cham.
- Gcaza, N., & Von Solms, R. (2017). A strategy for a cybersecurity culture: A South African perspective. *The Electronic Journal of Information Systems in Developing Countries*, 80(1), 1-17.
- Gcaza, N., von Solms, R., Grobler, M. M., & van Vuuren, J. J. (2017). A general morphological analysis: delineating a cyber-security culture. *Information & Computer Security*.
- Glaser, B. G., & Strauss, A. L. (1967). *The discovery of grounded theory: Strategies for qualitative research*. New Brunswick, New Jersey: AldineTransaction.
- Glaser, B. G., & Strauss, A. L. (1999). *The discovery of grounded theory: Strategies for qualitative research*. New Brunswick, NJ: Aldine Transaction.

- Govender, S., Kritzinger, E., & Looock, M. (2016, May). The influence of national culture on information security culture. In *2016 IST-Africa Week Conference* (pp. 1-9). IEEE.
- Grant, R. L. (2017). *Exploring effects of organizational culture upon implementation of information security awareness and training programs within the defense industry located in the Tennessee Valley Region* (Doctoral dissertation).
- Grasshoff, G., Bohmayr, W., Papritz, M., Leiendecker, J., Dombard, F., Bizimis, I., & Glance, A.A. (2018). Banking's cybersecurity blind spot—and How to fix it. BCG.com. Retrieved from <https://www.semanticscholar.org/paper/Banking%E2%80%99s-Cybersecurity-Blind-Spot%E2%80%94and-How-to-Fix-Grasshoff-Bohmayr/fabecc3e3096d4569153fde7b685fd466a93fd6a>
- Greenwald, J. (2016). Employers facing growing risk in tax season: Spear phishing. Retrieved from <http://www.businessinsurance.com>
- Gregorio, D. D., Kassicieh, S. K., & Neto, R. D. G. (2005). Drivers of e-business activity in developed and emerging markets. *IEEE Transactions on Engineering Management*, 52(2), 155-166.
- Grennan, J. (2019, March 29). A corporate culture channel: How increased shareholder governance reduces firm value. Available at SSRN: <https://ssrn.com/abstract=2345384> or <http://dx.doi.org/10.2139/ssrn.2345384>
- Guetterman, T. C. (2015). Descriptions of sampling practices within five approaches to qualitative research in education and the health sciences. *Forum Qual Soc Res*, 16(2): 25.
- Guion, L. A., Diehl, D. C., & McDonald, D. (2011). Triangulation: Establishing the validity of qualitative studies. *EDIS*, 2011(8), 3-3.
- Gupta, S., Singhal, A., & Kapoor, A. (2016, April). A literature survey on social engineering attacks: Phishing attack. In *2016 international conference on computing, communication and automation (ICCCA)* (pp. 537-540). IEEE.
- Gupta, B. B., Arachchilage, N. A., & Psannis, K. E. (2018). Defending against phishing attacks: Taxonomy of methods, current issues, and future directions. *Telecommunication Systems*, 67(2), 247-267.
- Hallas, B. (2018). Rethinking the human factor: A philosophical approach to information security awareness, behavior, and culture. The Hallas Institute.
- Hansen, J. M, Saridakis, G., Benson, V. (2018). Risk, trust, and the interaction of perceived ease of use and behavioral control in predicting consumers' use of social media for transactions. *Comput Hum Behav*, 80, 197-206. doi:10.1016/j.chb.2017.11.010.
- Hartnell, C. A., Ou, A. Y., & Kinicki, A. (2011). Organizational culture and organizational

- effectiveness: A meta-analytic investigation of the competing values framework's theoretical suppositions. *Journal of Applied Psychology*, 96, 677-694.
- Helfat, C. E., Harris, D., & Wolfson, P. J. (2006). The pipeline to the top: Women and men in the top executive ranks of US corporations. *Academy of Management Perspectives*, 20(4), 42-64.
- Henshel D., Sample C., Cains M., and Hoffman B. (2016). Integrating cultural factors into human factors framework and ontology for cyber attackers. In *Proc. of Advances in Human Factors in Cybersecurity (AHFC '16)*. Springer International Publishing, 123-37.
- Hofstede, G. (1984). *Culture's consequences: International differences in work-related values* (Vol. 5). Sage.
- Hofstede, G. (2001). *Culture's consequences: Comparing values, behaviors, institutions, and organizations across nations*. Sage Publications.
- Hofstede, G. (2014). National cultural dimensions. Retrieved from <http://geert-hofstede.com/dimensions.html>.
- House, R., Hanges, P., Javidan, M., Dorfman, P. & Gupta, V. (2004). *Leadership, culture, and organizations: The GLOBE Study of 62 Societies*, Sage Publications, Beverly Hills, CA.
- Howard, L. W. (1998). Validating the competing values model as a representation of organizational cultures. *International Journal of Organizational Analysis*, 6, 231-250.
- Hsieh, H.-F., & Shannon, S.E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research*, 15(9), 1277-1288.
- Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, 43(4), 615-660.
- Huang, K., & Pearlson, K. (2019, January). For what technology can't fix: Building a model of organizational cybersecurity culture. In *Proceedings of the 52nd Hawaii International Conference on System Sciences*.
- Ifinedo, P. (2008, October). I.T. security and privacy issues in global financial services institutions: do socio-economic and cultural factors matter?. In *2008 Sixth Annual Conference on Privacy, Security, and Trust* (pp. 75-84). IEEE.
- Ifinedo, P. (2014). The effects of national culture on the assessment of information security threats and controls in financial services industry. *International Journal of Electronic Business Management*, 12(2).
- Ioannou, M., Stavrou, E., & Bada, M. (2019, June). Cybersecurity Culture in Computer Security

- Incident Response Teams: Investigating difficulties in communication and coordination. In *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)* (pp. 1-4). IEEE.
- Iuga, C., Nurse, J. R., & Erola, A. (2016). Baiting the hook: factors impacting susceptibility to phishing attacks. *Human-centric Computing and Information Sciences*, 6(1), 8.
- Ivancevich, J. M., Konopaske, R., & Matteson, M. T. (2014). *Organizational behavior & management* (10th ed.). New York, NY: McGraw-Hill.
- Ivaturi, K., & Janczewski, L. (2013). Social engineering preparedness of online banks: An Asia-Pacific perspective. *Journal of Global Information Technology Management*, 16(4), 21-46.
- Jansen, H. (2010). The logic of qualitative survey research and its position in the field of social research methods. *Forum Qualitative Social Research*, 11(2). Retrieved from <http://www.qualitative-research.net/index.php/fqs/article/view/1450/2946>
- Johnston, A. C., Warkentin, M., & Luo, X. (2009). National culture and information privacy: the influential effects of individualism and collectivism on privacy concerns and organizational commitment. In *Proceedings of the International Federation of Information Processing (IFIP), International Workshop on Information Systems Security Research* (pp. 88-104).
- Kam, H. J., Katerattanakul, P., & Gogolin, G. (2013). A cross-industry study: differences in information security policy compliance between the banking industry and higher education. The Proceedings on *Thirty Fourth International Conference on Information Systems, Milan*
- Karahanna, E., Evaristo, R., & Srite, M. (2002, January-March). Methodological issues in MIS cross-cultural research. (Research Note). *Journal of Global Information Management*, 10(1), 48+. [https://link-gale-com.libproxy.temple.edu/apps/doc/A80848529/ITOF?u=temple\\_main&sid=ITOF&xid=91e037c5](https://link-gale-com.libproxy.temple.edu/apps/doc/A80848529/ITOF?u=temple_main&sid=ITOF&xid=91e037c5)
- Karahanna, E., Evaristo, J. R., & Srite, M. (2005). Levels of culture and individual behavior: an investigative perspective. *Journal of Global Information Management (JGIM)*, 13(2), 1-20.
- Kim, S., & McLean, G. N. (2014). The impact of national culture on informal learning in the workplace. *Adult Education Quarterly*, 64(1), 39-59.
- Kirlappos, I., & Sasse, M. A. (2011). Security education against phishing: A modest proposal for a major rethink. *IEEE Security & Privacy*, 10(2), 24-32.
- Kleitman, S., Law, M. K., & Kay, J. (2018). It's the deceiver and the receiver: Individual

- differences in phishing susceptibility and false positives with item profiling. *PLOS One*, 13(10).
- Krippendorff, K. (2004). *Content analysis: An introduction to its methodology*. Thousand Oaks, California: SAGE Publications.
- Krippendorff, K., & Allen, M. (2017). Intercoder reliability techniques: Krippendorff's alpha. *The SAGE Encyclopedia of Communication Research Methods*. SAGE Publishing Inc, Thousand Oaks, 743-751.
- Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology (TOIT)*, 10(2), 1-31.
- Leka, A. & Frieza, E. (2018). Cybercrime and impact on the financial system. *Proceedings of 4th International Conference on Computer Science Networks and Information Technology*. Montreal, Canada ISBN: 9780998900063
- MacPhail, C., Khoza, N., Abler, L., & Ranganathan, M. (2015). Process guidelines for establishing intercoder reliability in qualitative studies. *Qualitative Research*, 16(2), 198-212. doi: 10.1177/1468794115577012
- Madnick, S. (2018). How companies can create a cybersafe culture at work. MIT.edu. Retrieved from <http://web.mit.edu/smadnick/www/wp/2018-05.pdf>
- Marquardt, M., Berger, N., & Loan, P. (2004). *HRD in the age of globalization: A practical guide to workplace learning in the third millennium*. Basic Books.
- Matavire, R., & Brown, I. (2017). Profiling grounded theory approaches in information systems research. *European Journal of Information Systems*, 22(1),119-129. doi:10.1057/ejis.2011.35
- McDonald, N., Schoenebeck, S., & Forte, A. (2019). Reliability and inter-rater reliability in qualitative research. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW), 1-23. doi: 10.1145/3359174
- McKeown, D. A. (2019). Building a risk-based information security culture. *ISSA Journal*, 17(4), 14-21.
- Mervelskemper, L., Möller, R., & Schumacher, S. (2018). How does corporate culture affect banks' risk-taking?. Retrieved from <https://pdfs.semanticscholar.org/5045/47c8d65464c9f43887e57d9d8ecee0784e4f.pdf>
- Milberg, S., Smith, H. J. & Burke, S. (2000). Information privacy: corporate management and national regulation, *Organization Science*, 11(1), 35-57.
- Miranda, M. J. A. (2018). Enhancing cybersecurity awareness training: A comprehensive

- phishing exercise approach. *International Management Review*, 14(2), 5-10,56. Retrieved from <http://libproxy.temple.edu/login?url=https://www-proquest-com.libproxy.temple.edu/scholarly-journals/enhancing-cybersecurity-awareness-training/docview/2127156399/se-2?accountid=14270>
- Mirchandani, B. (2018, August 28). Laughing all the way to the bank: Cybercriminals targeting U.S. financial institutions. *Forbes.com*. Retrieved from <https://www.forbes.com/sites/bhaktimirchandani/2018/08/28/laughing-all-the-way-to-the-bank-cybercriminals-targeting-us-financial-institutions/#2548fdb56e90>
- Mouton, F., Leenen, L., Malan, M. M., & Venter, H. S. (2014, July). Towards an ontological model defining the social engineering domain. In *IFIP International Conference on Human Choice and Computers* (pp. 266-279). Springer, Berlin, Heidelberg.
- Mouton, F., Malan, M. M., Kimppa, K. K., & Venter, H. S. (2015). Necessity for ethics in social engineering research. *Computers & Security*, 55, 114–127.
- Muñiz, B. F., Peón, J. M. M., & Ordás, C. J. V. (2018). Assessing and measuring banking culture. In *Contemporary Issues in Banking* (pp. 363-387). Palgrave Macmillan, Cham.
- Naderifar, M., Goli, H., & Ghaljaie, F. (2017). Snowball sampling: A purposeful method of sampling in qualitative research. *Strides in Development of Medical Education*, 14(3), 1–6.
- Nassiff, E. (2012). *Understanding the value of enterprise architecture for organizations: A grounded theory approach* (Doctoral dissertation). Retrieved from ProQuest Dissertation Database. (UMI 3523496).
- Nguyen, D.D., Hagendorff, J., & Eshraghi, A. (2017). Does a CEO's cultural heritage affect performance under competitive pressure? *Rev. Finance Stud.*, 31 (1), 97–141.
- Nguyen, D. D., Nguyen, L., & Sila, V. (2019). Does corporate culture affect bank risk-taking? Evidence from loan-level data. *British Journal of Management*, 30(1), 106-133.
- O'Reilly, K., Paper, D., & Marx, S. (2012). Demystifying grounded theory for business research. *Organizational Research Methods*, 15(2), 247-262.
- Pavlou, P.A., & Chai, L. (2002). What drives electronic commerce across cultures? A cross-cultural empirical investigation of the theory of planned behavior. *Journal of Electronic Commerce Research* 3(4), 240–253 (2002).
- Peters, V., & Wester, F. (2007). How qualitative data analysis software may support the qualitative analysis process. *Quality and Quantity*, 41(5), 635-659.
- Pratt, M. G. (2009). For the lack of a boilerplate: Tips on writing up (and reviewing) qualitative research. *Academy of Management Journal*, 52(5), 856-862.  
Doi:10.5465/AMJ.2009.44632557

- Quinn, R.E. & Spreitzer, G.M. (1991). The psychometrics of the competing values culture instrument and an analysis of the impact of organizational culture on the quality of life. *Research in Organizational Change and Development*, Vol. 5, pp. 115-142.
- Raghavan, A. R., & Parthiban, L. (2014). The effect of cybercrime on a Bank's finances. *International Journal of Current Research & Academic Review*, 2(2), 173-178.
- Rekouche, K. (2011). Early phishing. arXiv preprint arXiv:1106.4692.
- Romano Jr., N. C., Donovan, C., Chen, H., & Nunamaker Jr., J. F. (2003). A methodology for analyzing web-based qualitative data. *Journal of Management Information Systems*, 19(4), 213-246.
- Saldana, J. (2016). *The coding manual for qualitative researchers* (3rd ed.). Thousand Oaks, CA: SAGE Publications Inc.
- Salehie, M., Pasquale, L., Omoronyia, I., Ali, R., & Nuseibeh, B. (2012, September). Requirements-driven adaptive security: Protecting variable assets at runtime. In *2012 20th IEEE international requirements engineering conference (RE)* (pp. 111-120). IEEE.
- Sample, C., Cowley, J., Hutchinson, S., & Bakdash, J. (2017, July). Culture+ cyber: exploring the relationship. In *International Conference on Applied Human Factors and Ergonomics* (pp. 185-196). Springer, Cham.
- San Martino, A., & Perramon, X. (2010). Phishing secrets: History, effects, countermeasures. *IJ Network Security*, 11(3), 163-171.
- Schein, E. H. (2011). *Organizational culture and leadership*, 2<sup>nd</sup> ed. John Wiley & Sons.
- Schlienger, T., & Teufel, S. (2003). Information security culture: From analysis to change. *South African Computer Journal*, 31, 46-52.
- Schmidt, M. B., Johnston, A. C., Arnett, K. P. Chen, J. Q. & Xi'an, S. L. (2008). A cross-cultural comparison of U.S. and Chinese computer security awareness. *Journal of Global Information Management*, 16(2), 91-103.
- Schneider, B., Ehrhart, M. G., & Macey, W. H. (2013). Organizational climate and culture. *Annual Review of Psychology*, 64, 361-388.
- Schreier, M., Stamann, C., Janssen, M., Dahl, T., & Whittal, A. (2019, September). Qualitative content analysis: Conceptualizations and challenges in research practice—Introduction to the FQS Special Issue" Qualitative Content Analysis. In *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research* (Vol. 20, No. 3).
- Schwartz, S. (2006). A theory of cultural value orientations: explication and applications.

*Comparative Sociology*, 2, 137–182.

- Scott, J. (2017, March). How to crush the health sector's ransomware pandemic: The machine learning-based artificial intelligence revolution starts now! ICITech.com. Retrieved from <https://icitech.org/wp-content/uploads/2017/03/ICIT-Analysis-Artificial-Intelligence-in-the-Health-Sector.pdf>
- Sebescen, N., & Vitak, J. (2017). Securing the human: Employee security vulnerability risk in organizational settings. *Journal of the Association for Information Science and Technology*, 68(9), 2237-2247.
- Sharma, G. (2017). Pros and cons of different sampling techniques. *International Journal of Applied Research*, 3(7), 749–752
- Sheng, S., Holbrook, M.B., Kumaraguru, P., Cranor, L.F., and Downs, J.S. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (Atlanta, Apr. 10–15). ACM Press, New York, 373–382
- Shi, F. (2020). Threat spotlight: Coronavirus-related phishing. Retrieved from <https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/>
- Sikolia, D., Biro, D., Mason, M., and Weiser, M. (2013). Trustworthiness of grounded theory methodology research in information systems. *MWAIS 2013 Proceeding*, 16. Retrieved from <https://aisel.aisnet.org/mwais2013/16>
- Soceanu, A., Vasylenko, M., & Gradinaru, A. (2017, March). Improving cybersecurity skills using network security virtual labs. In *Proceedings of the International MultiConference of Engineers and Computer Scientists 2017 Vol II, IMECS*.
- Sommestad, T., & Karlzén, H. (2019). A meta-analysis of field experiments on phishing susceptibility. In *2019 APWG Symposium on Electronic Crime Research (eCrime)*, 1-14). IEEE.
- Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, 36(2), 215-225.
- Spencer, F. G. (2019). *Does Organizational Culture Serve as an Antecedent to the Dynamic Capability of an Automated Customer Relationship System as an Example of a Big Data Analytics Program in a Firm? A Case Study* (Doctoral dissertation).
- Srivastav, A., & Hagendorff, J. (2015). Corporate governance and bank risk-taking. *Corp. Govern*, 24 (3), 334–345.
- Straub, D., Loch, K., Evaristo, R., Karahanna, E., & Srite, M. (2002, January-March). Toward a

- theory-based measurement of culture. *Journal of Global Information Management*, 10(1), 13+. [https://link-gale-com.libproxy.temple.edu/apps/doc/A80848526/AONE?u=temple\\_main&sid=AONE&xid=48c13ce2](https://link-gale-com.libproxy.temple.edu/apps/doc/A80848526/AONE?u=temple_main&sid=AONE&xid=48c13ce2)
- Strauss, A., & Corbin, J. (1990). *Basics of qualitative research: Grounded theory procedures and techniques*. Thousand Oaks, CA: Sage.
- Suddaby, R. (2006). From the editors: What grounded theory is not. [Editorial]. *Academy of Management Journal*, 49, 633-642. doi: 10.5465/AMJ.2006.22083020
- Sutton, J., & Austin, Z. (2015). Qualitative research: Data collection, analysis, and management. *The Canadian Journal of Hospital Pharmacy*, 68(3), 226.
- Symonds, J. E., & Gorard, S. (2010). Death of mixed methods? Or the rebirth of research as a craft. *Evaluation & Research in Education*, 23(2), 121-136.
- Tang, M., & Zhang, T. (2016). The impacts of organizational culture on information security culture: a case study. *Information Technology and Management*, 17(2), 179-186.
- Tembe, R., Hong, K. W., Murphy-Hill, E., Mayhorn, C. B., & Kelley, C. M. (2013, June). American and Indian conceptualizations of phishing. In *2013 Third Workshop on Socio-Technical Aspects in Security and Trust* (pp. 37-45). IEEE.
- Tembe, R., Zielinska, O., Liu, Y., Hong, K. W., Murphy-Hill, E., Mayhorn, C., & Ge, X. (2014). Phishing in international waters. Proceedings of the 2014 Symposium and Bootcamp on the Science of Security. HotSoS 2014: Symposium and Bootcamp on the Science of Security Raleigh, North Carolina.
- Terlizzi, M. A., Meirelles, F. D. S., & Viegas Cortez da Cunha, M. A. (2017). Behavior of Brazilian banks employees on Facebook and the cybersecurity governance. *Journal of*
- Ula, M., Ismail, Z., & Sidek, Z. M. (2011). A Framework for the governance of information security in banking system. *Journal of Information Assurance & Cyber Security*, 2011, 1-12.
- Urquhart, C., & Fernández, W. (2013). Using grounded theory method in information systems: The researcher as blank slate and other myths. *Journal of Information Technology*, 28(3), 224-236. doi: 10.1057/jit.2012.34
- Urquhart, C., Lehmann, H., & Myers, M. D. (2009). Putting the 'theory' back into grounded theory: Guidelines for grounded theory studies in information systems. *Information Systems Journal*, 20(4), 357-381. doi: 10.1111/j.1365-2575.2009.00328.x
- Wiesche, M., Jurisch, M. C., Yetton, P. W., & Krcmar, H. (2017). Grounded theory methodology in information systems research. *MIS Quarterly*, 41(3), 685-701.

- Wilson, C., & Argles, D. (2011, June). The fight against phishing: technology, the end-user and legislation. In *International Conference on Information Society (i-Society 2011)* (pp. 501-504). IEEE.
- Van Hoorn, A. (2017). Organizational culture in the financial sector: Evidence from a cross-industry analysis of employee personal values and career success. *Journal of Business Ethics*, 146(2), 451-467.
- Van Mourik, D. J. (2017). *Targeted attacks and the human vulnerability* (Doctoral dissertation, MS thesis, Cyber Security. Academy, The Hague, The Netherlands, 2017.[Online]. Available: <https://www.csacademy.nl/images/scripts/2017/Thesis-Van-Mourik.pdf>).
- Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, 29(4), 476-486.
- Vasileiou, K., Barnett, J., Thorpe, S., & Young, T. (2018). Characterising and justifying sample size sufficiency in interview-based studies: systematic analysis of qualitative health research over a 15-year period. *BMC medical research methodology*, 18(1), 1-18.
- Vayansky, I., & Kumar, S. (2018). Phishing—challenges and solutions. *Computer Fraud & Security*, (1), 15-20.
- Venkatesh, V., Brown, S., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *Management Information Systems Quarterly*, 37(1), 21-54.
- Verizon Enterprise [DBIR]. (2017). Data breach investigations report. Verizonenterprise.com. Retrieved from [https://enterprise.verizon.com/resources/reports/dbir/?utm\\_campaign=DBIR2017&utm\\_medium=TW&utm\\_source=brand](https://enterprise.verizon.com/resources/reports/dbir/?utm_campaign=DBIR2017&utm_medium=TW&utm_source=brand)
- Verizon Enterprise [DBIR]. (2020). Data breach investigations report. Verizonenterprise.com. Retrieved from <https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf>
- Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated information processing model. *Decision Support Systems*, 51(3), 576-586.
- Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research*, 45(8), 1146-1166.
- Wall, J. D., Palvia, P., & Lowry, P. B. (2013). Control-related motivations and information security policy compliance: The role of autonomy and efficacy. *Journal of Information Privacy and Security*, 9(4), 52-79.

- Wang, S. W., Ngamsiriudom, W., & Hsieh, C. (2015). Trust disposition, trust antecedents, trust, and behavioral intention. *Serv Ind J*, 35(10), p. 555-572.  
doi: 10.1080/02642069.2015.1047827
- Wash, R., & Cooper, M. M. (2018, April). Who provides phishing training? Facts, stories, and people like me. In *Proceedings of the 2018 Chi Conference on Human Factors in Computing Systems*, 1-12.
- Welch, C., Piekari, R., Plakoyiannaki, E., & Paavilainen-Mäntymäki, E. (2011). Theorising from case studies: Towards a pluralist future for international business research. *Journal of International Business Studies*, 42(5), 740-762.
- Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior*, 72, 412-421.
- Williams, E. J., Hinds, J., & Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies*, 120, 1-13.
- Winkler, I. (2021). Human system engineering: A new model for addressing the user problem. *States Cybersecurity Magazine*
- Winn, R. (2021). Cybersecurity: The danger of comfort zones. *United States Cybersecurity Magazine*
- Wolfe, D. (2011). Banks Fight Phishing with i?1/2 Phishing?" *American Banker*, 176. *Gale Academic OneFile*. Retrieved from [https://link-gale-com.libproxy.temple.edu/apps/doc/A274355342/AONE?u=temple\\_main&sid=AONE&xid=9fc72ed3](https://link-gale-com.libproxy.temple.edu/apps/doc/A274355342/AONE?u=temple_main&sid=AONE&xid=9fc72ed3).
- Yoo, C. W., & Sanders, G. (2013). An exploration of group information security compliance: A social network analysis perspective. *International Conference on Information Systems*, 388–399.
- Yu, W. D., Nargundkar, S., and Tiruthani, N. (2008, July). A phishing vulnerability analysis of web based systems. In *Proceedings of the 13th IEEE Symposium on Computers and Communications (ISCC 2008)*. Marrakech, Morocco: IEEE, 326–331.
- Yukl, G. (2008). How leaders influence organizational effectiveness. *The Leadership Quarterly*, 19(6), 708-722.
- Zahra, S. A., Sapienza, H. J., & Davidsson, P. (2006). Entrepreneurship and dynamic capabilities: A review, model and research agenda. *Journal of Management Studies*, 43(4), 917-955.
- Zaki, T.; Uddin, M.S.; Hasan, M.M.; and Islam, M.N. (2017). Security threats for big data: A

study on Enron e-mail dataset. *Proceedings of the 5th International Conference on Research and Innovation in Information Systems (ICRIIS)*. Langkawi, Malaysia, 1-6.

## APPENDICES

## APPENDIX A

### IRB SUBMISSION



Research Integrity & Compliance  
Student Faculty Center  
3340 N. Broad Street, Suite 304  
Philadelphia PA 19140

Institutional Review Board  
Phone: (215) 707-3390  
Fax: (215) 707-9100  
e-mail: [irb@temple.edu](mailto:irb@temple.edu)



Not Human Subject Research Determination

Date: 26-Mar-2020

Protocol Number: 26685

PI: VANCE, ANTHONY O.

Sponsor: NO EXTERNAL SPONSOR

Project Title: Exploring Banking Cybersecurity Culture and its Influences on the Susceptibility to Phishing

---

On 26-Mar-2020, the IRB reviewed the protocol 26685: Exploring Banking Cybersecurity Culture and its Influences on the Susceptibility to Phishing.

The proposed activity is not research involving human subjects as defined by DHHS or FDA regulations. Consequently, Temple IRB review and approval is not applicable. You are welcome to pursue the activity, obtaining any applicable administrative or departmental (non-IRB) approvals.

This determination applies only to the activities described in this IRB submission and does not apply should any changes be made. Changes could affect this determination, therefore please contact the IRB for guidance.

**DHHS Definitions:**

Research - a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge.

Human subject - a living individual about whom an investigator (whether professional or student) conducting research:

1. Obtains information or biospecimens through intervention or interaction with the individual, and uses, studies, or analyzes the information or biospecimens; or
2. Obtains, uses, studies, analyzes, or generates identifiable private information or identifiable biospecimens.

**FDA Definitions:**

Research - any experiment that involves a test article and one or more human subjects, and that either: a) must meet the requirements for prior submission to the Food and Drug Administration; or b) the results of which are intended to be later submitted to, or held for inspection by, the FDA as part of an application for a research or marketing permit.

Human subject - an individual who is or becomes a participant in research, either as a recipient of the test article or as a control. A subject may be either a healthy individual or a patient.

For additional information, please see HRP-001 Policy - Definitions and HRP-421 Worksheet - Human Research on the IRB Forms & Standard Operating Procedures page.

Please contact the IRB at (215) 707-3390 if you have any questions.

APPENDIX B  
INTERVIEW QUESTION GUIDE

Research ID Code: \_\_\_\_\_ Date: \_\_\_\_\_ Phone: \_\_\_\_\_

**Demographics Questions:**

1. What is your age?
2. Gender:
3. What is your job title?
4. How long have you been employed in the banking industry?
5. Have you ever been successfully phished?

**Opinions and Values Questions**

1. How does the cybersecurity culture impact your job?
- 1a. Please explain the values, assumptions, and artifacts and how they are used to reduce phishing susceptibility.
2. Explain how cybersecurity culture affects information security policy compliance reducing phishing susceptibility?
3. How does cybersecurity culture increase awareness to address phishing susceptibility?
4. What is the best way to prepare bank employees from becoming phishing victims?
5. Please explain the effectiveness of your company's phishing and training campaign.
6. Please explain what factors improve or affect phishing at your bank.

**Follow-on Question**

If you could change anything regarding your organization's phishing efforts, what would it be?

## APPENDIX C

### HUMAN SUBJECTS PARTICIPANT CONSENT

Dear Potential Research Participant,

My name is Calvin Nobles, and I am a Doctor of Business Administration Candidate at Temple University. I am in the process of recruiting participants for my doctoral research study entitled “Exploring Banking Cybersecurity Culture Influences on Phishing Susceptibility.”

The purpose of this study is to explore how banking cybersecurity culture influences phishing susceptibility, which remains underexplored and an existing research gap. Phishing attacks are rampant in the U.S. banking sector and remain a viable threat to banks’ reputations, brands, and operations. Senior managers are critical in resourcing, leading, and fostering a cybersecurity culture that prepares banking employees to recognize and counter phishing attempts. I want to extend an invitation to participate in my study. I encourage you to consider volunteering to participate.

The study is part of my dissertation curriculum, the final requirement to complete the Doctor of Business Administration University. For data collection, online interviews (video) using Zoom. I will ask the study participants a series of open-ended questions in a semi-structured format during the interviews. The online interviews will be secured in my possession in a password-protected folder. By participating in this study, you may learn that some of the questions might intrude on your leadership decision-making and commitment to cybersecurity. You may withdraw from the study at any point during the research. If you opt out after completing the online interview, your data, input, and interview will be deleted. Each study participant will be referred to using a pseudonym to protect the participant's anonymity and confidentiality. I will not include your actual names or identifying information of participants in this research or its publication.

The study’s results will contribute significantly to the banking sector in the U.S. as banks face increasing phishing attacks; consequently, requiring banking employees to maintain high levels of security awareness and security training. Therefore, the results of this study will aid in understanding how banking cybersecurity culture impacts phishing susceptibility.

Temple University mandates that research participants sign a consent form (Human Subjects Participant Consent) to participate in this study, which advises you on the study and your rights. Your participation is entirely voluntary, and you may terminate your involvement at any time. Participants will not receive any form of compensation or reward before, during, or after completing the research study. Thank you for your willingness to participate in this research study. Please do not hesitate to contact me at calvin.nobles@temple.edu or 443-472-3469 if for any questions, comments, or concerns regarding the study.

Sincerely,  
Calvin Nobles  
DBA Candidate  
Signature \_\_\_\_\_

Date \_\_\_\_\_

**\*\*Please note that signing this consent form indicates your agreement to participate in this study.**

## APPENDIX D

### RECRUITMENT LETTER OR EMAIL

Date

Dear Potential Study Participant,

My name is Calvin Nobles, and a Doctor of Business Administration Candidate studying at Temple University. I am writing to invite you to participate in my research study about banking cybersecurity culture influences on phishing susceptibility. You are eligible to participate in this study because you are a current employee in the banking industry.

If you decide to participate in this study, you are required to complete a pre-interview session via a phone call, signed an Informed Consent Form, and agree to an online interview via Zoom, which I will record. I would like to audio and video record your online video interview, and then we will use the information as part of the data collection process. Each participant will be assigned a pseudonym to protect their confidentiality throughout the study.

There is no form of compensation for participating in this study.

Remember, this is entirely voluntary. You can choose to participate or not partake in the study. If you would like to participate or have any questions about the study, please email or contact me at [calvin.nobles@temple.edu](mailto:calvin.nobles@temple.edu)

Thank you very much.

Sincerely,

Calvin Nobles  
Doctor of Business Administration Candidate  
Temple University

## APPENDIX E

### TABLE OF CODES, SOURCES, REFERENCES, AND SAMPLE EXCERPTS

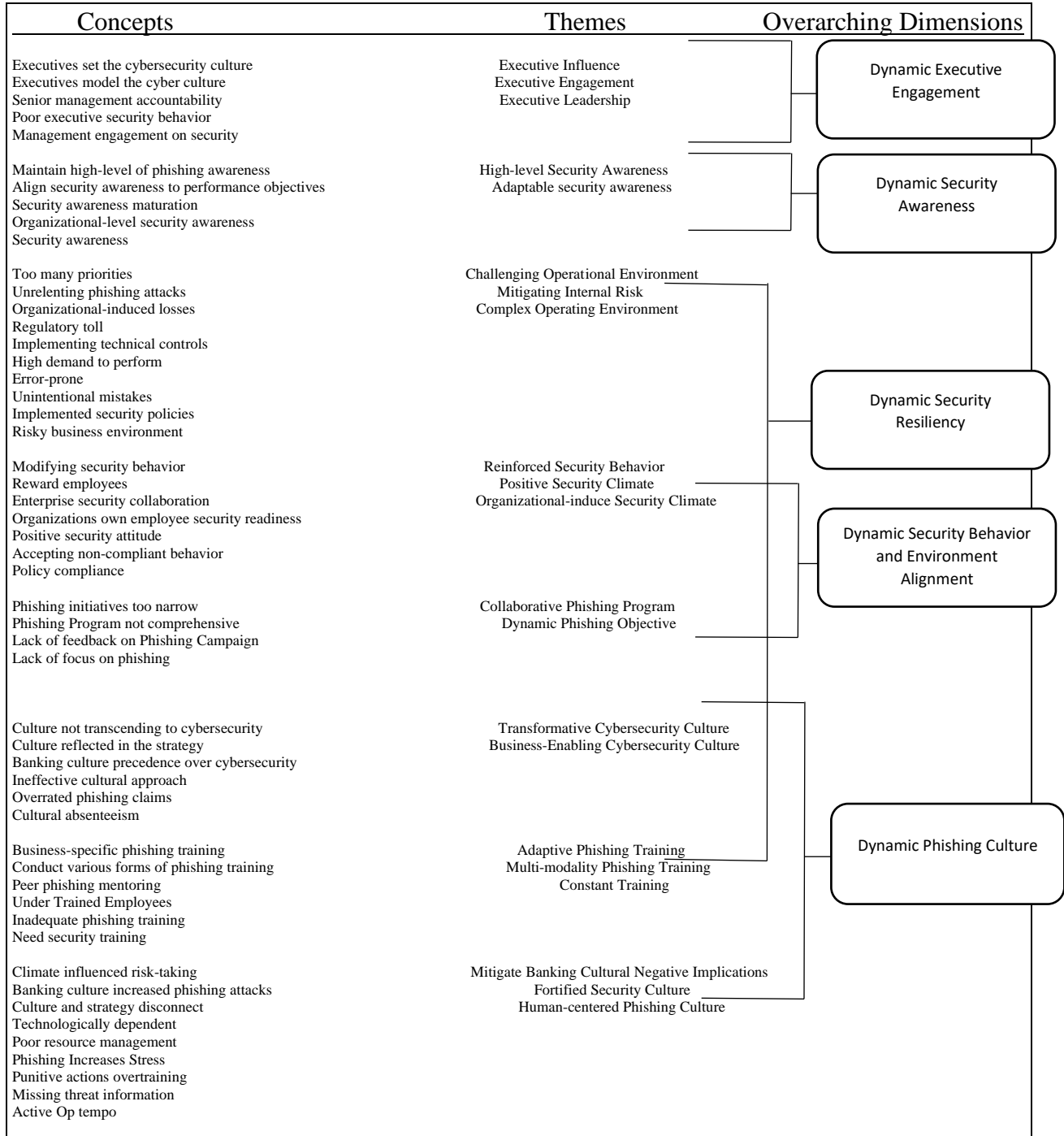
Code	Sources	References	Source and Sample Excerpt
Executives set the cybersecurity culture	17	22	STE-7 “Executives are responsible for driving the cybersecurity culture to meet the business needs”
Maintain high-level of phishing awareness	14	19	CYP-4 “Employees requires an increased level of phishing awareness to counter phishing attempts”
Executives model the cyber culture	9	16	CYP-9 “Executive are the security role models for employees and cultivate the security culture”
Too many priorities	7	11	NTE-1 “We have too many requirements that are not prioritized to focus on phishing”
Changing security behavior	15	21	STE-2 “Having a strong cybersecurity culture is to shape the security behavior of the organization”
Inadequate phishing training	18	27	STE-9 “Phishing attacks continue as a primary vector because employees are not properly trained to counter phishing attacks”
Lack of focus on phishing	12	15	NTE-5 “Employees receive phishing training once a year which is not enough to become proficient at avowing attacks”
Implementing technical controls	6	9	CYP-1 “Most banks implement technical controls are a measure to prevent phishing attacks”
High demand to perform	8	13	STE-4 “We have demanding operational tasks that make employees prone to phishing attacks”
Security awareness	24	31	STE-1 “ Security awareness is critical element for combatting phishing attacks in the bank sector”
Error-prone	11	15	CYP-7 “Humans are prone to make mistakes and these mistakes lead to successful phishing attacks”
Accepting non-compliant behavior	6	9	CPY-6 “Too many executives are the cause of non-compliant behavior”
Unintentional mistakes	5	12	NTE-13 “I have made several unintentional errors by clicking on links, and I immediately let my manager know”
Cultural absenteeism	10	17	NTE-8 “The important of phishing awareness do not transcend through the culture”
Active Op tempo	8	13	CYP-5 “The operations tempo is unbelievable and make employees susceptibility to phishing and all kinds of attacks”
Need security training	21	28	STE-10 “Employees need better and different modalities to increase their security proficiency”
Risky business environment	7	8	STE-8 “The nature of the banking culture is to take on risk and we will sort it later to include security risk”
Overrated phishing claims	3	9	NTE-9 “I believe the phishing attacks are overrated, we should click on links or open attachments”
Missing threat information	11	18	NTE-3 “I can stop or protect the bank if I don’t know what the threats are”
Implemented security policies	18	21	CYP -2 “Security policies are designed to produce a positive security behavior”

Positive security attitude	11	12	STE-11 "The purpose of cybersecurity culture is influence a positive security attitude"
Management engagement on security	9	10	STE-5 "As senior leaders, we have to engage all levels of the business to mitigate phishing"
Poor executive security behavior	6	7	CYP-1 "On numerous occasions, I have observed executives practicing poor security behavior"
Ineffective cultural approach	3	5	NTE-7 "When it comes to phishing, we sprinkle in a little phishing training as if it is not part of the culture"
Punitive actions overtraining	8	10	NTE-2 "My manager prefers punishment rather than training when we make mistakes"
Under Trained Employees	16	17	CYP-3 "Banking employees are woefully under-trained on phishing attack mitigation"
Phishing Increases Stress	7	7	STE-9 "Fighting phishing daily increases stress for employees"
Banking culture precedence over cybersecurity	10	14	STE-4 "Banking culture sets the tone for the organizational culture and cybersecurity"
Lack of feedback on Phishing Campaign	6	6	NTE-1 "Feedback on the organizational phishing program is not shared with the employees"
Organizations own employee security readiness	2	3	STE-7 "The responsibility for employee awareness for phishing is an organizational level"
Poor resource management	9	14	CYP-8 "Phishing is a poorly resourced rogram in the bank"
Culture not transcending to cybersecurity	8	8	CYP-5 "The cybersecurity culture is not representative of what the executives articulate"
Culture reflected in the strategy	4	4	NTE-3 "I see the culture transcending through the strategy and policies"
Phishing Program not comprehensive	2	4	NTE-5 "The phishing program does not address all phishing requirements completely"
Phishing initiatives too narrow	3	8	STE-1 "The bank's phishing approach is too narrow and lack focus"
Technologically dependent	13	14	CYB-6 "There is too much focus on technology than training employees on phishing defense"
Culture and strategy disconnect	8	11	STE-10 "Our track on cybersecurity incidents reflect a disconnect between culture and strategy"
Senior management accountability	9	9	STE-8 "Executives have to hold ourselves accountable for risk-related matters"
Regulatory toll	6	7	CYP-2 "The amount of regulatory red tape reduces focus on phishing"
Organizational-level security awareness	5	5	NTE-12 "Individual security awareness is a reflection of the organizational-level commitment to security"
Enterprise security collaboration	6	8	STE-1 "Security culture is reinforced through enterprise security collaboration"
Security awareness maturation	9	10	STE-4 "Successful phishing attacks is indicative of the bank's security awareness maturation"
Climate influenced risk-taking	4	7	CYP-9 "Increased risk-taking in cybersecurity is because of the banking culture"
Policy compliance	12	18	CYP-3 "Security behavior is directed through policy compliance"
Organizational-induced losses	3	5	NTE-12 "Phishing attacks are effective because organizations implement poor design"

Peer phishing mentoring	3	3	NTE-11 "I rely on peer mentoring when I have a phishing question"
Unrelenting phishing attacks	9	10	CYP-6 "The phishing attacks are non-stop and mentally fatiguing"
Banking culture increased phishing attacks	11	11	STE-2 "The risky culture of banks make them prone to phishing attacks"
Foster resilient security culture	5	6	STE-11 "Strict regulatory complicate makes banks resilient"
Conduct various forms of phishing training	4	6	NTE-14 "Phishing training lacks various forms"
Reward employees	8	10	NTE-4 "Compensate for not falling victim to phishing attempts"
Align security awareness to performance objectives	9	12	STE-3 "Security awareness needs to be reflected on performance objectives"
Business-specific phishing training	7	8	NTE-7 " The bank needs phishing training that is specific to the line of work"
Contagious cybersecurity culture	8	11	STE-5 "The banking culture drives an influential cybersecurity culture"

## APPENDIX F

### CONCEPTS, THEMES, AND OVERARCHING DIMENSIONS



APPENDIX G

FOUNDATIONAL WORK AND DATA FOR OVERARCHING DIMENSIONS

<b>Overarching Dimensions</b>	<b>Themes</b>	<b>Concepts</b>
Dynamic Executive Engagement		
	Executive Influence	<ul style="list-style-type: none"> <li>• STE-4 “As a security executive, I have a responsibility to directly drive the strategic objectives to shape the culture and organizational outcomes”</li> <li>• STE-8 “I must tirelessly advocate for the business to adopt and implement practices to meet the business objectives for phishing, I am responsible for partnering with other senior executives to ensure our workers are properly trained for phishing attacks”</li> <li>• STE-5 “The entire executive team are security champions for ensuring the business can effectively fight out phishing attacks and other security threats”</li> </ul>
	Executive Engagement	<ul style="list-style-type: none"> <li>• CYP-9 “From my level, what is missing is executive engagement, there is a disconnect from understanding the true issues that are causing phishing attacks and checking the boxes—the executives don’t listen to us”</li> <li>• NTE -2 “My senior manager takes phishing and all forms of cybersecurity threats seriously and keeps it top of mind during meetings and in email communications”</li> <li>• STE-1 “Because of my role in the company, the responsibility of success and failure falls squarely on shoulders and that is why I constantly meet and talk with other senior executives on being adaptive and proactive to phishing attacks”</li> </ul>
	Executive Leadership	<ul style="list-style-type: none"> <li>• STE-7 “Mitigating all forms of risk is an executive-level responsible, regardless if it is phishing, fraud, or account takeover”</li> <li>• NTE-4 “We need better training and phishing plans, the executives do not care because they are not punished for making mistakes, but we are held to higher standards for clicking on emails and attachments”</li> <li>• STE-3 “Executives must model the culture that we set for the enterprise”</li> <li>• CYP-6 “The bank is responsible for enhancing the security awareness of all employees through a series of training and informative sessions on the latest phishing threat vectors”</li> </ul>

Dynamic Security Awareness		
	High-level Security Awareness	<ul style="list-style-type: none"> <li>• CYP-1 “Information security awareness is vital for mitigating and protecting against phishing attacks”</li> <li>• STE-11 “Ever banking employee needs to a superb-level of security awareness”</li> <li>• STE-5 “Most phishing attack victims experience low levels of situational awareness during the phishing incident....we need a way to ensure employees are aware of the tactics used during phishing attacks”</li> <li>• NTE-7 “My security awareness is impeded by an increasing list of things to do and endless tasks to complete in a hurry”</li> <li>• NTE-4 “Security awareness is an essential tool for stopping phishing attacks”</li> </ul>
	Adaptable Security Awareness	<ul style="list-style-type: none"> <li>• CYP-8 “Security awareness needs to be adaptive based on the threat environment because employees are fooled into providing their credentials to unauthorized actors”</li> <li>• NTE-13 “I am a victim of a phishing attack at work and received severe punishment at work, but I was not trained on the phishing technique used against me....I was phished via my work cell phone”</li> <li>• NTE-11 “There are so many ways to phish someone, such as social engineering you starting with social media and targeting you at work. I am not sure the security awareness training I am receiving is effective....We need training that is updated and more frequent security awareness”</li> <li>• STE-1 “In today’s d, banking employees need an in-depth understanding of phishing attacks and security awareness....security awareness is a major defense mechanism for successfully stopping phishing attacks”</li> </ul>
Dynamic Security Resiliency		
	Challenging Operating Environment	<ul style="list-style-type: none"> <li>• STE-3 “The cybersecurity threats are complex and challenge the existing cultural approaches to phishing and other cybersecurity threats”</li> <li>• NTE-5 “There are too many phishing attacks and prevention methodologies that we are overwhelmed while trying to do our jobs in the bank”</li> <li>• CYP-1 “Human errors remain a significant threat because our operations are becoming too hard and unfair”</li> <li>• CYP-1 “Senior managers focus primarily on production and not information security because the bank is about making money at the risk of phishing attacks”</li> </ul>

		<ul style="list-style-type: none"> <li>• NTE-4 “I have made mistakes even though I did not mean to.....we implemented agile and now are running so fast at work that mistakes will happen”</li> </ul>
	Mitigating Internal Controls	<ul style="list-style-type: none"> <li>• STE-7 “One way of reducing risk in the organization is to implement security controls and restrict employees access to the network”</li> <li>• CYP-9 “Most organizations have implemented two-factor authentication as a technical control to restrict access and prevent unauthorized users from getting on our network”</li> <li>• “NTE-10 “At the bank today, we have limited access, and everything we do is monitored.....knowing that you are monitored is supposed to reduce bad behavior”</li> </ul>
	Adaptive Phishing Training	<ul style="list-style-type: none"> <li>• STE-7 “The number of successful phishing attacks in the bank is indicative of needing better phishing training....there are too many things working against our training such as workload, the pandemic, and cybercriminals targeting the banking sector”</li> <li>• NTE-12 “I don’t know what phishing training I should take”</li> <li>• NTE-12 “I rely on my peers and co-workers for assistance when I have a question about our because my I unsure if I know enough about phishing.....I argue for better training”</li> <li>• CYP-2 “Our training is too static and too old....banks do not know what training to provide to employees because there too many vendors pushing shitty training”</li> <li>• NTE-11 “Bank employees are poorly trained....we receive training once a year .....banking will continue to face phishing attacks until better training goes into effect”</li> </ul>
	Multi-modality Phishing Training	<ul style="list-style-type: none"> <li>• NTE-8 “We always have training on the computer or phishing simulation emails.....I don’t learn that way”</li> <li>• CYP-7 “I prefer face-to-face training so I can ask questions, but I only take computer-based training because that is what is offered”</li> <li>• CYP-8 “Other industries invest in real-world phishing training with companies that specialize in phishing.....banks have archaic phishing training”</li> <li>• NTE-1 “Our phishing training is one-stop training for all.....computer training....this is why phishing attacks continue to kill banks”</li> </ul>
	Continuous Training	<ul style="list-style-type: none"> <li>• STE-2 “Phishing attacks require a relentless training program.....training is trumped by work and making money</li> <li>• NTE-13 “We don’t stand a chance against phishing attacks because the training is a waste of time”</li> </ul>

		<ul style="list-style-type: none"> <li>NTE-4 “I can only fight against phishing based on the training I receive....the banks owe me better and more time to train consistently”</li> </ul>
Dynamic Security Behavior and Environment Alignment		
	Reinforced Security Behavior	<ul style="list-style-type: none"> <li>NTE-7 “Banks need to compensate employees for stopping phishing attacks”</li> <li>STE-1 “Demanding positive security behavior is imperative for countering phishing attacks.....this behavior must be set from the top”</li> <li>NTE-8 “Training and security awareness is not enough.....banks need to design ways to build stronger security behaviors creatively”</li> <li>CYP-3 “Increasing collaboration across directorates and teams to offer learning opportunities is one way to enhance security behavior by acquiring new knowledge”</li> </ul>
	Positive Security Climate	<ul style="list-style-type: none"> <li>STE-5 “Setting the climate of the organization is an executive function, and we continue to struggle with cybersecurity culture because most view security as a business impediment.....especially other executives who are concerned with profits/losses....security climate often clashes with the banking culture”</li> <li>STE-9 “Until we accept phishing as an equivalent risk to poor liquidity practices.....most banking employees will remain oblivious to phishing attacks.....our climate is skewed to fail”</li> <li>STE-4 “I accept the ownership for cultivating the climate to reduce phishing susceptibility.....the information security culture remains a high friction point for banking operations”</li> <li>NTE-11 “The increasing work demand shifts the focus from security to work bullshit....it is hard to build an individual security attitude that is constructive”</li> </ul>

	<p>Focused Collaboration</p>	<ul style="list-style-type: none"> <li>• NTE-9 “Our phishing initiatives lack feedback and follow-up.....we don’t see the data on any simulated phishing attacks”</li> <li>• CYP-6 “Most phishing programs are one way.....they are not open to partnering with security teams”</li> <li>• STE-2 “I have heard of some banks having a phishing competition, but my bank has a pretty lame program that is too narrowly focused”</li> <li>• STE-7 “Most banks phishing objectives are designed to be reactive.....making them vulnerable for phishing attacks”</li> <li>• CYP-1 “Employees don’t understand how phishing attacks happen.....a little training on the start to finish of an attack will help educate bank workers and remove the mystery.”</li> <li>• NTE-13 “I wonder why the phishing team does not share the scoring of phishing event by directorates....our program is dumb”</li> </ul>
<p>Dynamic Phishing Culture</p>		
	<p>Transformative Culture</p>	<ul style="list-style-type: none"> <li>• STE-5 “We need a transformative cybersecurity culture that provides extensive training on anti-phishing methods....as leaders, the onus is on us to change the culture to be more effective in the cybersecurity realm”</li> <li>• STE-8 “Our actions and behavior should be reflected in the culture and set the example for banking employees to follow....the culture and strategy can not contradict or be misaligned”</li> <li>• CYP-2 “I don’t see the culture in the strategy....the strategy is too abstract.....and often disregarded.....I do see leaders making bad decisions on cybersecurity threats”</li> <li>• CYP-5 “What strategy or culture.....we don’t discuss either on my team....both are missing”</li> </ul>
	<p>Business-Enabling Cybersecurity Culture</p>	<ul style="list-style-type: none"> <li>• NTE-14 “My manager encourages our team to leave the cybersecurity business to the IT folks....My manager does not discuss cybersecurity at all, he focuses only on our direct business”</li> <li>• STE-2 “A growing practice in most banks is to embed information security experts with the different business across the bank....this ensures the businesses are integrating information security practices in the day-to-day business efforts”</li> <li>• CYP-9 “Having a cybersecurity culture that is not shared across the bank is worthless....my job is to protect the bank’s business....but I need support from business teams”</li> </ul>

		<ul style="list-style-type: none"> <li>• CYP-6 “A peer told me on a different team that all the phishing concerns are overrated....just do your job and leave it to the security nerds”</li> </ul>
	Fortified Security Culture	<ul style="list-style-type: none"> <li>• STE-4 “It is time for executives to get off our asses and out in the spaces to talk cybersecurity and build partnerships with the CFOs, CMOs, and the COOs.....we have been fighting this battle too long by ourselves....a culture change is long overdue”</li> <li>• STE-3 “I believe a strong culture is based on executives setting the pace.....getting feedback from our direct reports....implementing changes to make the bank stronger in every aspect”</li> <li>• NTE-6 “The culture is one of punishing and terminating employees for making mistakes....all we need is better training”</li> <li>• STE-8 “When the CEO and COO are cybersecurity champions, the rest is history....that is where it starts and stops in the bank.....partnering with the right folks to shape the culture”</li> </ul>
	Human-centered Phishing Culture	<ul style="list-style-type: none"> <li>• NTE-1 “Why do we neglect phishing training, security awareness, and watch the same training videos every year.....give us something better for training”</li> <li>• CYP-4 “People are afraid to admit making mistakes out of fear of termination.....employees need the ability to self-report and not get fired”</li> <li>• CYP-9 “People are the weakest link because....leadership do not invest in its people”</li> <li>• STE-5 “Employees make mistakes at work because there are too many things on their plates....this is a normal practice in a bank.....it does not mean it is right”</li> </ul>