Enhancing Cyber Security Awareness in the UAE: Strategies Against Cyber Threats and Assets Protection

by

Mohamed Ahmed Saeed Abdulla AlZaabi

A thesis submitted in partial fulfilment for the requirements for the degree of (Doctor of Business Administration) at the University of Lancashire

October 2025

RESEARCH STUDENT DECLARATION FORM

Type of Award **Doctor of Business Administration**

School **University of Lancashire**

*Sections marked * delete as appropriate*

1. **Concurrent registration for two or more academic awards**

I declare that while registered as a candidate for the research degree, I have not been a registered candidate or enrolled student for another award of the University or other academic or professional institution

2. **Material submitted for another award**

I declare that no material contained in the thesis has been used in any other submission for an academic award and is solely my own work

3. **Collaboration**

Where a candidate's research programme is part of a collaborative project, the thesis must indicate in addition clearly the candidate's individual contribution and the extent of the collaboration. Please state below:

Not Applicable

4. **Use of a Proof-reader**

No proof-reading service was used in the compilation of this thesis**.**

Signature of Candidate 

Print name: **Mohamed Ahmed Saeed Abdulla AlZaabi**

ACKNOWLEDGEMENT

I would like to extend my heartfelt appreciation to all those who played a role in the successful completion of this research. I am particularly grateful to my Director of Studies, Dr. Udeme Jonah, and the entire supervisory team for their expert guidance, thoughtful feedback, and steadfast support throughout the course of this study. My sincere thanks also go to the participants who generously offered their time and shared their experiences, enriching this thesis with their valuable insights. I am deeply thankful to my family and friends for their ongoing encouragement and unwavering support throughout this journey. Finally, I recognize the academic and professional resources that have significantly contributed to the development and direction of this research.

TABLE OF CONTENT

Table of Contents

Abstract **7-8**

CHAPTER ONE **9-25**

1.1 Introduction 9
1.2 Background 9-17
1.3 Problem Statement 17-19
1.4 Research Aim & Objectives 19-20
1.5 Research Questions 20
1.6 Research Methodology 20-21
1.7 Research Significance 21-23
1.8 Research Structure 23-24
1.9 Research Limitation 24-25
1.10 Chapter-End Summary 25

CHAPTER TWO **26-95**

2.1 Introduction 26
2.2 History of Cyber Threats in Digital Space 26-32
2.3 Evolution of Asset Protection in Digital Space 32-33
2.4 Overview of cybersecurity awareness in digital space 33
2.5 History of Cybersecurity Awareness in the UAE 33-36
2.6 Definition of Cyber Threat 36-37
2.7 Types of Cyber Threats and Attacks 37-39
2.8 Concept of Cybersecurity Awareness 39-40
2.9 Importance of Cybersecurity Awareness 40-41
2.10 Components of Effective Cybersecurity Awareness Program 41-44
2.11 Cybersecurity Awareness and Asset Protection 44-46
2.12 Challenges of Cybersecurity Awareness 46-48
2.13 Cybersecurity Technologies and Innovations 48-52
2.14 Cybersecurity Best Practices 52-54
2.15 Strategies for Improving Cybersecurity Awareness 54-58
2.16 Prevalent Cyber Threats in the UAE 58-63
2.17 Current State of Cybersecurity Awareness in the UAE 63-64
2.18 Current Cybersecurity Policies and Strategies in the UAE 65
2.19 Recommendations for Strengthening Cybersecurity Awareness in the UAE 66-67
2.20 Underpinning theories 68-83
2.21 Comparative Analysis of Existing Studies 83-86
2.22 Gaps in Literature 86-89
2.23 Chapter Summary 89-95

CHAPTER THREE **96-112**

3.1 Chapter Overview 96
3.2 Research Philosophy 96-97
3.3 Research Approach 97-98
3.4 Research Strategy 98-99

3.5 Research Method Choice 99-101
3.6 Research Techniques and Procedure 101-104
3.7 Data Collection Method 104-106
3.8 Data Analysis Method 106-109
3.9 Summary of Data Analysis Method……...109-111
3.10 Chapter Summary 111-112

CHAPTER FOUR 113-155

4.1 Introduction 113
4.2 Qualitative Analysis (Key Insights & Patterns) 113-119
4.3 Summary of Current State of Cybersecurity Awareness and Threat Perception 120-121
4.4 Empirical Findings on Current Awareness and Strategy Effectiveness (Objective 1)...121-122
4.5 Sentiment Analysis 122-125
4.6 Summary of Organizational Strategy, Implementation, and Behavioral Challenges ... 126-127
4.7 Empirical Findings on Challenges and Recommended Strategies (Objective 2) 128-129
4.8 Thematic Categorization 129-134
4.9 Discussion 134-153
4.10 Chapter Summary 153-155

CHAPTER FIVE 156-173

5.1 Conclusion 156-158
5.2 Recommendations 158-162
5.3 Implications for Further Research 162-167
5.4 Research Contribution 167-172
5.5 Research Limitations 172-173

REFERENCES 174-180

APPENDICES 181-182

APPENDIX A: ETHICAL APPROVAL 181

APPENDIX B: INTERVIEW QUESTIONS 182

List of tables

Tables	Page
Table 1.1: Research Structure	**23**
Table 2.1: Internet Worms across History	**31**
Table 2.2: Significance of Cybersecurity Awareness	**40-41**
Table 2.3: Cybersecurity Best Practices	**53-54**
Table 2.4: Common Cyber Threats in the UAE	**61-62**
Table 2.5: General Studies	**72-78**
Table 2.6: UAE Studies	**78-83**
Table 4.1: Summary of Sentiment Analysis	**122**
Table 4.2: Summary of Key Themes	**130-131**
Table 5.1: Short Term Recommendations	**158-159**
Table 5.2: Medium-Term Recommendations	**159-160**
Table 5.3: Long-Term Recommendations	**161-162**

List of figures

Figures	Page
Figure 2.1: Phases of Cybersecurity Awareness in UAE	**35**
Figure 1.2: Cyber Threats and Attacks	**39**
Figure 2.3: Applications of AI in Cybersecurity	**49**
Figure 2.4: Significance of AI in Cybersecurity	**49**
Figure 2.5: Framework of Governance, Risk, and Compliance Practices (GRC)	**51**
Figure 2.6: Protection Motivation Theory	**68**
Figure 2.7: Technology Acceptance Model	**68**

Figure 2.8: Conceptual Model for Cybersecurity Training Acceptance (CTAM)	**70**
Figure 2.9: Theory of Planned Behavior	**71**

ABSTRACT

This research investigates the effectiveness of cybersecurity awareness strategies within the United Arab Emirates (UAE) and assesses their impact on reducing human-related vulnerabilities in organizational and national contexts. The study addresses the growing concern over insider threats, behavioral lapses, and insufficient public cybersecurity awareness, which persist despite the nation's ambitious digital transformation efforts.

The study adopted a mono-method qualitative research approach, rooted in an interpretivist paradigm, utilizing a phenomenological research strategy to explore participants' subjective experiences. The research focused on the highly critical UAE banking sector, which represents a vital, high-risk component of the national economy. The sample consisted of 50 employees ranging in age from 24 to 54 years and serving in key administrative, financial, technical, or cybersecurity-related roles. Primary data was gathered through semi-structured interviews, and the data was analyzed using thematic analysis. To ensure the credibility and trustworthiness of the findings, the analysis employed an iterative review process, peer debriefing, maintaining an audit trail, and member checking with selected participants.

The findings reveal a fundamental disconnect: a significant gap exists between national cybersecurity policy development and actual behavioral practice among employees and the public. While technical infrastructure is often well-developed, insider threats, negligence, and phishing susceptibility remain high. Employees displayed moderate theoretical knowledge of threats, but the practical application of cyber hygiene, such as strong password management, secure device usage, and timely incident reporting was often lacking. Many organizations lack comprehensive awareness programs tailored to specific roles. This deficiency, combined with insufficient integration of awareness initiatives and a lack of continuous training, confirms the problem is not merely technical but a profound socio-organizational and cultural challenge.

The research moves beyond traditional defense mechanisms to recommend a holistic, behaviorally informed strategy, offering specific contributions across three levels:

- Academic Contribution: The research bridges a significant gap by providing region-specific empirical analysis for the UAE context, which is currently underrepresented in global cybersecurity literature. It integrates interdisciplinary concepts from behavioral science and strategic management and proposes a multi-tiered analytical framework that connects individual awareness, organizational culture, and national policy for future scholarly adoption.
- Practical Contribution: The study delivers actionable, sector-specific strategies for organizational leaders. It recommends implementing a multi-layered awareness program that includes live hacking demonstrations, gamified e-learning, microlearning, and role-based training modules to enhance user engagement and behavioral reinforcement.
- Policy Implication: The findings directly inform policy development by identifying critical knowledge gaps and the need for greater enforcement in SMEs, which form most of the UAE economy. By fostering a resilient cybersecurity culture through cross-sector collaboration (government, private sector, and academia), the implementation of these strategies contributes directly to national security, economic stability, and the realization of the UAE's digital vision.

Keywords: Cybersecurity Awareness, Insider Threats, Behavioral Security, UAE Digital Strategy, Cyber Risk Management

CHAPTER 1: INTRODUCTION

1.1 Overview

In an increasingly interconnected world, where most transactions and operations are conducted digitally, cybersecurity has become a critical concern. The United Arab Emirates (UAE), as a rapidly developing nation integrating cutting-edge technologies, faces heightened risks from evolving cyber threats. This chapter presents an overview of the significance of cybersecurity, the growing need for cybersecurity awareness, and its impact on both personal and organizational asset protection within the UAE. Furthermore, it outlines the research aims, objectives, and questions that guide the study, which focuses on enhancing cybersecurity awareness as a strategy to combat cyber threats and protect assets.

1.2 Research Background

In recent decades, digital technologies have transformed the way individuals, businesses, and governments interact, conduct transactions, and share information. From social media interactions to online banking, from e-government services to global business operations, cyberspace is now a central feature of daily life. As the world becomes more reliant on interconnected digital infrastructures, the risks posed by cyber threats continue to escalate. This transformation has given rise to an urgent need for strong cybersecurity frameworks, especially

in regions that are increasingly adopting technology in both their public and private sectors, such as the United Arab Emirates (UAE).

Cyberattacks often have military or political intentions and frequently target groups with the intention of causing economic harm. These attacks, which include computer viruses, data breaches, and other attack techniques, happen on a variety of documents. Exclusive businesses utilize a variety of solutions, such as cybersecurity frameworks that continuously monitor state-of-the-art IT logs, to lessen the harm caused by hackers. (Alhasan et al., 2024) .

Furthermore, Information technology also mainly depends on cyber security. Cyber and security are the two keywords that make up this term. Cyber refers to the technology of networks and computers that contain information, whereas security refers to the safeguarding of that information on the internet or in systems. In other terms, cyber security is the process of protecting networks, devices, and applications against automated threats (Kaur, 2020). Moreover, cybersecurity is considered the technique of preventing sensitive data from being stolen or damaged (Taherdoost, 2022). It aims to protect computer and network systems against any malicious software, including viruses and Trojan horses. Furthermore, data mining is being utilized to provide solutions like audits and intrusion detection (Salem et al., 2022). According to Jaipong et al. (2023), cyber security is deemed essential since it only safeguards the immediate, useful, and continuous technological components.

1.2.1 The Rise of Cybersecurity Challenges

The rapid evolution of cyber threats, coupled with the growing sophistication of cyberattack techniques, makes cybersecurity a highly dynamic and pressing issue. Cyberattacks today are not limited to conventional forms like viruses and malware; they have evolved into more complex, multifaceted threats such as ransomware, denial-of-service attacks (DDoS), data

breaches, and advanced persistent threats (APT). These threats target individuals, corporations, and even governments, with malicious actors ranging from cybercriminals and hacktivists to state-sponsored hackers, all seeking to exploit vulnerabilities for financial gain, political motives, or social disruption.

Cybersecurity is a broad field that involves safeguards for computers and computer systems on the Internet. This could be understood in the context of government as the actions and measures taken by government agencies to safeguard citizens and institutions from online dangers like cyberwarfare, cyberterrorism, cybercrime, and espionage. Cybersecurity, in its most fundamental sense, refers to the protection of computer systems, networks, and data from unauthorized access, attacks, and damage. It encompasses a wide range of measures, from hardware and software protections to organizational policies and user training. At the same time, malware and ransomware like Flame and Shamoon have been proliferating and are a concern to both residential and business users. Therefore, cybersecurity encompasses both institutional and personal use (Ali, 2022). However, despite the growing recognition of cybersecurity's importance, many countries, including the UAE, still face significant challenges in fostering widespread awareness and preparedness among their populations.

Additionally, one of the main objectives of cybersecurity controls is to raise awareness of cybersecurity, its dangers, and its threats while also fostering a healthy cybersecurity culture. Additionally, preserving the privacy and security of vital information assets requires a high level of cybersecurity knowledge (Mohammed et al., 2022). The UAE has been at the forefront of technological innovation, making substantial investments in digital infrastructure, artificial intelligence, and the Internet of Things (IoT). This rapid technological progress, while a boon for economic development, has also exposed the nation to increased cyber risks. As government

services, financial institutions, healthcare systems, and critical infrastructure become increasingly digitized, the potential impact of cyberattacks grows exponentially.

According to the UAE's National Cybersecurity Strategy, the government has taken several measures to enhance the country's cyber defense mechanisms. These measures include the establishment of cybersecurity governance frameworks, national response capabilities, and the promotion of a cybersecurity culture. However, there remains a significant gap between the strategic vision and the actual level of cybersecurity awareness and preparedness among the general population and within organizations.

1.2.2 The Importance of Cybersecurity Awareness

A critical component of an effective cybersecurity strategy is raising awareness. Awareness programs aim to educate individuals and organizations about the risks they face in the digital world and equip them with the knowledge and tools necessary to prevent, detect, and respond to cyber threats. The absence of adequate cybersecurity awareness can lead to the exploitation of human vulnerabilities, such as weak passwords, phishing attacks, and the inadvertent disclosure of sensitive information.

Globally, many organizations and governments have recognized the importance of cybersecurity awareness programs. For instance, the European Union's General Data Protection Regulation (GDPR) requires organizations to train their employees regularly on security best practices. Similarly, the United States' National Institute of Standards and Technology (NIST) provides guidelines on improving cybersecurity practices, including awareness training. The UAE, recognizing the growing threats in the cyber landscape, has introduced several initiatives aimed at enhancing cybersecurity awareness, but challenges remain in effectively implementing these programs across the nation.

Research by the International Telecommunication Union (ITU) and the World Economic Forum (WEF) underscores the increasing sophistication of cyber threats, particularly targeting nations with high levels of digital adoption. In the UAE, which has positioned itself as a hub for technological innovation in the Middle East, this presents a critical vulnerability. Cybersecurity awareness campaigns are vital to mitigating this risk, yet there is limited research on their effectiveness, particularly in the context of the UAE's unique socio-cultural and technological environment.

Organizations follow up a systematic approach to cyber security awareness that can significantly reduce the risk of cyberattacks and protect their sensitive data and systems. Frameworks for cyber security awareness must be used to develop training programs that are both effective and address the unique demands and risks of an organization. Having basic cybersecurity awareness and knowing how to identify and report possible security incidents make it easier for all employees Depending on the awareness campaign's specific goal (Taherdoost, 2024). Among other things, ensuring cyber security awareness requires accurately identifying and comprehending the multilateral interdependence of services and tasks offered by businesses and government organizations because of the close relationships between critical infrastructure sectors and the sharing of information and communication technology resources.

Risk assessment processes, cyberspace modelling methods, and its dissemination inside cyberspace are all described (Amanowicz, 2024). Furthermore, while large organizations and governmental entities in the UAE often have established cybersecurity protocols, many small and medium-sized enterprises (SMEs), which form a significant portion of the economy, are still lagging in terms of cybersecurity preparedness. This discrepancy is often due to a lack of resources,

both financial and human, and an insufficient understanding of cybersecurity threats and best practices.

1.2.3 Cyber Threats in the UAE

The UAE is a prime target for cybercriminals due to its status as a global business hub, its high internet penetration rate, and its position as a key player in regional and international politics. Over the years, the UAE has experienced several high-profile cyberattacks. These include incidents targeting government websites, the financial sector, and critical infrastructure. A prominent example is the 2012 cyberattack that targeted UAE banks, which disrupted operations and exposed vulnerabilities in the country's financial system. Similarly, in 2016, a large-scale DDoS attack affected several UAE institutions, including government agencies and banks.

In recent years, sophisticated cyberattacks from state-sponsored hackers have also posed significant risks. One notable example is the Lazarus Group, a North Korean-affiliated hacking group that has been linked to a series of cyber espionage campaigns worldwide. In 2023, reports emerged that the Lazarus Group had been targeting organizations within the UAE, specifically in the defense and energy sectors. Such attacks underline the need for continuous vigilance and the development of advanced cybersecurity defense mechanisms, as well as the importance of fostering a cyber-aware culture within the UAE.

Cybercrime syndicates also pose a significant threat, with increasingly sophisticated methods of extorting money from victims through ransomware attacks. These groups often target both government and private entities, exploiting weak points in security infrastructures. The UAE's increasing reliance on cloud computing, data sharing, and digitalization of its critical infrastructure has further heightened the risk of such attacks.

In any given country, Policymakers can use the public's opinion of cyber security to evaluate awareness levels and develop appropriate cyber regulations that are fair, just, and acceptable to both citizens and companies. A nation's residents' extensive use of the internet, email correspondence, and other financial operations involving cyberspace should not be treated lightly (Maisikeli, 2020). Alongside the rapid advancement of technology, cyber risks are also evolving. Being ready for additional cyber threats is crucial. According to Luknar and Jovanović (2024), this study suggests aggressively conducting expert research, collaboration, experience sharing, and training. Every day, cyberthreats increase their intelligence. To avoid this kind of damage, it is important to cope with the knowledge related to the latest damages (Sripriya et al., 2020).

Cyber threats are characterized as harmful attempts to damage or interfere with computer networks and systems. It might have an impact on industries like government, healthcare, banking, business, and organizations that handle and exchange sensitive data. All facets of cybersecurity require defense mechanisms since cyber threats seek to compromise data availability, confidentiality, and integrity (Mahato et al., 2024). Consequently, Asset protection is the cornerstone of every task a protection officer performs. It is the protection officer's primary responsibility. Depending on who oversees drawing the lines between that role and function, asset protection might imply different things and serve different purposes. Security professionals are frequently required to contribute technical competence in effective and efficient security risk management operations since, in the end, asset protection is a function of organizational management (Ellis et al., 2020).

Also, understanding the categories of assets that an organization owns, and the associated risks is the initial step in asset protection. This will assist in determining the degree of control necessary to adequately protect each asset category. Strict authorization procedures, for instance, can secure

financial assets, while cybersecurity and encryption techniques can prevent data assets from being stolen or leaked (Igbojioyibo, 2024). A major development in 2023 was the discovery by CPX of the North Korean-affiliated Lazarus Group actively conducting cyber spying within the United Arab Emirates. As the United Arab Emirates continues to grow and integrate cutting-edge technologies like artificial intelligence (AI) asserting its prominence in regional and international arenas, it becomes an increasingly appealing target for cyber threat actors (Cyber Security Council, 2025).

1.2.4 The UAE's Cybersecurity Strategy

The UAE government has recognized the importance of cybersecurity and has taken several steps to address the challenges posed by cyber threats. The National Cybersecurity Strategy of the UAE is a comprehensive framework aimed at safeguarding the nation's digital infrastructure. It encompasses a range of initiatives, including the establishment of a cybersecurity council, the promotion of cybersecurity awareness programs, and the development of a national cybersecurity policy.

Consequently, the several integrated national policies that make up the UAE strategy landscape that oversees digital technologies work in tandem to support long-term goals like the UAE Vision 2071. It is understandable why national cyber security is one of these best practices. The market for cybersecurity, which is valued at AED 1.8 billion in the United Arab Emirates alone and AED 18 billion in the Middle East and North Africa (MENA), is a clear indication of its increasing significance. By the end of 2022, it is anticipated that the MENA cybersecurity markets would be valued at over AED 36 billion, driven by the GCC's especially robust growth (Telecommunication Regulatory Authority, 2018).

However, despite these efforts, the UAE faces significant challenges in fully realizing its cybersecurity vision. There is a noticeable gap between national strategies and the level of cybersecurity awareness at the individual and organizational levels. While large organizations may have the resources to invest in cybersecurity solutions, many smaller businesses and government entities still lack the necessary awareness and preparedness to combat modern cyber threats. To further elaborate on such initiatives, each strategy can be outlined severally as follows (United Arab Emirates, 2021):

1- The UAE Vision 2021 was introduced in 2010 by H.H. Sheikh Mohammed bin Rashid Al Maktoum, the Vice-President and Prime Minister of the United Arab Emirates. Its goal is to rank the United Arab Emirates among the world's greatest nations by the Union's Golden Jubilee.

2- “The UAE Vision 2071 is founded on the speech of His Highness Shaikh Mohammad Bin Zayed Al Nahyan, Crown Prince of Abu Dhabi and Deputy Supreme Commander of the UAE Armed Forces. The objective is for the next generation to live a better life in a better environment, with more opportunities and better communication with the world.

3- The National Cybersecurity Strategy of the United Arab Emirates is to establish a robust and secure cyber infrastructure in the country that permits residents to realize their dreams and businesses to prosper. The strategy's 60 projects and five pillars are designed to mobilize the UAE's entire cybersecurity ecosystem.

Therefore, the current research discusses cyber security and cyber threats, and it also manages to enhance cyber security awareness in the UAE strategies against cyber threats and Assets Protection.

1.3 Problem Statement

Organizations in the UAE must improve their cybersecurity plans since cyberthreats are always changing. Although organizations improve their external defenses, they frequently overlook securing sensitive information internally. Those with in-depth knowledge of system cycles, known as insiders, can do significant harm. Their motives range from data theft to harm, thus it's critical for organizations to understand and successfully combat these risks (Tubaishat & AlAleeli, 2024).

Moreover, Ignorance of how the nation's citizens view appropriate online conduct can also result in the growth of user monitoring, identity theft, phishing, viruses, spyware, Trojan horses, and cyberthreats to private companies, government agencies, utility grids, and military-related infrastructures. Ignoring online attitudes and behavior will result in inadequate policymaking, which is necessary to safeguard nations' IT assets, and will expose individuals to a wide range of cybercrimes. The technical skills of a nation's enterprises and financial institutions may also be compromised because of this negligence. Comparing the financial damage brought on by cybercrime to the corresponding danger, Canada and the UAE are comparable. These findings collectively indicate that the UAE needs more cyber security awareness programs (Maisikeli, 2020).

A wide range of entities, including nation-states, crime syndicates, insider threats, and politically motivated hacktivists, pose sophisticated cyberthreats in this context. Despite having different reasons for doing so, these enemies all aim to breach corporate networks and compromise confidential information. The UAE also faces a variety of attack techniques, ranging from ransomware and DDoS attacks to malware deployment and vulnerability exploitation.

Organizations in the UAE must not only comprehend the nature of these threats but also modify their defenses to proactively oppose the dynamic techniques used by these threat actors in order to meet these challenges (Cyber Security Council, 2025).

Additionally, there are three primary factors that make cybersecurity in the UAE a sector that requires particular attention. The first is the degree of digitalization and interconnection of the nation, which encompasses the sophistication and complexity gap, obsolete software systems, and rising digitalization. The second is the current lack of public knowledge, which is reflected in policies and is typically seen in society and the workplace. Last but not least, the necessity of building a comprehensive national capacity to help both individuals and organizations solve the deficiencies in the hiring of professionals is also regarded as a crucial justification for stepping up cybersecurity efforts (Ali, 2022).

Based on the above, Despite the UAE cybersecurity strategies that complement one another and act as enablers to serve long-term visions, the problems revolve around the lack of cybersecurity awareness in UAE amongst users and organizations' human resource in general. To make matters even more threatening, the UAE is confronted with an array of attack methodologies, from exploiting vulnerabilities and deploying malware to executing ransomware and DDoS attacks. Hence, UAE is in critical need of implementing more strategies to overcome Cyber Threats and Assets Protection through more optimized awareness-oriented strategies.

1.4 Research Aim and Objectives

The main aim of this study is to evaluate the enhancement of cybersecurity awareness in the UAE as a strategy for protecting assets and mitigating cyber threats.

The study's objectives are:

1. To assess the level of cybersecurity awareness in the UAE.

2. To examine the extent of implementation of cybersecurity strategies aimed at protecting against cyber threats and safeguarding assets.
3. To identify any statistically significant differences in participants' responses regarding how cybersecurity awareness strategies are enhanced.
4. To identify any statistically significant differences in participants' responses regarding how cybersecurity strategies are implemented to protect assets and prevent cyber threats.

1.5 Research Questions

The central research question (CRQ) for this study is:

- What is the extent to which cybersecurity awareness can be enhanced in the UAE to protect against cyber threats and asset damage?

To answer this central question, the study will address the following secondary research questions (SRQs):

1. What is the current level of cybersecurity awareness in the UAE?
2. What is the level of implementation of cybersecurity strategies in the UAE, specifically regarding the protection of assets and the mitigation of cyber threats?
3. Are there statistically significant differences in the responses of participants regarding the enhancement of cybersecurity awareness in the UAE?
4. Are there statistically significant differences in the responses of participants regarding the implementation of cybersecurity strategies for protecting assets and mitigating cyber threats in the UAE?

1.6 Research Methodology

This study employs a mono-method qualitative approach, rooted in interpretivist research philosophy. This technique allowed for a thorough exploration of participants' attitudes, living

experiences, and perceptions of cybersecurity threats and concerns. This philosophical stance is critically necessary because the research problem is fundamentally sociological and behavioral. The interpretivist paradigm allows for a deep, contextual exploration of how reality is socially constructed and perceived by human encounters**.**

The methodology utilizes an inductive research approach and adopts a case study strategy, focusing specifically on the highly vulnerable UAE banking sector. This case study is deliberate, favoring contextual insights over statistical generalizability, thereby resolving a key limitation of previous studies that lack region-specific data for the UAE. Primary data was gathered through semi-structured interviews; the interviews were recorded with the participants' informed consent and analysis was conducted using thematic analysis. Finding, examining, and summarizing patterns (or themes) in data is the main goal of thematic analysis, which is ideal for uncovering the hidden meanings, attitudes, and actions related to cybersecurity behavior and asset protection**.**

1.7 Research Significance

The significance lies in the potential to contribute to the ongoing efforts to improve cybersecurity in the UAE. The UAE is rapidly becoming one of the most technologically advanced countries in the region, and with this growth comes an increased risk of cyber threats. This research offers significant contributions by directly addressing the most critical vulnerability to the UAE's cybersecurity awareness and the protection of digital assets have become critical priorities in a highly volatile and rapidly digitizing economic environment.

1.7.1 Policy and National Security

The findings directly inform the strategic priorities of the UAE's National Cybersecurity Strategy by identifying concrete gaps in knowledge and understanding among employees that often render technical controls ineffective (Al Marzooqi, 2023). By offering behaviorally informed recommendations, the research contributes to a more resilient national infrastructure, safeguarding the nation against single, successful cyberattacks that could destabilize economic stability (Schneier, 2017). The shift from a purely technical compliance mindset to one emphasizing human-centric awareness directly supports the long-term, high-stakes goals outlined in the UAE Vision 2071. Therefore, the study acts as a vital evidence-base for policymakers to refine regulations and target awareness campaigns more effectively.

1.7.2 Academic Contribution

The research bridges a critical gap in scholarly literature by providing region-specific empirical analysis for the Middle East, a context significantly underrepresented in global cybersecurity studies (Al-Ghamdi & Al-Hashmi, 2020). Previous research often assumes the applicability of Western models, which may fail to account for unique cultural and organizational structures found in the UAE. This study moves beyond a purely technical focus by integrating concepts from behavioral science and strategic management to construct a holistic, multi-tiered analytical framework for cyber resilience. Furthermore, by applying qualitative methodology, specifically a case study approach validated by scholars like Yin (2018), the study provides the rich, contextual depth necessary to understand *why* behavioral vulnerabilities persist, a dimension often missed by large-scale quantitative surveys.

1.7.3 Practical and Corporate Benefits

For organizations, particularly those in the highly regulated banking sector, the study delivers actionable, evidence-based strategies for designing more effective, non-compliance-based

awareness programs. It provides concrete insights into the adoption of modern training techniques, such as gamified learning mechanisms (York & deHaan, 2018), which have been shown to enhance user engagement and knowledge retention far better than traditional mandatory training. By illuminating the critical factors that drive or inhibit secure behavior, the research empowers organizational leaders to mitigate insider threats and negligence proactively, thereby optimizing their return on investment in technical security infrastructure and fostering a strong, positive cybersecurity culture.

1.8 Research Structure

This thesis is structured into five chapters, detailing the research process from problem definition to final recommendations.

Table 1.1: Research Structure

Section	Description
Chapter I: Introduction	Establishes the research background, problem statement, aims, objectives, and guiding research questions, setting out the study's scope and overall structure.
Chapter II: Literature Review	Systematically reviews existing academic and industry literature on cyber threats, asset protection, and cybersecurity awareness, identifying the theoretical and empirical gaps that this study addresses.
Chapter III: Methodology	Details the qualitative, interpretivist framework, research strategy, sampling, and the rigorous procedures used for data collection (interviews) and analysis (thematic analysis).

Chapter IV: Findings of the Data-Analysis Procedure and Discussion	Presents and discusses the results derived from the thematic analysis of the data, directly answering the research questions and comparing findings to existing literature.
Chapter V: Recommendations and Conclusion	Summarizes the study's conclusions, outlines the academic and practical contributions, and provides specific recommendations for policymakers and organizations in the UAE.

1.9 Research Limitations

The scope and methodology of this research impose certain limitations that were accepted as necessary trade-offs to achieve the required depth and context-specificity:

- Geographical and Sample Limitation: The research is strictly geographically limited to the UAE and focuses on a specific sample of professionals, primarily within the banking sector. This qualitative approach, while necessary for generating rich, contextually grounded data, means the findings lack generalizability to other countries or to drastically different sectors (e.g., critical infrastructure) within the UAE.
- Methodological Limitation (Qualitative Focus): The use of a mono-method qualitative approach relying on interview data provides perceptual and behavioral insights but does not generate statistically predictive models or measure actual behavioral outcomes. Therefore, the research offers an in-depth understanding of *why* human vulnerabilities persist, rather than providing statistically correlational evidence.

- Temporal Limitation: The research is conducted within a specific timeframe (academic year of 2025). Given that the cybersecurity environment is exceptionally dynamic and rapidly evolving, the findings reflect the state of awareness and policy at the time of data collection and may require continuous revision in light of emerging, sophisticated threats.

1.10 Chapter Summary

This chapter has provided an introduction to the study, highlighting the importance of cybersecurity awareness and the ongoing challenges in the UAE. It has outlined research questions, aims, objectives, and methodology, setting the stage for a deeper exploration into how cybersecurity awareness can be enhanced to protect against cyber threats and safeguard critical assets. The following chapters will review existing literature, detail the research methodology, and present the findings that will contribute to the UAE's efforts in improving cybersecurity.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

The very rapid advancement of human civilization in the first few decades of the new century has brought about both many benefits for every aspect of human society and several drawbacks that jeopardize the way modern society functions. This is also the reason why maintaining safety is becoming more important. Cybersecurity is one of the most important topics in the security domain. The rapid development and widespread use of new, modern technologies, particularly information and communication technologies, the growing use of augmented reality, artificial intelligence, and the Internet of Things, as well as the general rise in digital transformation, the process by which businesses and organizations incorporate digital technologies into their operations and activities to boost productivity, creativity, and competitiveness, all contribute to its steadily growing significance. Along with new prospects, this also presents new security issues that are directly tied to safeguarding their systems, data, information, operations, etc. from online attacks (Ivančík, R., & Kazanský, 2024). A major worry in the connected world of today is cybersecurity. An exponential surge in cyber dangers has resulted from the quick development of technology and our growing reliance on digital systems (Sharma et al., 2023).

2.2 History of Cyber Threats in Digital Space

The history of cyber threats parallels the evolution of computing and digital communications. As societies adopted digital technologies for personal, commercial, and governmental purposes, new avenues for exploitation emerged. Cybersecurity, originally a niche concern within IT departments has since grown into a critical global issue, encompassing

everything from individual privacy to national security. The threats that once targeted standalone computers have now evolved to affect entire nations, financial markets, infrastructure, and global supply chains.

Cyber threats are generally classified into three main categories: cybercrimes, cyberwarfare, and cyberterrorism. Understanding these classifications is fundamental to recognizing the intent, scale, and potential harm behind each threat type.

- Cybercrime refers to illegal activities carried out using digital technologies, often for financial gain. These include identity theft, phishing, ransomware, credit card fraud, and unauthorized data access.
- Cyberwarfare is state-sponsored or politically motivated activity aimed at disabling or disrupting another nation's digital infrastructure, including government databases, communication networks, or energy grids.
- Cyberterrorism involves attacks by non-state actors or terrorist organizations to cause fear, disrupt services, or manipulate information systems with the goal of achieving ideological objectives.

As Malik et al. (2022) note, the categorization and regulation of these threats have become essential to law enforcement and legal frameworks. Cybersecurity legislation now operates under both domestic and international law, addressing concerns ranging from privacy violations to cross-border cyber espionage. Regulatory bodies such as the European Union Agency for Cybersecurity (ENISA), the U.S. Cybersecurity and Infrastructure Security Agency (CISA), and the UAE's Telecommunications and Digital Government Regulatory Authority (TDRA) all contribute to shaping global cyber governance. With the world increasingly dependent on technology, the nature of cybersecurity threats has also grown more complex, sophisticated, and pervasive. This

complexity stems from the expansion of the digital environment itself. The proliferation of mobile devices, Internet of Things (IoT) gadgets, cloud computing, and smart infrastructure has dramatically increased the number of vulnerable entry points. Moreover, hackers have access to more powerful and user-friendly tools than ever before, making it easier to launch attacks with minimal technical knowledge.

One of the first well-known cyber incidents was the Morris Worm, released in 1988. Designed by a university student, this worm exploited vulnerabilities in Unix systems, causing major disruptions across early versions of the Internet. Though not intended to cause harm, the Morris Worm infected nearly 10% of the approximately 60,000 computers connected to the Internet at the time, demonstrating the severe consequences of unchecked vulnerabilities even in a nascent digital world. Fast forward to the early 2000s, the SQL Slammer worm in 2003 spread within minutes by exploiting a known vulnerability in Microsoft's SQL Server. This worm caused widespread network outages, including disruptions to banking systems and emergency services. Unlike earlier viruses that required users to open attachments or execute files, SQL Slammer propagated automatically and rapidly, setting the stage for a new wave of self-propagating malware.

Cyber threats evolved further with the emergence of targeted attacks such as Stuxnet in 2010. Believed to be a joint U.S.-Israeli operation, Stuxnet was a worm designed to target Iran's nuclear centrifuges. It marked a watershed moment, as it was the first known malware designed to physically sabotage industrial infrastructure. This demonstrated that cyber threats had progressed beyond data theft into the realm of geopolitical warfare. Parallel to these developments, ransomware gained traction as a lucrative tool for cybercriminals. In ransomware attacks, malicious software encrypts a victim's data and demands payment, often in cryptocurrency, for the

decryption key. Notable examples include WannaCry (2017) and NotPetya (2017), both of which affected systems worldwide, including healthcare institutions, government offices, and multinational corporations. These incidents showed how cyber threats can cripple operations, disrupt supply chains, and incur massive financial losses.

In recent years, cyber attackers have also employed social engineering, exploiting human behavior rather than technical vulnerabilities. Tactics such as spear-phishing, highly targeted and personalized phishing attacks have become increasingly common. Social engineering is particularly dangerous because it can bypass even the most advanced technological defenses if a human user is tricked into disclosing credentials or downloading malware. A major accelerant in the history of cyber threats is the rise of Artificial Intelligence (AI) and Machine Learning (ML). These technologies, while also used defensively to detect anomalies and automate responses, are being adopted by cybercriminals to design more evasive malware and automate large-scale attacks. According to Bakar and Zolkipli (2023), AI models enable attackers to learn from defensive patterns, mimic user behavior, and identify system vulnerabilities faster than traditional methods allow. For example, AI-driven phishing tools can generate grammatically correct and contextually relevant phishing emails at scale, improving their chances of deceiving recipients.

Cyberterrorists, too, have adapted their strategies in response to the digital age. They now deploy propaganda campaigns, data leaks, and service disruptions as part of psychological and ideological warfare. The use of deepfake technology, which leverages AI to fabricate believable audio or video impersonations has raised alarm over its potential for misinformation and blackmail. The increasing interconnection of systems has introduced the concept of supply chain attacks, where an attacker infiltrates a trusted third-party vendor to compromise their clients. The SolarWinds breach in 2020 is a prominent example, affecting U.S. federal agencies and major corporations.

This attack highlighted the vulnerability of trusted software updates as vectors for massive and stealthy breaches.

To cope with this escalating threat landscape, cybersecurity defenses have also evolved. Zero Trust Architecture, which assumes no implicit trust for users inside or outside the network, is becoming a standard model. Behavioral analytics, biometric authentication, and real-time monitoring are now being integrated into cybersecurity infrastructure. Furthermore, cyber threat intelligence sharing across organizations and nations has gained momentum, with platforms like MITRE ATT&CK and information-sharing communities promoting a more collective approach to defense. Amid this evolution, cybersecurity awareness among users and employees remains a critical defense layer. Even the most secure systems can be compromised if end-users are unaware of safe practices. Therefore, cybersecurity training and awareness campaigns are now integral to organizational defense strategies.

The UAE, for example, has recognized the growing importance of cybersecurity through national strategies and initiatives. Institutions like the UAE Cybersecurity Council and the establishment of the Computer Emergency Response Team (aeCERT) reflect a proactive stance. Cybersecurity education and public awareness campaigns have been implemented across schools and workplaces, reinforcing the country's preparedness. As we project into the future, cyber threats are expected to become more autonomous, adaptive, and undetectable, especially with the development of quantum computing. While this technology holds promise for data processing, it also poses a significant risk to current encryption standards, which could be rendered obsolete almost overnight. Therefore, research into post-quantum cryptography is already underway, illustrating the need for continuous innovation in both offensive and defensive cybersecurity strategies.

Travis et al., (2023) summarize the internet worms in the following table:

Table 2.1: Internet Worms across History

Worm	Year	Spread Method	Impact	Infection Rate	Estimated Cost
Morris Worm	1988	Exploited finger, send mail and login vulnerabilities; searched local files (e.g., hosts) and scanned local network	Severe disruption of global Internet and local enterprise networks due to replication traffic	Infected roughly 10% of Internet computers	$100 million (approx. $156 million in 2003 dollars)
SQL Slammer	2003	Single-packet infection exploiting SQL Server vulnerability; scanned 25,000 hosts per second.	Severe global disruption within 8 minutes; doubled in size every 8 seconds	Less than 1 in 1,000 Internet computers infected	Approximately $1 billion

In summary, the history of cyber threats reveals a rapid and unrelenting evolution driven by advances in technology, changes in human behavior, and geopolitical shifts. The transition from simple worms to AI-driven, state-sponsored cyberattacks underscores the critical need for holistic, forward-thinking cybersecurity frameworks. As the digital frontier continues to expand, so too must our vigilance, readiness, and collective efforts to defend it.

2.3 Evolution of Asset Protection in Digital Space

According to Ellis et al., (2020), asset protection moved from physical assets to a complex approach that incorporates cybersecurity, compliance matters, and advanced technology in securing digital assets. Some of the most critical concerns regarding such a transition are:

1. Onset of Cyber Threats: The proliferation of digital technology has introduced new threats like hacking, identity theft, and data breaches into the forefront, and organizations were compelled to make both digital and physical asset preservation their top priority.
2. Multi-Level Security Measures: Digital asset protection uses multi-level security measures including firewalls, encryption, intrusion detection systems, and multi-factor authentication to form robust layers of protection against cyber-attacks.
3. Compliance Burden: Companies are required to adhere to GDPR, HIPAA, and PCI-DSS compliance regulation standards to effectively deploy digital asset protection as non-compliance would be associated with humongous financial costs and loss of company reputation.
4. Organizational Cybersecurity Focus Shift: E-business has witnessed the focus shift at the organizational level to cybersecurity, requiring professionals to possess a broader set of skills, with the integration of IT and security functions becoming more and more critical.

5. Incident Response Planning and Advanced Technology Implementation: Organizations now need to have documented incident response plans and implement advanced technologies like artificial intelligence and machine learning in the field of cybersecurity to repel threats and safeguard digital assets.

2.4 Overview of cybersecurity awareness in digital space

Cybersecurity awareness can be defined as the level of awareness among users of the Internet about the possibility of manipulation of Internet information and the tools to prevent that crime don't occur on the Internet (Zahiroh, 2019). Cybersecurity in the digital world matters due to the risk of malicious actors globally, the convergence of the physical and virtual worlds, and the dynamics of intricate cyber networks. As a step towards enhancing online security, individuals and institutions need to adopt basic cyber habits, or "cyber hygiene," such as having good passwords, updating software, being cautious with suspicious links, and activating multi-factor authentication. Private and public spheres must design individualized cybersecurity responses to protect activities because the increased use of information technology increases the threat of vital interruptions that might impact the economy and normal daily life (Cybersecurity and Infrastructure Security Agency (CISA), 2025).

2.5 History of Cybersecurity Awareness in the UAE

According to The United Arab Emirates' Government portal. (2025) The History of Cybersecurity Awareness in the UAE can be understood through the following phases:

- **Early Initiatives:** The UAE began emphasizing cybersecurity awareness early in the 2000s when the nation embraced technology and digitalization aggressively.

- **Creation of Key Organizations:** The UAE initiated the Telecommunications and Digital Government Regulatory Authority (TDRA) in 2008, and it became the focal organization for the creation of cybersecurity policies as well as public awareness programs.
- **The aeCERT:** Once again, in 2008, the UAE Computer Emergency Response Team (aeCERT) was established to address cyber incidents as well as, no less importantly, warning the public and companies about cyber threats and safety precautions.
- **Targeted Awareness Campaigns:** Over the years, the UAE carried out nationwide awareness campaigns to enlighten the public, especially children and youth, on internet safety, cyberbullying, and scams, as well as digital ethics. These efforts were carried out through schools, public forums, and the Internet.
- **Digital Citizenship Emphasis:** The UAE has in recent years put a stronger emphasis on digital citizenship, calling for not only technical safety but also moral conduct on the Internet at all levels—government, organizations, families, and students.
- **Collaboration & International Standards:** The UAE has worked actively with global cybersecurity authorities so that its awareness campaigns take the best global practices, especially in the era of increased cyber-attacks.
- **Evolution Continues:** Now, the UAE cybersecurity awareness strategy is integrated into national security and digital transformation agendas so that education, awareness, and proactive prevention keep pace with the most recent technological advancements.

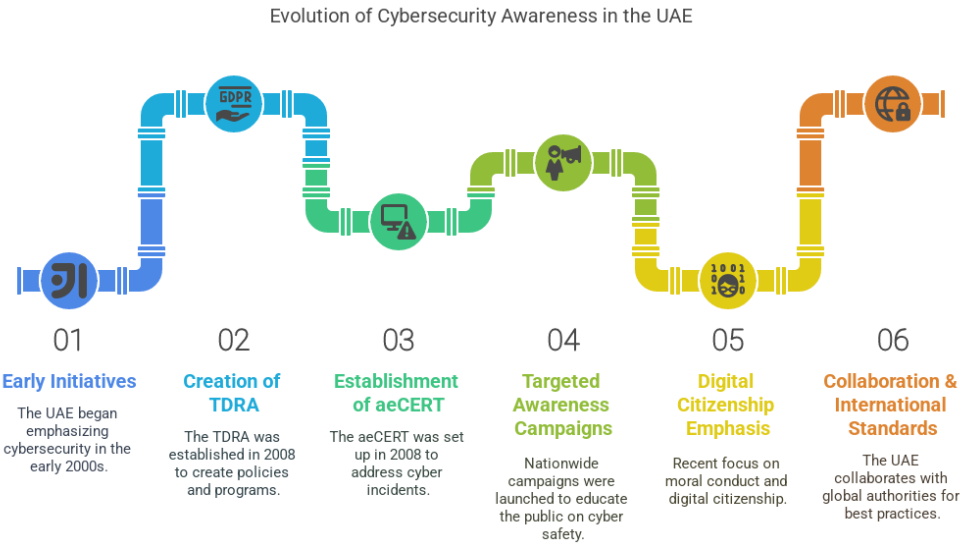


Figure 2.2: Phases of Cybersecurity Awareness in UAE

Source: Created by the Researcher

Based on the above it can be concluded that cybersecurity awareness and asset protection have evolved with the increasing sophistication of cyber threats and the pace of digital transformation. As complex cyberattacks developed, it became clear that technological controls alone are not enough — awareness and promoting proactive cybersecurity behaviours are essential components of any effective security strategy. In the UAE, cybersecurity awareness has grown from general awareness campaigns to full-fledged national plans supported by specialized agencies like TDRA and aeCERT and targeted public campaigns. Cybersecurity awareness is no longer a purely technical issue today, but a central aspect of digital citizenship in which citizens, organizations, and government join hands together in protecting the digital environment. This continuous evolution reflects the UAE's commitment to enhancing cyber resilience and staying ahead of emerging cyber threats, ensuring a safer digital future for all.

Second: Theoretical Framework

There are many kinds of cyber threats, as hackers and cybercriminals are always trying to come up with new ways to get into digital systems for a variety of reasons. It takes a great deal of technical skill to manipulate software setups and program code to mitigate certain specific cyberattacks (Barbhuiya, 2024).

2.6 Definition of Cyber Threat

In the following section, there is a presentation of critical definitions regarding cyber threats, outlining how the term has evolved and highlighting the various forms, sources, and impacts of these threats as coined by recent studies and experts: According to Calvo-Mora et al., (2022) cybernetics, the discipline of comprehending how machines move, is where the name "cyber" first appeared. These days, the phrase is used to refer to information security issues. Any harmful act that aims to steal confidential information, interfere with regular business activities, corrupt data, or render it unusable is considered a cyber threat. Unauthorized individuals (often cyber attackers) trying to access allowed data are the source of cyber threats. Malware, ransomware, DoS, DDoS, data breaches, and phishing are a few examples of frequent cyberattacks.

Bahmanova and Lace (2024) also indicated that cyber threats are the ever-changing risks presented by malevolent online activity directed against people and institutions in a variety of industries. These risks include a range of difficulties brought on by developing technologies and illegal strategies, such as cybercrime, cyberterrorism, and espionage. In addition to that, Kashika et al., (2024) stated that any hostile act by a person or entity that poses a risk to the confidentiality, integrity, and availability of assets by taking advantage of vulnerabilities is referred to as a cyber-threat.

In summary, the mentioned definitions lead towards the dynamic nature of evolving cyber threats and the rising complexity of cyber risks faced by individuals, organizations, and governments. Good cybersecurity strategies are developed with an understanding of these definitions, they can create awareness and facilitate enhanced readiness to tackle emerging digital threats in the increasingly connected world.

2.7 Types of Cyber Threats and Attacks

There are many types of cyber threats and attacks, and they are as follows:

- **Phishing**: The effort to get private data, including credit card numbers, login passwords, or personal information, using deceptive means that pose as emails, websites, or other offers (Mahato et al., 2024).
- **Threats originating from malware**: Malicious software that is intended to compromise, harm, or steal data from computer systems is the source of malware-based threats. These dangerous software programs include, but are not limited to, spyware, ransomware, and viruses Barbhuiya, (2024). It is a malicious software program that infiltrates, steals, disrupts, and generally damages systems in computer settings. It is employed in Trojan horses, worms, ransomware, spyware, and adware. (Mahato et al., 2024)
- **Distributed Denial of Service, or DDoS**: is the process of purposefully flooding a server with requests to bring down a target website or network infrastructure. Depending on how much your company depends on the Internet, users won't be able to access your site or network, which might lead to a partial or whole closure of operations (SBIR, 2016). DDoS and DoS Attacks: DoS and DDoS attacks

operate by flooding servers and networks with excessive traffic volumes, which can prevent authorized users from accessing necessary resources by depleting system resources (Mahato et al., 2024).

- **Password attacks**: The easiest method for hackers to access their target's databases and accounts is to crack a password. Password attacks can be divided into three categories: dictionary attacks, which use a program to try various dictionary word combinations; brute force attacks, which guess passwords until the hacker gains access; and keylogging, which records every keystroke a user makes, including login IDs and passwords (SBIR, 2016).
- **Zero-Day Exploits**: These are flaws in specific software that the vendor supplying it is unaware of or for which there are currently no fixes. The assaulter makes use of the (Mahato et al., 2024). The following figure shows the various types of cyber threats and attacks:

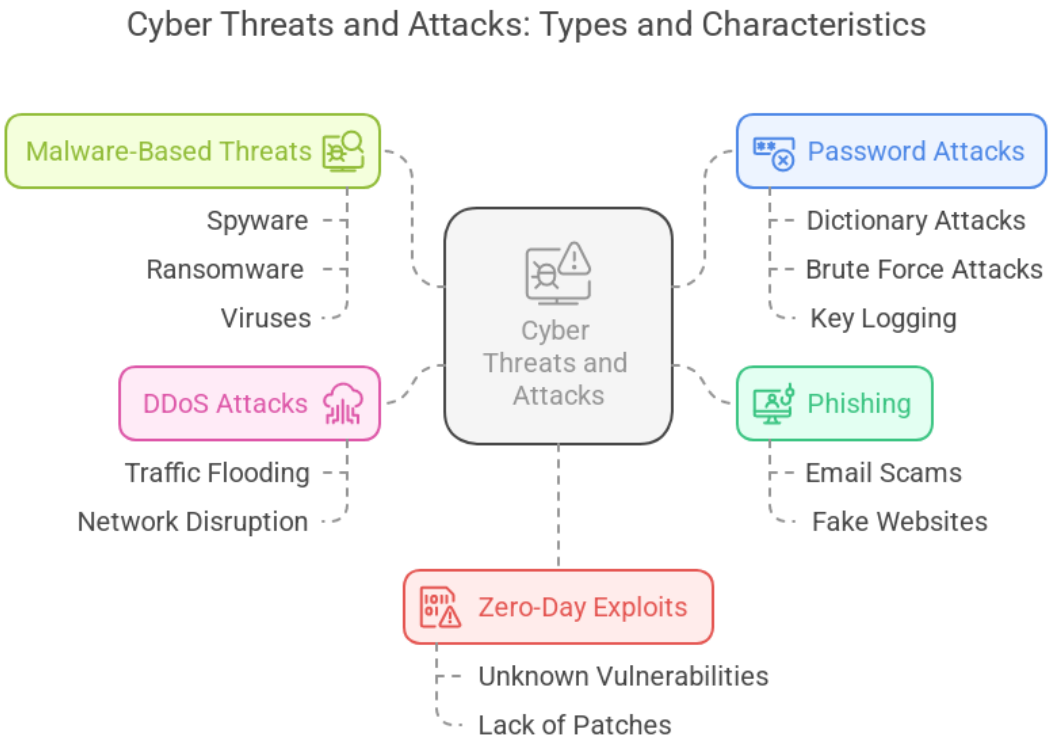


Figure 3.2: Cyber Threats and Attacks

Source: Created by the Researcher

2.8 Concept of Cybersecurity Awareness

According to Zaidi et al., (2020), cybersecurity refers to the creation of methods to safeguard computers, networks, smart devices, and data from harm or illegal access, such as to meet the fundamental security objectives of availability, confidentiality, and integrity. Nowadays, network security and cybersecurity remain top concerns for computer workers. Damingo et al., (2024) indicated that cyber security is concerned with avoiding illegal use, intrusions, sabotage, and natural disasters from affecting information, hardware, and software on the internet. Because computer systems and data can be utilized against them in many ways, cyber security is a rapidly

developing field. Bank online account details, medical or financial information, and personal pictures are some of the information that may require cyber protection

2.9 Importance of Cybersecurity Awareness

According to Nair (2024), the significance of cybersecurity awareness can be summarized in the following table:

Table 2.2: Significance of Cybersecurity Awareness

Key Point	Explanation
Protection against Cyber Threats	Cybersecurity training equips individuals with knowledge and skills to identify and respond to cyber threats such as malware, phishing, ransomware, and other cyberattacks. It also helps individuals understand tactics used by cybercriminals.
Data Security	Training emphasizes securing sensitive data, including data encryption, secure transmission methods, and data access controls. It helps prevent data breaches and unauthorized access to confidential information.
Risk Management	Understanding risks allows individuals and organizations to assess and manage threats effectively. Training covers risk assessment and management strategies to help organizations implement proactive measures to mitigate potential cyber incidents.
Compliance and Regulations	Training ensures individuals and organizations comply with industry regulations and requirements. It helps foster a culture of compliance, reducing legal and financial risks from non-compliance.

Incident Response and Recovery	Training prepares individuals to respond to cyber incidents efficiently. It covers containment, eradication, and recovery processes, minimizing the impact of attacks.
Employee Awareness	Employees become the first line of defence through training. It increases awareness of risks, helps employees recognize and report suspicious activities, and fosters a cybersecurity-conscious culture.
Protection of Critical Infrastructure	Critical infrastructure (power grids, communication networks, healthcare systems) relies on digital technology. Cybersecurity training is essential to protect these critical assets from threats with severe consequences.
Continuous Learning	Cybersecurity is constantly evolving. Regular training keeps professionals updated with the latest threats, technologies, and best practices.
Global Security	Cyber threats cross borders, so a well-trained workforce enhances global security by preventing and responding to cyber incidents with international implications.

2.10 Components of Effective Cybersecurity Awareness Program

Creating an effective cybersecurity awareness program requires the strategic integration of several interrelated components designed to foster a culture of security consciousness across all organizational levels. The core objective of such programs is to influence the behavior of employees by equipping them with the knowledge, skills, and attitudes necessary to prevent and respond to cyber threats. According to Parsons et al. (2017), continuous training and education

are foundational. In today's dynamic cyber landscape, new threats emerge regularly, including sophisticated phishing schemes, ransomware attacks, and social engineering techniques. Without regular updates, employee knowledge can become obsolete, making the organization vulnerable. Continuous training, often delivered through workshops, e-learning modules, and microlearning content, helps maintain high levels of vigilance among employees and ensures that security practices remain fresh in their minds.

Another vital component is executive leadership and support. Cybersecurity cannot thrive in isolation; it must be embedded within the strategic priorities of the organization. Tawiah et al. (2021) stress that executive endorsement signals to employees that cybersecurity is a shared responsibility, not just an IT department issue. When leaders actively participate in awareness campaigns and model secure behavior, they set a tone from the top that encourages compliance and accountability. Periodic testing and simulation exercises are also crucial in gauging the real-world effectiveness of awareness initiatives. Simulated phishing attacks, for instance, provide a controlled environment where employees can demonstrate their ability to recognize and respond to malicious emails without actual risk. Alshaikh (2020) emphasizes that such exercises can reveal gaps in employee knowledge, offering valuable data to refine future training efforts. Likewise, penetration testing and red teaming can uncover systemic vulnerabilities and provide insight into how employees interact with security protocols under pressure.

One size does not fit all in cybersecurity awareness. Tailored content is essential to ensure relevance and engagement. Employees in finance, human resources, and IT face different types of cyber risks and require training suited to their roles. Schinagl and Shahim (2020) found that role-specific training significantly increases retention and behavior change, as employees can directly relate the material to their daily responsibilities. Furthermore, delivering content in

varied formats, videos, infographics, quizzes, and interactive games caters to diverse learning preferences and enhances understanding.

Incorporating real-time feedback mechanisms is another hallmark of effective programs. When employees receive instant feedback on their behaviors such as failing a phishing simulation—they are more likely to internalize lessons and correct future actions. Bada and Nurse (2019) highlight the importance of positive reinforcement, suggesting that rewarding secure behavior (e.g., through recognition or incentives) fosters long-term engagement and establishes cybersecurity as part of organizational identity.

Additionally, integration with onboarding and ongoing HR processes ensures that cybersecurity awareness becomes part of the employee lifecycle. New hires should be introduced to the organization's security protocols from day one, while periodic refresher sessions can reinforce expectations and accommodate changes in the threat domain. An often-overlooked component is the use of metrics and analytics to measure program effectiveness. Organizations need key performance indicators (KPIs) such as phishing simulation click rates, quiz scores, incident reporting rates, and training completion levels to assess progress and identify areas for improvement. As noted by Uchendu et al. (2021), data-driven programs can adapt over time and allocate resources where they are most needed.

Finally, programs should be embedded into organizational culture. A culture that prioritizes cybersecurity integrates secure behavior into everyday workflows, rather than treating it as an afterthought. This cultural integration can be supported by storytelling, gamification, leadership communication, and employee-driven initiatives. Organizations like SoSafe Awareness (2025) advocate gamification to maintain interest, turning security training into an engaging and rewarding experience rather than a routine obligation. In summary, effective cybersecurity

awareness programs are dynamic, inclusive, and aligned with organizational objectives. They must combine leadership support, continuous education, contextual relevance, testing, feedback, and cultural integration to foster sustainable behavior change.

2.11 Cybersecurity Awareness and Asset Protection

Cybersecurity awareness plays a critical role in protecting an organization's assets—both tangible (e.g., devices, systems) and intangible (e.g., intellectual property, customer data, reputation). In the digital age, the value of intangible assets has surged, with data often being more valuable than physical assets. As a result, human behavior becomes a frontline defense mechanism, and awareness becomes a strategic imperative. Alshaikh (2020) argues that the essence of cybersecurity awareness lies in educating employees to recognize and respond appropriately to cyber threats. Whether it's avoiding phishing emails, using strong passwords, or following correct procedures when accessing confidential information, well-informed employees are far less likely to inadvertently expose the organization to risk. Awareness initiatives must therefore go beyond basic training and evolve into behavior modification strategies aimed at habitual secure practices.

The importance of cybersecurity awareness transcends technical departments. As Hadlington (2018) points out, many cyber incidents are initiated not through sophisticated hacking, but through human errors such as clicking on a malicious link or sending sensitive data to the wrong recipient. For this reason, awareness must be organization wide. From executives to administrative staff, everyone should understand their role in protecting assets and adhering to organizational policies. Furthermore, asset protection involves understanding the classification and value of different assets and making employees aware of how their behavior can affect those assets. For example, customer records, financial documents, and internal communications each

require varying levels of confidentiality and protection. When employees understand the business impact of asset compromise, they are more likely to adopt secure behaviors. This aligns with Protection Motivation Theory (Rogers, 1975), which suggests that perceived severity and vulnerability influence individuals' motivation to engage in protective behaviors.

Incorporating cybersecurity awareness into asset management processes is also beneficial. Awareness efforts can be integrated with data governance, access control policies, and asset inventories to ensure a unified approach to security. When employees understand which assets are most critical and how to handle them, organizations are better equipped to enforce controls and mitigate risk. Leadership again plays a pivotal role. When executives prioritize asset protection and invest in cybersecurity education, they model the importance of safeguarding resources. Additionally, creating clear accountability mechanisms such as incident reporting protocols and user access tracking reinforces the message that protecting assets is everyone's responsibility.

Asset protection also relies on the psychological ownership employees feel toward the organization. According to Burns et al. (2019), when employees feel personally responsible for their organization's wellbeing, they are more likely to take proactive steps to prevent cyber incidents. Awareness programs that cultivate this ownership by demonstrating the real-world consequences of poor security and recognizing good behavior can be highly effective. From a regulatory standpoint, many industries require formalized awareness training as part of compliance frameworks such as GDPR, HIPAA, and ISO/IEC 27001. In this context, cybersecurity awareness becomes not only a protective mechanism but also a legal obligation tied directly to organizational governance and risk management.

In summary, cybersecurity awareness and asset protection are deeply interconnected. Awareness informs employees of their responsibilities, while asset protection strategies provide the context and structure needed for those responsibilities to be fulfilled. Together, they create a dual-layered approach that protects organizations from both internal and external threats.

2.12 Challenges of Cybersecurity Awareness

Despite its critical importance, implementing a successful cybersecurity awareness program comes with numerous challenges. These challenges are often multifaceted, involving behavioral, cultural, organizational, and technical factors. One of the most significant challenges is the lack of integration into organizational culture. According to Alshaikh (2020), many organizations treat awareness programs as periodic compliance exercises rather than as strategic imperatives. This approach results in superficial training that lacks depth and continuity. When cybersecurity is not woven into the everyday culture, employees may not internalize its importance, leading to risky behaviors and apathy.

Another challenge is employee engagement and motivation. Security training is often perceived as dull, irrelevant, or overly technical, leading to low participation rates and poor retention. Bada and Sasse (2019) emphasize the gap between knowledge and behavior, employees may know what secure practices are but fail to implement them. This "intention-action" gap is influenced by factors such as lack of reinforcement, organizational indifference, or perceived inconvenience. A third major challenge is the one-size-fits-all approach. Organizations frequently deliver the same content to all employees regardless of their job function, technical aptitude, or risk exposure. This results in low relevance and even resentment among employees who feel that the training does not address their needs. Tailored awareness initiatives, based on role, department, and security responsibilities, are far more effective but require additional resources and planning.

Additionally, overloading employees with information, particularly technical jargon, can lead to cognitive fatigue and disengagement. As Bada and Nurse (2019) note, the overuse of acronyms, complex diagrams, and hypothetical scenarios can make content difficult to digest, especially for non-technical staff. Instead, awareness programs should aim for clarity, simplicity, and practical examples grounded in real-world scenarios. Social engineering threats present a particularly difficult challenge. Phishing, baiting, and pretexting attacks exploit human psychology, often bypassing technical defenses. Because these attacks leverage trust, urgency, and emotion, they are harder to counter with traditional awareness content. Training programs must therefore include psychological elements such as role-play, gamification, or scenario-based simulations to prepare employees for manipulative tactics.

Another obstacle is the absence of leadership involvement. Without visible support from senior management, awareness programs may be perceived as optional or unimportant. Furthermore, if leadership fails to follow security protocols themselves, it undermines the program's credibility and effectiveness. A security-conscious culture starts from the top. Measurement is also a persistent challenge. Many organizations struggle to assess the effectiveness of their awareness programs. Metrics such as training completion rates or phishing test failures provide some insight, but they do not necessarily capture behavioral change or risk reduction. Uchendu et al. (2021) argue that more nuanced, long-term metrics like reductions in incident response time, increase in security incident reports, or improved password hygiene are needed to assess real impact.

Finally, the constantly evolving threat landscape requires organizations to keep pace with new attack vectors and technologies. Static awareness content quickly becomes outdated. For example, the rise of deepfakes and AI-powered phishing requires a new kind of literacy among

employees, one that traditional training modules may not address adequately (Pedersen et al., 2025). Failure to update training content leaves employees vulnerable to emerging threats. In response to these challenges, the best practices include implementing behavioral science principles, multimodal delivery, and continuous improvement loops. Using rewards and nudges, enabling peer learning, and incorporating feedback mechanisms can increase engagement. Furthermore, ongoing leadership involvement and adaptive program designs ensure that awareness remains relevant, effective, and actionable.

In summary, while the challenges of cybersecurity awareness are substantial, they are not insurmountable. Organizations must take a strategic, employee-centered, and evolving approach to ensure that awareness programs lead to meaningful and lasting security behavior change.

2.13 Cybersecurity Technologies and Innovations

The key cybersecurity technologies and innovations are as follows:

1. **Artificial Intelligence (AI) and Machine Learning (ML) :**

AI and ML are being implemented for enhancing threat detection, automating responses to cyber threats, and searching large volumes of data for malicious activity. These technologies help in identifying patterns and predicting potential vulnerabilities in systems**.** (Mustaphaa et al., 2024)**.** Ansari et al., (2022) indicated that the applications of AI in cybersecurity include password protection and authentication, vulnerability management, phishing detection and prevention control, behavioural analytics, and network security.

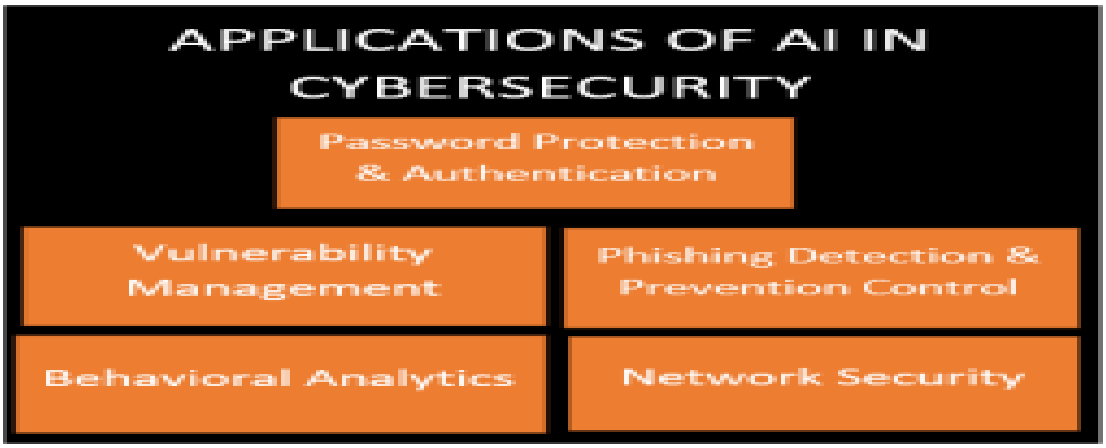


Figure 2.4: Applications of AI in Cybersecurity

Source: (Ansari et al., 2022)

The Role of Artificial Intelligence in Cybersecurity covers several key areas that are significant in enhancing digital security measures across different sectors. They include faster detection, behaviour analysis, phishing attempt detection, secure authentication, and network integrity protection (Jonas et al., 2023).



Figure 2.5: Significance of AI in Cybersecurity

Source: (Jonas et al., 2023)

2. Blockchain Technology:

Blockchain is also being utilized in identity and personal data protection, supply chains becoming more transparent, and transaction integrity is being improved. Since it's decentralized, it's a very robust tampering and fraud prevention solution (Mustaphaa et al., 2024). Blockchain technology keeps developing and discovering new applications in the contemporary environment. It has been researched and used in several promising fields, including cybersecurity. The Blockchain architecture makes it quite feasible to solve the current security issues in domains like networks, IoT devices, and data storage and transmission. Blockchain protects data during storage and transmission by using encrypted blocks that are difficult to manipulate and can only be accessed by the parties involved (Mathew, 2019).

3. Cloud Security Technologies

Cloud security technologies entail the use of technologies such as encryption, tokenization, and single sign-on technologies in order to provide security to data held in public and hybrid clouds. Such practices help secure sensitive information against unauthorized access (Mustaphaa et al., 2024)**.**

4. Threat Intelligence:

It is the method of gathering and breaking down data from various sources for the purposes of predicting and responding to recognized as well as unseen threats. Threat intelligence is situated at the nucleus of modern-day cybersecurity practice because it embodies futuristic thinking (Mustaphaa et al., 2024). The dissemination of fact-driven reports on actualized or probable dangers is termed as a threat intelligence. Increased security functions, effectiveness and productivity in investigative as well as precautionary powers are some advantages associated with threat intelligence. A repository of knowledge of threat information and an expressive way of

presenting this data is essential for effective threat intelligence in cyber space. Ontologies, taxonomies, and sharing standards are used to achieve this (Mavroeidis, & Bromander, 2017).

5. Governance, Risk Management, and Compliance (GRC) Frameworks:

There should be strong GRC foundations to deal with cybersecurity threats and regulations like GDPR and CCPA. These include clear roles and responsibility, regular audits, and adherence to industry standards (Mustaphaa et al., 2024). Governance, risk, and compliance (GRC) workflows can be used in cybersecurity to protect data and systems from security and integrity threats. Organizations must adopt sophisticated technology to drive their GRC processes because more advanced cyber-attacks are emerging. Efficient Governance, Risk, and Compliance (GRC) processes were created in response to such threats' emergence. With methods, processes, and guidelines by which companies govern their IT infrastructure, GRC practices reduce the risk and bring regulatory compliance. It is easy for organizations to manage cybersecurity for digital assets through the issuance of well-delineated roles and responsibilities and having specific governance frameworks. Organizations can become aware of cybersecurity threats and compliance obligations using robust GRC processes (Urhobo, 2024).



Figure 2.6: Framework of Governance, Risk, and Compliance Practices (GRC)

Source: (Urhobo, 2024).

6. **Emerging Technologies:**

There are upcoming technologies such as quantum computing and the security concerns it presents, along with the need to manage vulnerabilities surrounding the Internet of Things (IoT) and deepfakes (Mustaphaa et al., 2024).

2.14 Cybersecurity Best Practices

Cybersecurity behavioral best practices seek to shape the public into having safer online habits through easy guidance and expert advice. Certain practices include having good passwords and securing them, possessing and maintaining anti-virus systems and firewalls, and always using up-to-date software. They also point to the necessity of logging off websites once they have been used, shutting down computers, and using only secure and trusted connections, computers, devices, websites, and services. Having knowledge of risks, avoiding scams and phishing attempts, providing only the bare minimum of personal information, and protecting one's identity is also essential. Besides this, people are called upon to be sensitive to their physical surroundings online and report cybercrime and cybercriminals to the authorities (Coventry et al., 2014). Also, according to (Mahato et al., 2024) the methods for preventing cyber threats are as follows:

1. **Create strong, one-of-a-kind passwords always:** not using the same one for many websites. Creating a complex password for each account and employing tools that can generate and store passwords to aid in the process.
2. **Keep Software Current and Available:** Update the operating system, applications, and antivirus software with the latest security patches and vulnerability protection.
3. **Data Backup:** Developing a regular backup routine for all the important documents and data. Having secure and easily retrievable backups in the event of data loss or ransomware by backing them up offline or on cloud storage.

4. **Using Secure Wi-Fi:** Joining password-protected, encrypted networks, such as WPA2 or WPA3. Refraining from using unprotected public Wi-Fi networks to access private data or carry out financial activities.

Moreover, the best cybersecurity practices according to the Cybersecurity and Infrastructure Security Agency (2024), are as follows:

Table 2.3: Cybersecurity Best Practices

Cybersecurity Best Practice	Description
Use Strong Passwords	Use Strong Passwords and change them periodically.
Back-Up Data	Protecting Sensitive and Personal Information
Implement Multifactor Authentication (MFA)	Turn on MFA
Engage in Collaboration & Information Sharing	Joint Cyber Defense Collaborative
Regularly Update	Use CISA Free Cybersecurity Services & Tools

Firmware & Software	
Segment the Network	Manage Network Security Through Segmentation
User Education and Training	Recognize and Report Phishing
Institute Role-Based Access Control	Information Sharing Architecture (ISA) Access Control Specification (ACS)
Utilize Encryption	Converting data into a secure format that can only be read by authorized individuals or systems.

2.15 Strategies for Improving Cybersecurity Awareness

Cybersecurity awareness is a cornerstone of organizational and national digital resilience. As cyber threats grow in complexity and frequency, improving awareness across all user levels becomes essential. Hörnemann et al. (2024) present several strategic formats for enhancing cybersecurity understanding and behavior change, ranging from interactive live events to self-paced digital learning. These strategies are essential in bridging the knowledge-behavior gap and cultivating a proactive security culture.

2.15.1 Live Hacking Demonstrations

Live hacking events are dynamic, attention-grabbing experiences where ethical hackers perform simulated cyberattacks on stage. The goal is to demonstrate, in real time, how

vulnerabilities can be exploited and how users can prevent such breaches. These sessions typically last between 30 to 90 minutes and are designed to engage both technical and non-technical audiences.

Live hacking has proven effective in generating emotional responses such as shock or urgency, which can be powerful motivators for behavior change. Participants witness the speed and simplicity with which attackers can bypass poorly configured systems, guess weak passwords, or exploit unpatched software. For instance, a live demo might include an attacker stealing login credentials using a phishing link or gaining access to a mobile device using public Wi-Fi.

This method is particularly impactful in corporate environments, executive briefings, or public awareness campaigns. It fosters empathy for cybersecurity professionals and translates abstract risks into tangible experiences. Importantly, live hacking must be followed by guidance on how to prevent the attacks shown, ensuring that awareness translates into action.

2.15.2 Phishing Campaign Simulations

Phishing remains one of the most common attack vectors, responsible for many high-profile breaches. A phishing simulation campaign is a controlled test wherein realistic phishing emails are sent to employees without prior notice. The objective is to evaluate who clicks on malicious links, enters credentials, or reports suspicious messages. These campaigns provide valuable data on organizational risk posture. Security teams can assess which departments or user demographics are most vulnerable, what types of phishing messages are most effective, and how quickly users respond to potential threats. Insights gained can be used to tailor subsequent training or reinforce specific policies.

Moreover, phishing simulations introduces the concept of learning by doing, a principle that helps users internalize security lessons more effectively than theoretical instruction. After the exercise,

debriefing sessions or individual feedback reports help users understand what they did right or wrong. This non-punitive approach promotes a culture of learning rather than blame.

Organizations such as Google and IBM have reported significant reductions in phishing susceptibility following repeated simulation training. Importantly, phishing campaigns must evolve constantly, incorporating new tactics like voice phishing (vishing) or QR-code phishing, to remain relevant against evolving threats.

2.15.3 Seminars, Workshops, and Certification Courses

Seminars, workshops, and multi-day courses form the foundation of traditional cybersecurity education. These in-depth sessions are ideal for building technical and behavioral competencies among staff, IT professionals, and organizational leaders. A workshop format, with 15 to 30 participants, allows for interactive learning through case studies, role-playing scenarios, and collaborative problem-solving. It also facilitates peer learning—participants share real-life incidents, successful practices, and personal strategies, thereby enriching the learning environment. Workshops often culminate in certifications, which serve both as incentives for participation and as indicators of proficiency. For example, programs like Certified Information Systems Security Professional (CISSP) or Certified Ethical Hacker (CEH) offer internationally recognized credentials that enhance career mobility and organizational trust.

In the UAE, workshops tailored to specific industries like healthcare data security or financial transaction protection are increasingly common. These address sector-specific risks and compliance requirements (e.g., GDPR, HIPAA, or Central Bank cybersecurity frameworks). Workshops also prepare organizations to meet audit and regulatory expectations by embedding best practices into operations.

2.15.4 E-Learning Platforms and Microlearning Modules

E-learning provides scalable, cost-effective, and flexible training opportunities for geographically dispersed teams. These platforms typically offer short, engaging modules on topics such as password management, recognizing phishing, safe browsing, and mobile device security. Lessons are often accompanied by videos, animations, and quizzes to reinforce learning. Microlearning, the delivery of content in small, focused chunks has emerged as an effective technique for sustaining attention and improving retention. Learners can engage with content at their own pace, repeat modules, and apply knowledge immediately. Platforms such as Cybereclipse (2024) advocate microlearning as a tool for embedding secure behavior into everyday routines.

Gamified e-learning where participants earn badges, level up, or compete on leaderboards adds an element of intrinsic motivation. This is especially effective among younger employees or in competitive work environments. E-learning platforms can also incorporate adaptive learning, where content difficulty adjusts based on user performance. For example, a user who scores poorly on phishing quizzes may be guided toward additional practice or advanced materials. Critically, e-learning content should be updated regularly to reflect new threats and compliance standards. Customization for specific roles (e.g., HR, Finance, IT) increases relevance and applicability, aligning with best practices for behavior-based cybersecurity training.

2.15.5 Combining Methods for Maximum Impact

A single method rarely achieves sustained awareness and behavior change. Thus, an integrated approach combining live events, simulations, workshops, and digital content often proves most effective. For example, an organization might launch a live hacking demo, follow up with phishing simulations, and then enroll staff in a six-week e-learning program supplemented by workshops.

Additionally, regular communications such as newsletters, posters, and internal social media posts keep cybersecurity top of mind. Feedback mechanisms such as surveys, knowledge checks, and incident reports allow organizations to continuously improve their training strategy.

Ultimately, improving cybersecurity awareness is not a one-time event but an ongoing cultural transformation. Organizations that embed cybersecurity into daily operations, leadership behavior, and employee expectations are best positioned to defend against ever-evolving threats.

2.16 Prevalent Cyber Threats in the UAE

The United Arab Emirates (UAE) has emerged as a regional digital and economic hub, driven by aggressive digital transformation initiatives and widespread technology adoption. With over 85% of the population online and smart government programs advancing rapidly, the country faces both exceptional opportunities and significant cybersecurity risks. As digital infrastructure deepens, cybercriminals, hacktivists, and state-sponsored actors increasingly target the UAE, making cyber threats a central issue in national and organizational risk management.

2.16.1 Current Threat Domain

According to Alalawi (2024), the UAE experienced a 71% increase in cyberattacks in 2021 compared to the previous year. Organizations face an average of 925 attacks per week, with 1.1 million phishing attempts recorded during the same period. The financial and reputational damage from these attacks is severe particularly in sectors like banking, telecommunications, and government services.

1. Identity Theft in the Banking Sector

Identity theft is a major concern, especially in the UAE's robust financial services sector. Cybercriminals employ phishing emails, fake login pages, and mobile app clones to steal banking

credentials. With mobile banking and fintech platforms gaining popularity, attackers exploit vulnerabilities in user behavior and device security to access sensitive financial data. The consequences include not just financial loss for customers but also regulatory fines for institutions under data protection laws such as the UAE's Personal Data Protection Law (PDPL). Reputation damage and loss of customer trust often exceed the immediate monetary impact.

2. Ransomware Attacks

Ransomware has emerged as one of the most disruptive cyber threats in the UAE. In 2021, 59% of organizations were affected by ransomware, with an average ransom payment of $225,338. The cost of remediation—including data recovery, incident investigation, and operational disruption—reached $1.26 million per incident, representing a 144% increase from 2020. These attacks often exploit weak email filters, poor endpoint protection, and unpatched vulnerabilities. Critical infrastructure, including hospitals and transportation systems, are particularly vulnerable due to legacy systems and the essential nature of their services.

3. Sector-Wide Impacts

Cyberattacks in the UAE are not confined to one industry. Several key sectors have been repeatedly targeted:

- Government: Attacks aim to disrupt services or leak sensitive citizen data. State-sponsored actors often seek political leverage through cyber espionage.
- Energy: As a major oil producer, the UAE faces threats to SCADA (Supervisory Control and Data Acquisition) systems. Malware targeting industrial control systems could cause catastrophic damage.
- Education: With the rise of e-learning, schools and universities have become targets of data theft, ransomware, and account hijacking.

- Healthcare: Hospitals face phishing attacks, ransomware, and data breaches. Patient records are highly valuable on the dark web.
- Telecommunications: Telcos are frequent targets due to their control over communications infrastructure and customer metadata.

4. AI-Powered Attacks and Deepfakes

The UAE has also witnessed an increase in AI-enhanced attacks. AI is used to craft convincing phishing lures, automate password guessing, and even generate deepfakes fake audio or video used to impersonate individuals in social engineering schemes. Executives and public officials are particularly vulnerable, as impersonation can be used for fraud, blackmail, or misinformation.

5. Advanced Persistent Threats (APTs)

APTs are highly sophisticated, prolonged attacks often attributed to nation-state actors. They typically involve multiple stages, including reconnaissance, exploitation, lateral movement, and data exfiltration. APTs target critical infrastructure, government databases, and research institutions. The use of AI and zero-day vulnerabilities makes detection extremely difficult.

6. Misconfiguration and Unpatched Systems

Around 32% of security incidents in the UAE arise from misconfigured systems, incorrect access controls, exposed databases, or poorly implemented security settings. Over 223,800 digital assets were found to be publicly exposed due to misconfigurations or outdated software, with some vulnerabilities left unaddressed for more than five years. This is particularly problematic in cloud environments where default configurations are not adequately secured. Attackers often scan for such weaknesses using automated tools.

7. Drive-by Downloads and Web Compromises

Drive-by downloads occur when a user visits a compromised website, triggering automatic malware installation without any user interaction. These types of attacks have grown in prevalence in the UAE, often targeting social media users, e-commerce platforms, or news sites.

Similarly, web server compromises involve attackers exploiting vulnerable websites to inject malicious scripts or use the server as a botnet command center.

8. Economic Impact and Global Ranking

The Middle East, including the UAE, has one of the highest average costs of data breaches globally. The financial services and oil and gas industries are seen as lucrative targets by organized cybercrime groups. The economic damage, when factoring in loss of revenue, regulatory penalties, and customer churn, runs into billions of dollars annually.

According to Emirates news agency- WAM (2025), the prevalent cyber threats in the UAE comprise:

Table 2.4: Common Cyber Threats in the UAE

Cyber Threat	Description
Exposed Assets and Unpatched Vulnerabilities	Over 223,800 assets in the UAE are potentially exposed to cyber-attacks, with critical vulnerabilities left unaddressed for over five years.
Misconfiguration (32% of Incidents)	Incorrect system settings remain a major cause of security breaches.
Improper Usage and Unlawful	Includes insider threats, unauthorized access, and policy violations.

Activity (19% of Incidents)	
Drive-By Downloads	A common initial entry method where malware is installed when users visit compromised websites.
Phishing and Web Server Compromises	Attackers use advanced AI-driven phishing lures and exploit web vulnerabilities to gain access.
AI-Powered Social Engineering and Deepfake Technology	Cybercriminals leverage AI to enhance phishing attacks and impersonate individuals using deepfakes.
Ransomware Attacks	There has been a 58% increase in ransomware groups operating in the UAE.
Advanced Persistent Threats (APTs) and State-Sponsored Attacks	Nation-state actors are integrating AI into their attack frameworks, posing significant risks.
Economic Cybercrime	The UAE and the Middle East have the second-highest data breach costs globally, making them lucrative targets for cybercriminals.

Declining but Still Present DDoS Attacks	While DDoS attacks dropped from 58,538 to 2,301 between 2023 and 2024, they remain a concern.

In summary, the UAE's position as a digital innovator has made it a magnet for cyber threats. With increasing adoption of cloud computing, AI, and smart infrastructure, the attack surface continues to expand. Addressing these challenges requires a multi-layered approach—robust infrastructure, updated laws, real-time threat intelligence, and above all, a well-informed public. As cyber threats grow in sophistication, cybersecurity awareness and cross-sectoral cooperation will be critical in safeguarding the UAE's digital future.

2.17 Current State of Cybersecurity Awareness in the UAE

In the current interconnected world, individuals, public institutions, private corporations, and governments are exposed to ever-evolving cyber-attacks and threats, necessitating that people and organizations learn about cybersecurity fully. Cyberattacks have impacted numerous countries and infrastructures in several industries across the world, such as the United Arab Emirates (UAE), which has become a major target for cybercrime due to its booming economy and tourism. The UAE considers cybersecurity an increasingly important issue in our digital world and raising awareness of cybersecurity among residents is essential to protect themselves and their organizations against cyberattacks (Alalawi, 2024).

The state of cybersecurity awareness in the UAE, according to the State of the UAE Cybersecurity Report (2025), highlights some of the following points:

1. Recognition of Cybersecurity's Importance: The UAE recognizes cybersecurity as essential to national security and economic stability, and thus, strategic measures are being undertaken to strengthen cyber resilience.
2. Proactive Government Initiatives: The government has undertaken comprehensive plans, such as the National Cybersecurity Strategy, encompassing public awareness and education of citizens and businesses regarding potential cyber threats, particularly concerning new technologies such as AI.
3. New Technologies and Threats: Businesses adopting new technologies such as AI are faced with a changing threat landscape since malicious actors are also adopting these technologies, highlighting the need for greater awareness and preparedness.
4. Public-Private Partnership: Dynamic public-private partnership for cybersecurity awareness and defence mechanism is facilitated by integration with the National Cyber Security Operations Center (NSOC) for threat intelligence sharing.
5. Evolving Cyber Threats: Despite progress, the report identifies an increase in cyber threats, such as DDoS attacks and ransomware attacks, indicating an imperative need for ongoing education and training to recognize and avert such occurrences.
6. Educational Initiatives and Governance: AI governance policy formulation and compliance with regulation are essential in propelling the ethical application of AI and stakeholder education.
7. Employee Awareness: Emphasizing the personality of an educated workforce, employees are encouraged to take preventive measures and train themselves in a bid to avert cyber-attacks.

2.18 Current Cybersecurity Policies and Strategies in the UAE

According to the United Arab Emirates' Government portal (2025), the UAE's National Cybersecurity Strategy, launched in 2019 by the Telecommunications and Digital Government Regulatory Authority (TDRA), aims to establish a secure cyberinfrastructure for the benefit of citizens and businesses. The strategy is based on five pillars and includes 60 initiatives that will propel the growth of the UAE's cybersecurity ecosystem. The execution of the strategy will be monitored by the TDRA using several governance frameworks and performance metrics. The strategy will be in force for three years, with the possibility of amendment based on future cybersecurity requirements and expert advice. Some of the main points of the strategy are:

1. Legal and Regulatory Framework: Developing comprehensive legislation to regulate cybercrimes, secure technologies, and safeguard SMEs against cyberattacks.
2. Cybersecurity Ecosystem Development: Growing the UAE AED 1.8 billion cybersecurity sector, for example, training over 40,000 professionals, fostering careers and national awareness in cybersecurity.
3. National Cyber Incident Response Plan: Creating a shared response plan for cyber incidents with detection, reporting, and evaluation procedures.
4. Protecting Critical Assets: Identifying nine priority sectors such as energy, finance, and health to secure critical infrastructure.
5. Ecosystem Mobilization: Enabling coordination between the private and public sectors, academe, and international partners for the achievement of cybersecurity goals.

2.19 Recommendations for Strengthening Cybersecurity Awareness in the UAE

The past years brought significant advancements to the UAE in developing its digital infrastructure along with accelerating digital transformation throughout different industrial sectors. Higher dependence on technology demands higher attention from society as well as organizations and government agencies about cyber threats alongside defensive measures for digital assets. National defense alongside sensitive data protection and public service trust depends on an active cybersecurity culture which has become mandatory for every citizen and organization. The following recommendations aim to boost the current efforts of cybersecurity awareness throughout the UAE to develop a resilient digital community that stays ahead of cyber threats.

1. A widespread national education initiative should exist to teach people and organizations about changing online security threats while instructing them how to use the internet safely. Multiple campaigns must use basic language with compelling content as well as interactive media and formats to reach different audiences effectively.
2. The school curriculum must integrate cybersecurity education to establish awareness throughout students' academic careers. This strategy enables education about online asset protections and information security to all new generations early in development.
3. The government along with private sector industries and educational centers should unite through Public-Private Partnership programs to establish collaborative security awareness plans and trade information sharing systems and field-oriented training activities.
4. The implementation of training programs specific to each sector needs to provide solutions to combat threats unique to finance systems as well as healthcare companies and critical infrastructure groups. This way professionals can learn how to fight these specific sector threats.

5. Nudge Cyber Hygiene Behaviors: Emphasize the importance of basic cyber hygiene, such as strong password security, regular software updates, and safe handling of emails and attachments. Multiple platforms need to consistently present these behaviors to strengthen their implementations.
6. Offer award programs that lead people and organizations to join cybersecurity awareness programs and implement best cybersecurity standards.
7. The implementation of continuous assessment and ongoing improvements requires organizations to develop permanent mechanisms which should review campaign effectiveness, collect feedback from participants and adapt their security strategies to emerging threats and modern technological developments.

2.20 Underpinning theories

Protection Motivation Theory: Sulaiman et al., (2023) discuss the application of Protection Motivation Theory (PMT) to cybersecurity awareness. PMT is a theory that explains individuals' appraisal of threats and decisions regarding protective behaviours in terms of two general factors: threat appraisal and coping appraisal.

1. The analysis of threats includes perception of both severity and ability to fall victim to cybersecurity threats which drive protective action motivation.
2. The final evaluation stage involving security measures depends on response efficacy combined with self-efficacy and the apparent costs of security measures to decide

protective action outcomes.

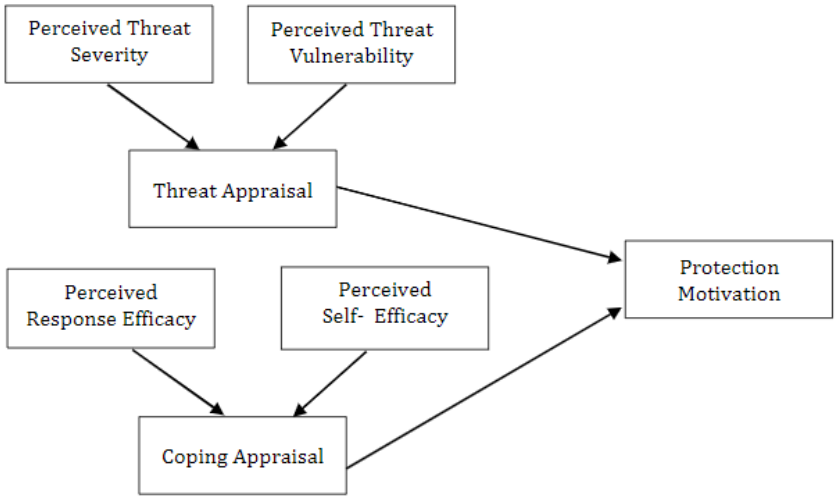


Figure 2.7: Protection Motivation Theory

Source: (Sulaiman et al., 2023)

Technology Acceptance Model: The Technology Acceptance Model, or TAM, may be employed as one of the core theory models for the explanation and prediction of acceptance and adoption of emerging technologies (Hossain et al., 2024).

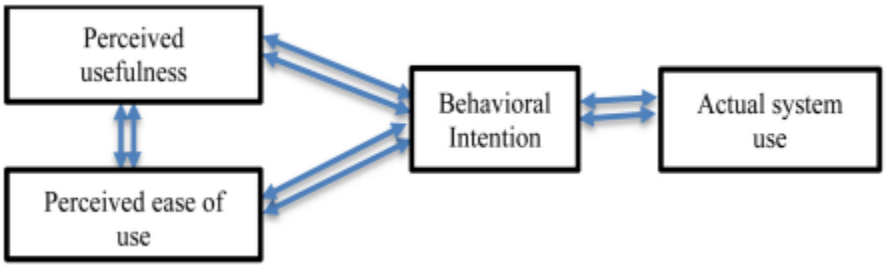


Figure 2.8: Technology Acceptance Model

Source: (Hossain et al., 2024).

The figure described by Fallatah (2024) depicts the elements that influence training program adoption in cybersecurity through technology acceptance models such as TAM and

UTAUT. The model relies on both perceived usefulness along with perceived ease of use to influence users' decisions toward adopting training programs. The perception of training benefits among individuals results from several determining factors that include system complexity along with image and social presence and perceived quality level. The combination of individual self-belief with social influences and operational factors determines how easy users find training to use which determines their training engagement. The model analyzes the effects of regulatory control together with psychological aspects that influence the decision process to adopt training. The strength of behavioral intention depends on experience combined with innovative activities until users make their adoption choice. Playfulness and end-user support together with anxiety emerge as new research topics according to the figure but this presentation additionally discusses usability issues and external control perception as obstacles to acceptance of training systems.

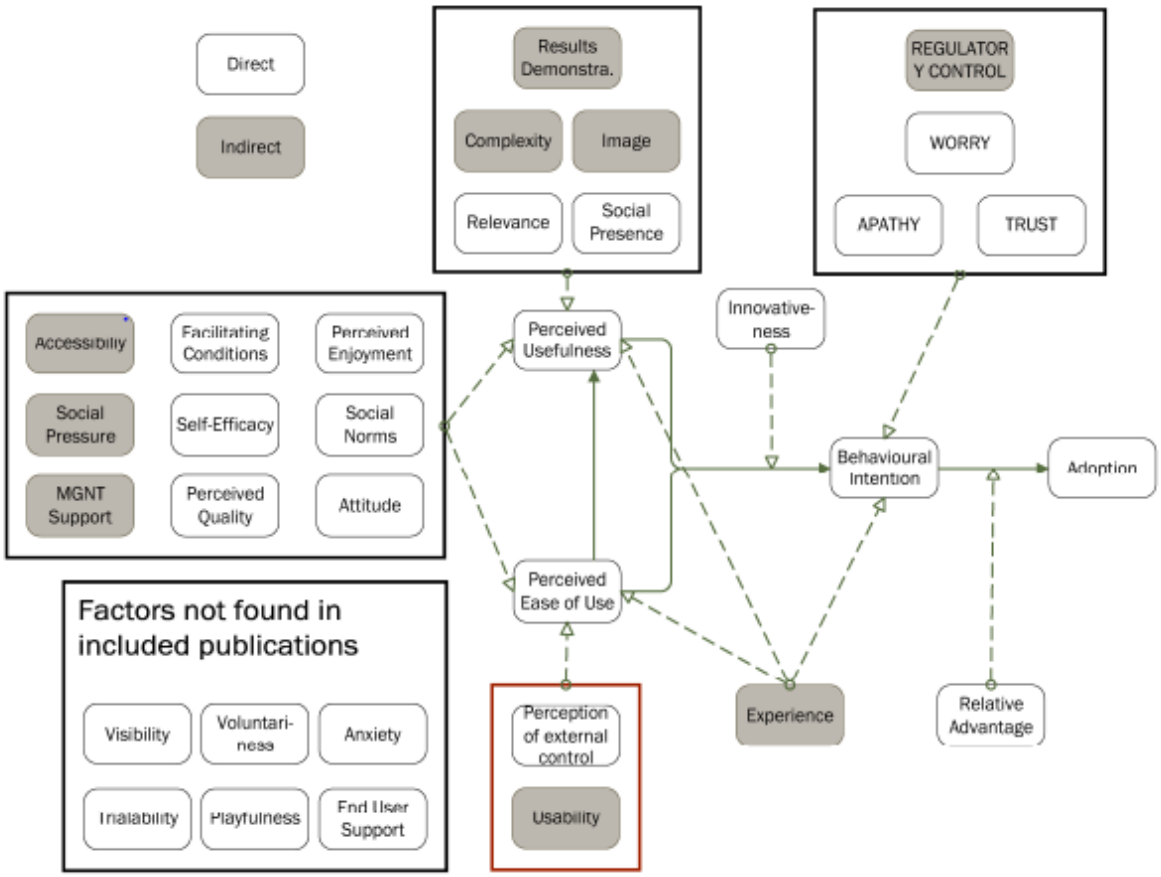


Figure 2.9: Conceptual Model for Cybersecurity Training Acceptance (CTAM)

Source: (Fallatah, 2024)

Theory of Planned Behavior: Cybersecurity procedures and policies are typical countermeasures used to protect organizations from cybercrimes and security violations. Without human actions being considered, the countermeasures will be useless. Cybersecurity behaviour has gained much attention in recent years (Almansoori et al., 2023)

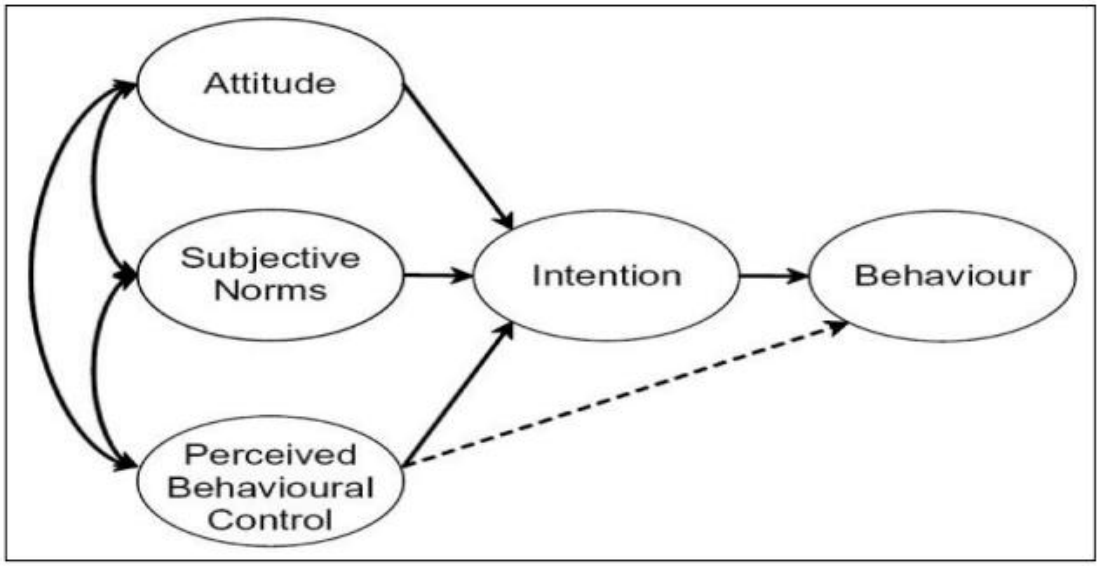


Figure 2.10: Theory of Planned Behavior

Source: (Apau & Koranteng, 2019)

Based on the above, it can be concluded that The Theory of Planned Behavior (TPB) uses intention as the central element to anticipate and describe user cybersecurity actions through its connections between attitudes and norms and perceived control. According to Lombardi et al., (2021) TPB theory receives expansion through integration of Awareness and Context-Based Information showing that customized cybersecurity information enhances user awareness and leads to improved security behaviors. These extensions of TPB enhance the framework to become an efficient tool that aids in understanding cybersecurity behavior while improving its promotion.

In short, multiple security attack types including phishing along with malware and DDoS and password attacks and zero-day exploits constitute the dynamic cybersecurity threat environment. Organizations along with individuals need cybersecurity awareness for identifying threats to effectively combat them. There must be continuous training, tailored material, and executive sponsorship in an effective cybersecurity awareness program addressing the issues of organizational culture and employee behavior. Emerging technologies like AI, blockchain, and

cloud security have become the key contributors to enhancing cybersecurity practices, while best practices of strong password security and software updating are key to protecting confidential information. Cyber-attacks increasingly finding a place in the UAE require an open approach towards developing awareness of cybersecurity through government interventions and public-private partnerships. Widespread campaigns, incorporation into educational curricula, and occupational-specific training have been proposed steps towards enhancing awareness. Theoretical frameworks such as Protection Motivation Theory, Technology Acceptance Model, and Theory of Planned Behavior are helpful in the comprehension and improvement of cybersecurity practices. Generally, creating a culture of cybersecurity awareness is critical in safeguarding digital assets and achieving national security in an increasingly interconnected world.

Third: Empirical Literature Review

This section offers an empirical literature review focusing on research that examines various facets of cybersecurity, primarily organizational resilience, awareness, leadership, and emerging technologies. The review encompasses both general international studies and UAE-specific studies to offer a comparative analysis of the evolution of cybersecurity challenges and solutions in various settings.

Table 2.5: General Studies

Author	Aim	Methodology	Results	Research Gap
Shoumya Singh **&** Deepak Kumar (2024)	The study seeks to explore the role of big	The study employed a comprehensive review of	There is an effective role for big data analysis, as it enables real-	The rising frequency along with the sophistication of

	data analytics in cybersecurity defence and asset protection.	existing literature and case studies.	time monitoring and analysis of network traffic, log files, and user behaviour, allowing instant detection of potential threats, and protecting digital assets from cyber-attacks.	cyber threats that organizations face. Research needs to operate continuously because threats increasingly evolve with new sophistication levels.
Nalini Nadarajah, Rahul Arulkumaran, Amit Mangal, Dr S P Singh, Shalu Jain, and Raghav Agarwal (2024)	The study aims to explore the role of advanced cyber security strategies designed to protect digital assets in a rapidly evolving	The study employed a mixed-methods approach combining quantitative and qualitative methodologies.	The study confirms that there is an important role for modern strategies such as artificial intelligence, multiple authentications, behaviour analytics, continuous	The study points to several research gaps, such as the need to improve the accuracy of AI in detecting threats through integrating deep temporal analytics.

	threat landscape.		training and privacy enhancement technologies to protect digital assets from growing cyber threats. Constant monitoring and immediate response also help minimize potential damage, making organizations better able to adapt and respond to attacks before they significantly affect their digital assets.	
Muhammad Fakhrul	The study aimed to	This research used literature	The most important steps	More studies are needed to explore

Safitra, Muharman Lubis, and Hanif Fakhrurroja (2023)	identify the key factors that shape an organization's cyber resilience against cyberattacks.	review and concept analysis to develop a conceptual framework for the relationship between digital transformation capability and cybersecurity resilience.	that organizations can take to enhance their resilience in the face of cyber threats are to develop effective and proven incident response strategies, implement appropriate preventive measures, increase resilience to emerging threats, and cooperate with external entities to enhance cybersecurity resilience. By considering these	how to effectively integrate digitization capabilities into cybersecurity resilience frameworks.

			measures, organizations can protect themselves from cyber-attacks.	
Santhananthan Gopal Krishnan, Abdulaziz Al-Nahari, Noor Azma Ismail, and Danny Ngo Lung Yao (2023)	The study aimed to investigate the role of cybersecurity awareness among bank employees and its implications for mitigating cybersecurity risks.	The study used the quantitative method and used a survey questionnaire.	There is an effective role for cyber security awareness, as it works to strengthen comprehensive security measures within banks. There is also a positive relationship between cyber security awareness and various factors, such as the level of analysis,	The research highlights an absence of detailed practical approaches and methods which effectively improve the cybersecurity awareness of bank staff within current academic literature.

			implementation of strategies, and the presence of cyber security gaps.	
Halima Ibrahim Kure, Shareeful Islam, Mustansar Ghazanfar, Asad Raza, and Maruf Pasha (2022)	The study seeks to Develop an effective cybersecurity risk management practice for cybersecurity systems by assessing the importance of assets and predicting the types of risks, using fuzzy set theory to assess the importance of	The study used an analytical approach.	The use of fuzzy set theory in assessing asset importance helps stakeholders implement effective risk management practices, also machine learning algorithms have proven highly efficient in predicting various types of risks, including Denial of Service (DoS) attacks, cyber	The study identifies a missing link in machine learning applications for risk type prediction which would improve total risk management efficiency.

	assets, and machine learning algorithms to predict risks.		espionage, and crimeware.	

Table 2.6: UAE Studies				
Author	**Aim**	**Methodology**	**Results**	**Research Gap**
Meera Humaid Alalawi (2024)	The study seeks to Assess the level of cybersecurity awareness among individuals in the UAE.	The study employed a mixed-methods approach combining quantitative and qualitative methodologies.	The study identified gaps in the Ministry of Education's curriculum for Grades 1 to 12 in UAE public schools about cyber threats, highlighting the need for more direct	There is a lack of local studies and applications specifically designed to promote cybersecurity awareness in the UAE.

			and in-depth cyber security education.	
Abdallah Tubaishat and Humaid AlAleeli (2024)	The study aimed to detect the impact of organized and unorganized cybercrimes within the UAE.	The study employed qualitative.	The study showed that cyber-attacks create extensive effects on businesses since every respondent agreed that cybercrimes result in major damage to business brand identity and reputation. The deterioration of reputation	More research is needed about proactive cybersecurity measures and their effectiveness in different organizational contexts.

			results in customer confidence diminishment because organizations are perceived as unable to protect sensitive customer data from theft attempts	
Nabil Hasan Al-Kumaim and Sultan Khalifa Alshamsi (2023)	The study seeks to explore the role of cybersecurity leadership in limiting cyberattacks in financial	The research employed a quantitative method.	There is an effective role for leadership in the field of cybersecurity, as effective leadership is considered an important element for	There is a lack of empirical studies that investigate the organizational factors and the role of leadership in cybersecurity

	organizations in the UAE.		preventing the attempts of cyber-attacks in the cyberspace environment and promoting awareness of cybersecurity within financial institutions and society in the UAE.	awareness in the UAE.
Sayyed G. Maisikeli (2020)	The study aimed to assess the UAE's cybersecurity perceptions and compare them to risks	The study used a survey as a methodology.	The study found that the UAE's level of Relative risk is comparable with those of France and	Research into cyber behavioural patterns requires more attention to explain both the risk-taking

	in other developed countries.		Germany. When it comes to comparing monetary loss due to cybercrime versus relative risk, the UAE is at par with Canada.	behaviours of the local population and how educational initiatives affect this behaviour.
Abdulla Al Neaimi, Tago Ranginya, and Philip Lutaaya (2015)	The study aimed to identify the strategic guidelines for the effective management of cybersecurity threats for UAE	The study employed a comprehensive review of existing literature on existing cybersecurity strategies within the UAE.	Strategic guidelines for cybersecurity were to strengthen the technical, operational and analytical capabilities of all relevant institutions, protect critical	The need for sensitive training and awareness programs on integrating cybersecurity strategies for the UAE context.

	government agencies.		infrastructure and strategic assets, promote and facilitate public-private partnerships to strengthen national property, strengthen cyber security and fully support international cooperation.	

2.21 Comparative Analysis of Existing Studies

A critical analysis of the extant literature reveals a dynamic but often fragmented field, characterized by distinct methodological preferences and thematic focuses. Comparing and contrasting these studies helps to crystallize the areas where the present research offers novel contributions.

2.21.1 Methodological Divide: Quantitative vs. Qualitative Approaches

The literature is primarily dominated by quantitative studies that rely on large-scale surveys to test hypotheses derived from established theories like the Technology Acceptance Model (TAM) or the Theory of Planned Behavior (TPB).

- Quantitative Studies (e.g., Choi & Hwang, 2021): These studies offer strong generalizability regarding the *extent* of awareness or the statistical *correlation* between variables (e.g., training frequency and security incidents). Their strength lies in providing a macro-level view of compliance rates.
- Qualitative Studies (Contrast): In contrast, the few existing qualitative studies focus on depth and context. While lacking statistical power, they excel at uncovering the lived experiences and psychological rationales behind policy non-adherence (Vance et al., 2018). The current thesis aligns with this approach, seeking to understand the *why* of behavioral failure, which quantitative metrics cannot capture.

2.21.2 Thematic Focus: Technical Controls vs. Human Factors

A central contrast exists in the literature's primary focus, which dictates the solutions proposed.

- Technical/Compliance Focus (Prevalent): Much research, particularly in the early 2010s, treated security as a technical problem solvable through mandatory compliance and policy enforcement (Kandukuri et al., 2022). Solutions centered on firewall deployment, patch management, and strict policy documents.

- Behavioral/Cultural Focus (Contrast): More recent and impactful studies, such as those by Vance et al. (2018), have shifted the focus to the human and cultural factors. These works recognize that the human element is the weakest link and advocate for solutions rooted in organizational culture and leadership modeling. This thesis adopts and extends the latter, arguing that technical controls are moot without behavioral congruence.

2.21.3 Scope and Context: Global Models vs. Regional Specificity

The scope of research reveals a significant geographic imbalance that the current study seeks to rectify.

- Global/Western Models (Prevalent): Most foundational theories are tested and refined using data from North American or European workforces, where individualistic cultures and specific labor laws prevail (Schneier, 2017). These models often assume a high degree of user agency and organizational transparency.
- Regional Specificity (Contrast): Studies focusing on the Middle East, while sparse, highlight the need to account for unique collectivist cultures, hierarchical management styles, and rapidly evolving regulatory environments (Al-Ghamdi & Al-Hashmi, 2020). The current research is distinct in its narrow, high context focus on the UAE banking sector, providing a granularity that broad global studies necessarily omit.

2.21.4 Solution Strategy: Traditional Training vs. Behavioral Nudging

Finally, a comparative look at proposed solutions demonstrates a clear evolution in pedagogical thinking.

- Traditional Strategy (Contrast): Older models primarily proposed solutions involving increased mandatory training and punitive measures. The focus was on input: more hours = more awareness.
- Behavioral Nudging (This Study's Alignment): Newer studies demonstrate the efficacy of continuous, engaging, and personalized reinforcement. This includes the use of gamified learning mechanisms to increase engagement (York & deHaan, 2018) and contextual nudges or sophisticated phishing simulations to condition users against specific threats (Henshaw et al., 2020). This thesis critically evaluates the potential of these innovative pedagogical tools as opposed to outdated, compliance-based approaches.

2.22 Gaps in Literature

While significant scholarly attention has been dedicated to the technical infrastructure of cyber defense and the theoretical models of behavioral intention, critical gaps remain that necessitate the present study. Framing these gaps critically is essential for establishing the original and practical contribution of this thesis.

2.22.1 The Regional Contextual Gap: Lack of Empirical Data from the UAE

The majority of existing security awareness research is geographically and culturally constrained, relying overwhelmingly on data and case studies from North America and Europe. There is a pronounced lack of empirical qualitative research that specifically explores cybersecurity awareness, the influence of organizational culture, and unique regulatory dynamics within the UAE and the broader Middle East (Al-Ghamdi & Al-Hashmi, 2020). Security behavior is not a universal phenomenon; it is profoundly mediated by local management styles,

hierarchical structures, and cultural norms. Assuming that behavioral findings from Western organizations can be directly applied to the high-stakes, rapidly digitizing environment of the UAE banking sector is academically invalid and leads to ineffective, misplaced policy design. This study directly addresses this deficit by providing region-specific, primary qualitative data.

2.22.2 The Methodological Gap: The Failure to Explain Why

A significant limitation is the prevalence of quantitative survey-based studies that measure the *extent* of security awareness or the *correlation* between training and behavior (Choi & Hwang, 2021). These methods often provide statistical breadth but lack depth. There is a lack of in-depth, interpretivist qualitative studies that employ methodologies like phenomenology to explore the lived experiences, psychological drivers, and cultural rationalizations behind security policy non-compliance. Quantitative data identifies *what* the problem is (e.g., policy violation rates), but it fundamentally fails to explain the *why* behind deliberate acts of non-adherence, such as why an employee knowingly shares a password or bypass multi-factor authentication for convenience (Vance et al., 2018). This research, by utilizing thematic analysis on thorough interview data, aims to uncover the deep-rooted cultural and organizational barriers that deter secure behavior.

2.22.3 The Theoretical Integration Gap: Disconnect Between Policy and Behavior

Existing literature frequently treats high-level national cybersecurity policy and micro-level organizational behavior as two separate domains. Current research fails to provide a cohesive, integrated analytical framework that systematically links the success of broad national strategy (e.g., the *UAE National Cybersecurity Strategy*) with measurable, positive behavioral outcomes at the employee level. The efficacy of any national strategy is ultimately determined by its

successful translation into consistent, daily behavior (Schneier, 2017). This study's contribution is the development of a framework that critically assesses this crucial policy-to-practice continuum, specifically analyzing how governmental and regulatory mandates are *interpreted, implemented, and resisted* within the financial sector.

2.22.4 The Practical Application Gap: Sustaining Secure Behavior

While studies universally advocate for better training, they often remain theoretical, failing to provide empirical guidance on the successful implementation and sustainment of behaviorally informed strategies beyond simple compliance checklists. There is a need for research that moves beyond generic calls for "more training" to empirically validate the practical mechanisms necessary to successfully implement advanced, engaging awareness programs, such as gamification (York & deHaan, 2018) or contextual nudges (Henshaw et al., 2020), within a specific organizational context. By focusing on the banking sector, this study aims to deliver actionable, evidence-based recommendations that help organizational leaders transition from a mandatory compliance culture to one that incentivizes and simplifies secure choices, thereby overcoming the "training fatigue" and usability issues identified in the literature (Kandukuri et al., 2022).

Thus, the reviewed literature emphasizes the heightened demand for cybersecurity in industries, particularly in the context of digital transformation. International research emphasizes the significance of big data analytics, cybersecurity awareness, leadership, and emerging technologies in enabling cyber resilience. However, there are still gaps in the capacity to appropriately integrate these factors into the UAE context. In the UAE, cybersecurity is a national issue due to the country's rapid digital development, smart government initiatives, and increasing digitization of industries such as finance, education, and public services. Although some progress

has been made, there is a clear need for more localized research that addresses the UAE's specific cybersecurity challenges, cultural aspects, and regulatory environment.

By bridging these gaps, subsequent studies can assist in constructing a comprehensive, responsive, and culturally attuned cybersecurity framework that will further augment the UAE's resilience against evolving cyber threats. This will necessitate a multi-disciplinary strategy, combining technical measures, education initiatives, leadership training, and behavior studies to construct an entire cybersecurity ecosystem.

2.23 Chapter-End Summary

This chapter presents a comprehensive review of literature addressing the evolving landscape of cybersecurity, emphasizing awareness, asset protection, technological innovation, and behavioral theories that underpin cybersecurity practices. The discussion is structured around the historical development of cybersecurity, current global and UAE-specific perspectives, empirical studies, and theoretical models guiding cybersecurity awareness and behavior.

1. Historical and Conceptual Foundations of Cybersecurity: The chapter opens with a reflection on the significance of cybersecurity in an era marked by rapid digital transformation. As modern societies become increasingly dependent on digital technologies such as artificial intelligence (AI), the Internet of Things (IoT), and cloud computing, the potential for cyber threats has grown exponentially. Cybersecurity has evolved from addressing isolated technical problems to becoming a cornerstone of organizational risk management and national security strategies.

A historical perspective on cyber threats showcases the transformation from early incidents, such as the Morris Worm of 1988, to more recent and sophisticated attacks like the SQL Slammer.

These events reflect the progression in attack methodologies, infection rates, and economic costs. As these threats continue to evolve in complexity and impact, they demand more dynamic and proactive defense mechanisms, including cybersecurity awareness and preparedness strategies.

2. Asset Protection in the Digital Age: The literature reveals a shift in asset protection from traditional physical security toward comprehensive digital safeguarding mechanisms. Organizations now implement multi-level security strategies involving encryption, intrusion detection systems, and multi-factor authentication. Furthermore, compliance with data protection regulations such as GDPR and HIPAA has become essential to preserving digital trust and avoiding legal liabilities.

Modern asset protection is intricately tied to cybersecurity awareness, as human error remains a leading cause of security breaches. The understanding and protection of digital assets now involve not only technological tools but also employee behavior, policy enforcement, and organizational culture. This requires an approach that combines technical solutions with continuous education and awareness initiatives, emphasizing the value of both tangible and intangible assets.

3. Cybersecurity Awareness: Importance and Implementation: Cybersecurity awareness is defined as users' understanding of cyber threats and the knowledge to act appropriately in preventing and responding to them. It encompasses more than just knowing how to create a strong password, it extends to recognizing phishing attempts, securely handling sensitive data, and understanding the broader implications of online behavior. In the UAE, cybersecurity awareness has evolved significantly. The government has spearheaded campaigns and established institutions such as the Telecommunications and Digital Government Regulatory Authority (TDRA) and aeCERT to raise awareness and coordinate responses to cyber incidents.

These initiatives have transitioned from general information-sharing campaigns to strategic, multi-stakeholder efforts integrated into the national digital transformation agenda.

4. Components of an Effective Cybersecurity Awareness Program: The literature identifies several core elements of an effective cybersecurity awareness program. Key among these is continuous education that adapts to emerging threats and technologies. Training must be frequent, engaging, and contextualized to employees' roles. Additionally, leadership support is paramount when senior management actively promotes cybersecurity, it reinforces a culture of accountability and prioritizes security across departments.

Other crucial elements include testing and simulation exercises to assess preparedness (e.g., simulated phishing attacks), real-time feedback mechanisms to correct unsafe behaviors promptly, and gamification to boost engagement. Tailored content for various roles enhances relevance and ensures that employees can directly apply their knowledge to daily tasks. Metrics such as training completion, phishing resilience, and incident reporting rates help evaluate program effectiveness and guide improvements.

5. Challenges to Cybersecurity Awareness: Despite its importance, cybersecurity awareness faces numerous implementation challenges. Organizational culture often undermines awareness efforts, treating them as checkbox compliance tasks rather than strategic investments. Many employees view cybersecurity training as boring, overly technical, or irrelevant, leading to low engagement and minimal behavior change. Another critical challenge is the gap between knowledge and practice. Employees may understand security protocols but fail to follow them due to habit, convenience, or lack of reinforcement. Additionally, most awareness programs inadequately address social engineering, areas where attackers exploit human psychology to bypass technological defenses.

Effective programs must address these behavioral, motivational, and cultural barriers. This includes designing training that is engaging, relevant, and aligned with employees' realities, supported by leadership, and embedded into everyday workflows. Organizations must also adopt adaptive strategies informed by behavioral science to bridge the gap between knowing and doing.

6. Cybersecurity Technologies and Innovations: Technological advancements play a crucial role in enhancing cybersecurity resilience. Artificial Intelligence (AI) and Machine Learning (ML) are increasingly used to detect anomalies, automate responses, and predict potential vulnerabilities. Applications include phishing detection, user behavior analytics, and automated incident response. Blockchain is recognized for its potential to enhance data integrity and prevent fraud due to its decentralized and tamper-proof structure. Cloud security technologies such as encryption, tokenization, and identity management are vital as more organizations migrate sensitive data to the cloud.

Threat intelligence and Governance, Risk, and Compliance (GRC) frameworks provide proactive defense by enabling organizations to anticipate, prepare for, and mitigate risks. The adoption of emerging technologies such as quantum computing, deepfake detection tools, and IoT security solutions are also discussed as future areas of focus.

7. Cybersecurity Best Practices: Best practices in cybersecurity encompass individual behaviors and organizational policies. These include using strong passwords, backing up data regularly, enabling multi-factor authentication, segmenting networks, and updating software frequently. Employees are encouraged to follow safe online habits and report suspicious activities. According to the Cybersecurity and Infrastructure Security Agency (CISA), practices such as role-based access control, encryption, and the use of CISA-provided free tools help

organizations bolster their defense mechanisms. Consistent application of these practices can mitigate risks from both external and internal threats.

8. Strategies for Improving Awareness and Resilience: To improve cybersecurity awareness, organizations are encouraged to employ a variety of strategies, including live hacking demonstrations, phishing simulations, workshops, e-learning platforms, and gamified content. Sector-specific training enhances relevance, while public-private partnerships support widespread information-sharing and collaborative defense. Embedding cybersecurity into education systems ensures future generations understand safe digital behavior from an early age. National awareness campaigns using multimedia and simple language can reach broader audiences, especially when adapted to cultural and linguistic contexts.

9. Theoretical Foundations of Cybersecurity Behavior: Several behavioral theories underpin effective cybersecurity awareness initiatives:

- **Protection Motivation Theory (PMT)** explains how individuals assess threats and their ability to respond, emphasizing the role of fear and efficacy in motivating protective behavior.
- **Technology Acceptance Model (TAM)** explores how perceived usefulness and ease of use influence individuals' adoption of cybersecurity tools and training programs.
- **Theory of Planned Behavior (TPB)** integrates attitudes, subjective norms, and perceived behavioral control to predict cybersecurity behavior, with extensions incorporating context and awareness.

These models offer valuable insights into the psychological and social factors influencing cybersecurity practices, helping organizations design more effective, evidence-based awareness programs.

10. Cybersecurity in the UAE: Current Status and Challenges: The UAE has made commendable progress in cybersecurity awareness through national strategies, educational reforms, and institutional initiatives. However, cyber threats ranging from phishing and ransomware to AI-powered attacks continue to grow. Sectors such as banking, healthcare, and energy are particularly vulnerable. Challenges include unpatched systems, misconfigurations, insider threats, and insufficient public awareness. Although government strategies are in place, the fast-evolving threat landscape necessitates ongoing public education, adaptive policy frameworks, and collaboration across sectors.

11. Research Gaps and Future Directions

Despite extensive global research, gaps remain in localized frameworks tailored to the UAE's regulatory, technological, and cultural contexts. There is also limited empirical research on cybersecurity leadership, behavioral factors, and proactive defense technologies in the region. More research is needed on integrating cybersecurity education into schools and improving individual risk perception.

In summary, this literature review underscores the critical role of cybersecurity awareness in safeguarding digital infrastructure and organizational assets. It highlights the interplay between technology, behavior, leadership, and policy in creating a secure digital environment. As cyber threats grow in frequency and sophistication, developing adaptive, culturally relevant, and behaviorally informed cybersecurity programs become indispensable. The UAE’s national

efforts provide a strong foundation, but continued investment in education, research, and collaboration is essential to build a resilient and cyber-aware society.

CHAPTER 3: METHODOLOGY

3.1 Chapter Overview

This chapter presents the methodological framework used to explore how cybersecurity awareness can be enhanced in the UAE, with particular attention to strategies that mitigate cyber threats and promote asset protection. The chapter outlines the research philosophy, approach, strategy, method choice, data collection and analysis procedures, as well as ethical considerations. The qualitative methodology, conducted through online interviews using Microsoft Teams, was chosen to gain meaningful and relative insights from cybersecurity professionals in the UAE.

3.2 Research Philosophy

This study adopted an interpretivist research philosophy, which is widely recognized in qualitative research for its emphasis on understanding the intricacies of human experiences. Research philosophy refers to the set of beliefs concerning the nature of reality (ontology) and the nature of knowledge (epistemology) that underpins a study's methodology (Saunders, Lewis, & Thornhill, 2019). Interpretivism posits that reality is not objective or singular but rather socially constructed and shaped by human interpretation (Creswell & Poth, 2018).

Interpretivism is grounded in the belief that knowledge is gained through subjective interpretation, and it rejects the notion that social phenomena can be studied using the same methods as the natural sciences (Collis & Hussey, 2021). It acknowledges that individuals bring their own unique experiences, values, and meanings to a given situation. As such, interpretivist researchers aim to uncover the perspectives and lived experiences of participants within their specific contexts.

This philosophy is particularly appropriate for this research, which seeks to explore how cybersecurity professionals in the UAE perceive and implement awareness strategies to combat cyber threats. Understanding these experiences requires more than mere observation of behavior or statistics; it necessitates a deep exploration of participants' meanings, motivations, and interpretations (Thanh & Thanh, 2015). The interpretivist approach, therefore, enables the researcher to generate rich, in-depth narratives by engaging directly with professionals' personal accounts and contextual knowledge.

By using interpretivism, the study provided nuanced insights into how cybersecurity strategies are shaped by organizational culture, individual beliefs, and socio-technological contexts in the UAE. This aligns with the goal of qualitative inquiry, which is not to generalize findings but to understand the complexity of a phenomenon within its natural setting.

3.3 Research Approach

A qualitative inductive approach is employed in this study to explore the nuanced and context-specific experiences of participants. Unlike deductive methods that begin with a predefined theory or hypothesis, inductive research allows themes, patterns, and theories to emerge organically from the data (Creswell & Poth, 2018). This approach is particularly well-suited for studies aiming to gain a deep understanding of human behavior, organizational practices, and socio-cultural dynamics in specific contexts. In this case, the inductive methodology aligns closely with the study's objective of uncovering authentic strategies, challenges, and adaptive practices within the evolving cybersecurity landscape of the United Arab Emirates (UAE).

As the UAE continues to rapidly modernize and digitalize, especially in critical infrastructure and governance, an inductive approach ensures that the insights gathered are grounded in real-life

experiences and responsive to local realities (Braun & Clarke, 2021). Furthermore, by privileging participant voices and emergent patterns over pre-imposed frameworks, this method supports the co-construction of knowledge that is contextually relevant and practically applicable in shaping cybersecurity policy and organizational responses (Merriam & Tisdell, 2016).

3.4 Research Strategy

The research strategy adopted in this study is the case study approach, a qualitative method well-suited to developing an in-depth, multifaceted understanding of a contemporary issue within its real-world context (Yin, 2018). This strategy is especially appropriate given the complexity of cybersecurity awareness in the UAE banking sector—a setting that encompasses diverse technological infrastructures, regulatory frameworks, and employee attitudes. By focusing on this specific sector, the study aims to generate rich insights into how cybersecurity threats are perceived, managed, and mitigated at the institutional level.

Case studies are ideal for answering “how” and “why” questions, particularly in environments where the boundaries between the phenomenon and context are blurred (Yin, 2018). In this research, the case study approach allows for the exploration of how bank employees interpret cybersecurity policies, why certain threats are prioritized, and how awareness campaigns are internalized across different organizational roles. This sector-specific inquiry captures the sociotechnical dynamics of cybersecurity, highlighting the interplay between digital systems, institutional culture, and individual behaviors (Stake, 1995).

Aligned with the interpretivist paradigm, this strategy emphasizes the importance of subjective experiences and contextually grounded meanings (Creswell & Poth, 2018). Rather than seeking universal laws or predictive models, the study is grounded in understanding the lived experiences

of employees and IT professionals who operate within the evolving cybersecurity ecosystem of the UAE. This philosophical orientation recognizes that perceptions of cyber threats and risk management practices are shaped by cultural, organizational, and regulatory factors unique to the local context (Lincoln, Lynham, & Guba, 2018).

Additionally, the inductive logic embedded in the case study strategy allows for the development of theory from the ground up, rather than testing pre-established frameworks (Saunders, Lewis, & Thornhill, 2019). By identifying emerging themes and patterns from participant narratives, the study will build a conceptual understanding of effective cybersecurity awareness strategies that are relevant, scalable, and culturally sensitive to the UAE.

The effectiveness of case study research in the field of cybersecurity is well-established. For example, Alshaikh et al. (2018) employed a qualitative case study approach to examine the cultural dimensions of cybersecurity in Saudi organizations, demonstrating how context influences awareness and policy implementation. Similarly, Okere et al. (2012) used a case study to investigate information security governance in South African public institutions, yielding practical recommendations for policy development and institutional alignment.

Given these precedents, the case study strategy offers a robust methodological foundation for this research. It enables the researcher to generate actionable insights and localized recommendations that can inform national cybersecurity strategies and improve institutional resilience in the banking sector.

3.5 Research Method Choice

This study adopts a qualitative research methodology, utilizing semi-structured interviews as the primary method of data collection. This approach is chosen for its ability to capture the

depth and complexity of human experiences, especially in areas such as cybersecurity, where the interplay between technological systems and human behavior is nuanced and dynamic (Denzin & Lincoln, 2018; Merriam & Tisdell, 2016). By focusing on the lived experiences and perceptions of IT professionals and cybersecurity specialists within the UAE, the research seeks to explore not only the technical aspects of cybersecurity threats but also the strategies, cultural contexts, and behavioral responses to these threats.

Semi-structured interviews offer an effective balance between consistency and flexibility. The use of a guiding set of questions ensures that all key themes are addressed across interviews, while the open-ended nature of the method allows participants the freedom to elaborate on issues most meaningful to them (Kallio et al., 2016). This adaptability enables the researcher to probe deeper perceptions and follow up on emerging ideas in real time (Gill et al., 2008).

This method has been widely adopted in previous studies that examine cybersecurity awareness, organizational risk culture, and technology adoption. For example, Alshaikh et al. (2018) used semi-structured interviews to explore information security culture in Saudi Arabian organizations, revealing how cultural factors influence cybersecurity practices. Similarly, Parsons et al. (2017) employed qualitative interviews to understand end-user cybersecurity behavior, identifying cognitive and contextual factors that impact compliance with security policies. In another study, Okere et al. (2012) utilized semi-structured interviews to assess information security governance in South African public organizations, offering practical insights into policy implementation and institutional challenges.

Furthermore, in the UAE and broader Middle East context, qualitative interviews have been used to examine digital transformation, data privacy, and national cybersecurity strategies

(Al-Khouri, 2012; Alkhalil et al., 2021), reinforcing the value of qualitative inquiry in understanding sociotechnical systems in evolving digital landscapes.

Overall, this method is well-suited to the phenomenological orientation of the study, as it foregrounds the voices and real-life experiences of participants. It allows for a rich understanding of not only what cybersecurity strategies are being used but how they are interpreted, experienced, and adapted in practice.

3.6 Research Techniques and Procedure

This study employed qualitative research techniques to explore the experiences, perceptions, and insights of professionals working in cybersecurity-related roles within the United Arab Emirates (UAE). The research design was guided by an interpretivist paradigm, aiming to understand how individuals construct meaning around cybersecurity awareness and practice in their professional environments.

3.6.1 Participant Selection and Recruitment

A purposive sampling strategy was used to identify and select participants who were most likely to contribute rich and relevant data to the study. Specifically, the sample included cybersecurity professionals, IT personnel, and digital systems analysts employed in the UAE banking sector. These individuals were chosen based on their direct involvement in the implementation, oversight, or strategic planning of cybersecurity systems within their organizations.

To initiate contact, the researcher utilized a combination of professional networks, LinkedIn connections, and referrals through industry associations. A formal email invitation outlining the

purpose of the study, the confidentiality of responses, and participation expectations was sent to potential participants. Those who expressed interest were provided with a participant information sheet and a consent form, both of which were approved by the UCLan ethics review board.

3.6.2 Justification for Focusing on Banking Professionals

3.6.2.1 Strategic Relevance of the UAE Banking Sector

The decision to focus the case study on banking professionals is strategic, not arbitrary, and is directly linked to the research's aim of enhancing national cybersecurity awareness and asset protection.

1. Critical National Infrastructure (CNI) Status: The UAE banking and finance sector constitutes a vital segment of the nation’s Critical National Infrastructure (CNI). A successful cyberattack on a major financial institution would not only result in massive monetary losses but could also trigger systemic financial instability, erode consumer trust, and directly threaten the economic stability and international reputation of the UAE. Therefore, the sector represents the highest possible risk environment, making the study of its vulnerabilities a national security imperative.

2. Regulatory and Compliance Intensity: The banking sector is subjected to the most stringent and frequently updated cybersecurity regulations from the UAE Central Bank and the National Cybersecurity Council. This high-compliance environment means that any findings regarding policy failures, training deficiencies, or behavioral lapses occur despite the application of maximum regulatory pressure. This makes the banking sector an ideal stress test environment for assessing the efficacy of national policies.

3. Advanced and Complex Threat Landscape: Banks handle vast quantities of high-value, sensitive data (personal information, transaction records, proprietary algorithms), making them prime targets for sophisticated, state-sponsored, or highly organized criminal groups. The threats faced are rarely simple malware attacks; they involve advanced persistent threats (APTs), zero-day exploits, and, most relevant to this study, highly sophisticated social engineering and insider threats aimed at exploiting the human element. The cybersecurity awareness challenges found here represent the highest level of difficulty.

3.6.2.2 Transferability of Findings (Generalization in Qualitative Research)

While qualitative research, particularly a single-sector case study, does not aim for statistical generalization (Yin, 2018), its findings hold high transferability to other contexts and sectors facing similar challenges.

1. Conceptual Transferability (The "Human Problem"): The core research questions revolve around behavioral failure, the intention-action gap, and the translation of policy into practice. These are challenges common to *all* organizations. The psychological and cultural drivers for bypassing security protocols (e.g., convenience, lack of managerial accountability, training fatigue) are not unique to banks; they are universal human factors (Vance et al., 2018).

2. Sectoral Transferability (High-Risk/High-Compliance): The findings from the banking sector are highly transferable to other high-risk, high-compliance sectors within the UAE's CNI, such as:

- Energy/Oil & Gas: They manage complex operational technology (OT) and information technology (IT) environments and are subject to stringent safety and security regulations.
- Government/Public Services: They handle vast amounts of citizen data and face similar threats of espionage and policy mandates.

3. Policy Transferability (Best Practice Model): The successful strategies and effective solutions identified within the banking sector (e.g., role-based training, incentivization mechanisms, leadership modeling) represent a gold standard for mitigating human risk. These effective practices can be directly adapted and scaled by policymakers and security managers across the UAE public and private sectors seeking to enhance their own security culture. The lessons learned in this demanding environment can therefore inform national best practice guidelines.

3.7 Data Collection Procedure

To ensure both safety and convenience, particularly considering ongoing post-pandemic considerations, all interviews were conducted virtually using Microsoft Teams. This platform was selected due to its security features, widespread accessibility, and its ability to facilitate real-time, synchronous communication regardless of participants' physical location.

The data collection process involved the following steps:

- Scheduling: Participants selected interview slots based on their availability. Flexibility was offered to accommodate diverse work schedules, especially for participants in critical infrastructure roles.
- Pre-Interview Briefing: At the beginning of each session, the researcher reiterated the study's objectives, explained the confidentiality protocols, and obtained verbal reaffirmation of informed consent, including consent for audio recording.
- Interview Duration: Each session lasted approximately 30 to 45 minutes, depending on the depth and direction of participant responses.
- Interview Guide: A semi-structured interview guide was used to ensure consistency across interviews while allowing space for spontaneous elaboration and clarification. The guide contained open-ended questions (as outlined in Section 3.7) designed to probe participants' understanding of cybersecurity threats, their experiences with past incidents, familiarity with national policies, and views on awareness challenges and solutions.
- Audio Recording and Note-Taking: With participants' permission, interviews were audio recorded using the built-in Microsoft Teams functionality. The researcher also took supplementary notes during the interviews to capture non-verbal cues, significant points, and emergent themes that might require further exploration.
- Post-Interview Documentation: Immediately after each session, interview recordings were securely saved on a password-protected device, and the researcher prepared preliminary reflective memos. These memos supported early theme identification and contributed to analytic transparency.

3.7.3 Ethical Considerations and Confidentiality

The research process was governed by strict ethical protocols to ensure the protection of participant identity, privacy, and data security. Participants were assured that:

- All responses would remain confidential and anonymized in the final report.
- Names, organizational affiliations, and any potentially identifiable information were excluded or generalized.
- Participation was entirely voluntary, with the option to withdraw at any stage without penalty.

The digital nature of the interviews helped mitigate any physical safety concerns and contributed to an environment where participants could speak candidly from their preferred private settings.

3.8 Data Collection Method

Data were collected using semi-structured interviews, which were deemed appropriate for this qualitative study due to their flexibility and ability to elicit detailed, context-specific responses. This method enabled the researcher to explore both anticipated and unforeseen factors influencing cybersecurity awareness among banking sector employees in the United Arab Emirates (UAE).

3.8.1 Participant Profile and Sampling Frame

The research focused on employees within the UAE banking sector, which comprises an estimated 35,830 professionals as of 2022. A purposive sampling strategy was adopted to select individuals who were most likely to provide relevant and informed responses, based on their roles and exposure to digital platforms.

Inclusion Criteria:

Eligible participants were required to:

- be currently employed in the UAE banking sector.
- Serve in administrative, financial, technical, or cybersecurity-related roles.
- Be active users of digital banking platforms or the Internet in their day-to-day work.
- Be aged between 24 and 54 years, to ensure engagement with cyber tools and capacity for reflective analysis.

Exclusion Criteria:

Participants were excluded if they:

- were not currently working in the banking sector (e.g., retirees, former employees).
- Held roles unrelated to digital infrastructure (e.g., general administrative staff, receptionists, maintenance workers).
- were younger than 24 or older than 54 years.

3.8.2 Interview Administration and Ethical Considerations

All interviews were conducted online via Microsoft Teams to facilitate accessibility, maintain convenience for participants, and expedite ethical clearance. The virtual setting eliminated the need for physical meetings, reducing logistical barriers and enhancing participant comfort and privacy.

Prior to beginning the interview, participants were briefed on the purpose and scope of the research. Informed consent was obtained for participation and for the audio recording of the sessions. Recordings were stored securely and used solely for transcription and data analysis purposes, in full compliance with ethical research standards.

3.8.3 Interview Scope and Areas of Inquiry

The interview aimed to assess participants' knowledge, experiences, and perceptions of cybersecurity threats and defense mechanisms within the UAE's banking environment. Questions addressed key issues such as:

- Awareness of cybersecurity risks.
- Experience with cyber incidents.
- Familiarity with national policies and regulations.
- Organizational efforts to improve awareness.
- Perceived gaps in training or compliance.
- Recommendations for improving the cybersecurity landscape in the UAE.

Plan of Interview: Strengthening Cybersecurity Awareness in the Banking Sector of the United Arab Emirates

The following guide was used to structure each semi-structured interview:

1. Can you describe the current level of cybersecurity awareness among employees in UAE organizations?
2. From your viewpoint, how critical is cybersecurity awareness in protecting personal and organizational assets in the UAE?
3. What are the most prevalent cyber threats facing individuals and businesses in the UAE today?
4. Can you share any recent cybersecurity incidents that have impacted your organization?
5. What are the most common tactics currently used by cybercriminals to target individuals or businesses in the UAE?
6. Are you familiar with the UAE's existing cybersecurity policies and regulations?
7. Have you participated in any cybersecurity awareness campaigns?

8. What are the main challenges preventing employees from adopting best cybersecurity practices?
9. From your viewpoint, what changes need to be made to the UAE's cybersecurity policies or regulations to overcome cyber threats?
10. Is there anything else you would like to share regarding cybersecurity protection strategies in the UAE?

The data collected through these interviews provided valuable insight into both individual and organizational readiness to address cybersecurity threats, as well as perceived gaps in the current regulatory and institutional frameworks.

3.9 Summary of Data Analysis Method

Data analysis was conducted using thematic analysis, guided by Braun and Clarke's (2006) widely recognized six-step framework. This approach involves:

1. Familiarization with the data by thoroughly reading and re-reading interview transcripts to immerse in the data and identify initial patterns.
2. Generating initial codes by systematically labeling relevant features of the data that relate to the research questions.
3. Searching for themes by grouping codes into broader themes that capture important patterns across the dataset.
4. Reviewing themes by refining themes by checking their consistency and coherence against coded extracts and the entire dataset.
5. Defining and naming themes by articulating the essence of each theme and assigning clear, descriptive names.

6. Producing the final report by integrating the thematic findings into a compelling narrative that addresses the study's objectives.

Thematic analysis is a flexible and accessible qualitative method that is particularly suitable for interview data, as it allows researchers to uncover both explicit and implicit meanings, attitudes, and behaviors (Braun & Clarke, 2006). This method enables a rich, detailed exploration of cybersecurity practices and awareness strategies, facilitating an understanding of how participants perceive and engage with asset protection in the UAE context.

Initially, the interview transcripts were reviewed manually to enhance the researcher's familiarity and ensure contextual understanding. To manage the complexity and volume of qualitative data efficiently, qualitative data analysis software was employed. NVivo was used to assist with organizing and coding data, offering powerful tools for visualizing code relationships and supporting systematic theme development (Welsh, 2002). However, given the extensive dataset comprising numerous interview transcripts from multiple sources, MAXQDA was introduced to complement NVivo's capabilities.

MAXQDA provides advanced features for data management, including flexible coding, memo writing, and sophisticated retrieval options, which streamline the analysis process (Kuckartz & Rädiker, 2019). Its ability to integrate diverse data types and track coding across sources made it particularly useful for maintaining consistency and enhancing transparency in theme development. Furthermore, MAXQDA's visualization tools such as code maps and thematic networks—facilitated the identification of complex patterns and relationships within the data, contributing to a more nuanced and comprehensive analysis.

Despite its advantages, thematic analysis carries validity concerns that warrant careful consideration. Given its flexibility, researchers must guard against subjective bias during coding and theme selection, which can influence how patterns are identified and interpreted (Nowell et al., 2017). To mitigate this, the analysis involved iterative review cycles, peer debriefing, and maintaining an audit trail of coding decisions, enhancing the credibility and dependability of findings. Transparency in how themes were defined and supported by data extracts was prioritized to ensure confirmability. Additionally, member checking with selected participants was employed to validate the interpretations and improve the trustworthiness of the results. Together, the combined use of thematic analysis and these qualitative data analysis tools ensured a rigorous and transparent approach. This methodological rigor is essential for producing credible insights into cybersecurity awareness and practices, ultimately supporting evidence-based recommendations for enhancing asset protection strategies in the UAE.

3.10 Chapter Summary

This chapter provided a comprehensive overview of the research methodology employed to investigate cybersecurity awareness strategies within the context of the United Arab Emirates (UAE). Given the exploratory nature of the study and the focus on understanding participants' lived experiences and perceptions, a qualitative research design rooted in an interpretivist paradigm was adopted. Specifically, a phenomenological research strategy was selected to capture the essence of individuals' subjective experiences regarding cybersecurity awareness. The data collection process involved conducting semi-structured interviews, which allowed for flexibility in probing participants' insights while maintaining a consistent thematic focus across sessions. These interviews were carried out virtually via Microsoft Teams, a platform that

facilitated accessibility and convenience for participants dispersed across various locations in the UAE.

Following data collection, a rigorous thematic analysis approach was applied to identify, analyze, and interpret patterns and themes emerging from the interview transcripts. This method enabled a rich and nuanced understanding of the factors influencing cybersecurity awareness and the effectiveness of current strategies. In addition, the chapter outlined the ethical considerations integral to the research process. Measures to ensure informed consent, confidentiality, and the secure handling of data were described, reflecting the commitment to uphold participants' rights and maintain the integrity of the research.

In summary, this chapter established the methodological foundation for the study, detailing the rationale behind the chosen approach, the data collection techniques, analytical procedures, and ethical considerations. The following chapter will build upon this foundation by presenting and discussing the key findings derived from the interview data, shedding light on the practical implications for cybersecurity awareness initiatives in the UAE.

CHAPTER 4: FINDINGS & DISCUSSION

4.1 Introduction

This chapter presents a comprehensive analysis of the qualitative data collected from 50 employees across various roles within the UAE banking sector, focusing on their experiences and perceptions of cybersecurity awareness strategies. The analysis is structured around three key dimensions: qualitative insights revealing patterns and themes; sentiment analysis to assess employees' attitudes toward cybersecurity; and thematic categorization to organize responses into meaningful sections for further research and policy implications. The aim is to interpret current levels of cybersecurity awareness, identify prevalent threats and challenges, and gather employee-driven recommendations to enhance cybersecurity posture. The findings provided valuable context for understanding human factors in cybersecurity and informing targeted interventions.

4.2 Qualitative Analysis (Key Insights & Patterns)

4.2.1 Cybersecurity Awareness Levels

Employees across the banking sector widely acknowledge that overall cybersecurity awareness has improved in recent years, reflecting increased organizational efforts and external regulatory pressures. However, several participants highlighted a troubling inconsistency in the actual adherence to best practices. While many employees are knowledgeable about cybersecurity principles, a significant portion still neglects critical habits such as regularly

updating passwords, avoiding suspicious links, or safeguarding sensitive information. This gap between awareness and behavior was explicitly mentioned in Responses 1 through 5, suggesting that awareness alone is insufficient to drive consistent security compliance.

A notable pattern emerged regarding awareness disparities by job role and seniority. Senior employees and those in IT or risk management functions demonstrated a more thorough understanding of cybersecurity risks and protocols, as exemplified in Response 6. Conversely, junior staff and employees in non-technical roles exhibited lower awareness, which may stem from limited exposure to specialized training or less perceived relevance of cybersecurity to their daily tasks. This uneven distribution highlights a critical area for targeted educational initiatives to elevate baseline awareness across all staff tiers.

Employees also reflected on the quality and impact of existing cybersecurity training programs. While training is available, many felt it lacked engagement or practical relevance, leading to low retention of key security messages (Response 8). The perception that training is often repetitive or overly generic suggests a need for more dynamic, role-specific, and interactive learning approaches to better equip employees.

4.2.2 Importance of Cybersecurity Awareness

Participants consistently emphasized cybersecurity's vital role in maintaining the integrity and trustworthiness of banking operations (Responses 6-10). Given the sensitive nature of financial data and transactions, employees view cybersecurity not just as a technical necessity but as a foundational element for protecting customers and the institution's reputation.

Many respondents underscored the "human factor" as one of the most significant vulnerabilities in cybersecurity frameworks (Responses 8, 10). They noted that despite sophisticated technical

controls, human errors such as falling for phishing emails or mishandling confidential data remain a primary cause of security breaches. This perception aligns with industry understandings that technology alone cannot fully mitigate cyber risk without strong human awareness and discipline.

Several employees proposed that cybersecurity should transcend its traditional role as an IT department responsibility and instead be embedded within the overall company culture (Response 7). This cultural integration involves fostering a shared sense of ownership and accountability for cybersecurity at every organizational level, encouraging open communication about threats, and normalizing security-conscious behaviors as part of everyday business practices.

4.2.3 Cybersecurity Threats in the UAE

The most frequently cited threats reflect the global cybercrime landscape but are particularly salient in the UAE's banking context. Phishing and social engineering attacks emerged as the predominant concerns, reported by multiple employees as persistent and evolving threats (Responses 11-15). These attacks exploit human trust and curiosity, often masquerading as legitimate communications to extract credentials or deliver malware.

Employees also observed an alarming rise in ransomware incidents, the proliferation of fake banking applications, and various email scams aimed at deceiving both staff and customers (Responses 12-15). The growing sophistication of these attacks demands equally advanced detection and response strategies.

Furthermore, insider threats whether intentional or accidental, alongside human error were repeatedly highlighted as persistent risks (Response 14). This includes employees

inadvertently exposing systems to vulnerabilities or misusing access privileges, reinforcing the need for stringent internal controls and ongoing training.

4.2.4 Cybersecurity Incidents in the Workplace

Within the workplace, employees reported multiple instances of cybersecurity incidents ranging from phishing attacks and malware infections to full-scale data breaches (Responses 16-20). These incidents underscore the ever-present threat landscape confronting financial institutions.

Importantly, several responses indicated that many of these security breaches were preventable, attributing their occurrence to employee negligence or lapses in vigilance (Responses 18-19). For example, clicking suspicious email links or bypassing security protocols were common behaviors linked to incident triggers.

Despite these challenges, employees expressed appreciation for proactive cybersecurity measures implemented by their organizations, such as real-time threat monitoring and rapid incident response teams, which successfully mitigated the impact of some attacks and prevented larger breaches (Response 17). This proactive posture helps build employee confidence and trust in the institution's cybersecurity capabilities.

4.2.5 Cybercriminal Tactics & Attack Methods

The respondents provided detailed descriptions of the tactics employed by cybercriminals targeting the banking sector. Fake emails, often carefully crafted to mimic official communications, remain a primary vector for attacks. Additionally, spoofed IT support calls—where attackers impersonate internal helpdesk personnel to extract sensitive information—and social media scams are frequently reported (Responses 21-25).

A subset of employees noted that cybercriminals are increasingly employing sophisticated techniques, including deepfake audio or video scams that are more difficult to detect and counter (Response 23). This evolution in attack methods signals an urgent need for continuous awareness updates and advanced technological defenses.

4.2.6 Familiarity with UAE Cybersecurity Policies

Awareness of the UAE's cybersecurity regulations and policies among employees was found to be varied and generally limited (Responses 26-30). While many respondents recognized that regulatory frameworks exist, there was a widespread lack of in-depth understanding of the specifics or implications of these laws on their daily work (Response 28).

This knowledge gap often resulted in employees deferring responsibility for compliance to IT departments or security specialists, rather than actively engaging with or familiarizing themselves with policy requirements (Response 29). Such reliance could pose risks if non-IT staff inadvertently violate regulations due to ignorance, highlighting the need for broader policy education across all employee groups.

4.2.7 Cybersecurity Awareness Campaigns & Training

Employees reported varying levels of participation in cybersecurity awareness initiatives, including formal training programs, phishing simulation exercises, and online courses designed to reinforce secure behaviors (Responses 31-35). While many appreciated the availability of these resources, some found the training content overly simplistic or lacking in engagement, reducing its effectiveness in sustaining long-term behavioral change (Response 34).

Moreover, a small proportion of employees candidly admitted to having never participated in any cybersecurity awareness campaigns, reflecting either gaps in training delivery or issues with

employee accessibility and motivation (Response 35). This underscores the importance of ensuring inclusivity and relevance in program design.

4.2.8 Challenges in Cybersecurity Adoption

A recurrent theme among responses was the identification of key barriers hindering effective cybersecurity adoption. Complacency emerged as a significant challenge, with some employees underestimating the likelihood or impact of cyber threats (Responses 36-40). Additionally, the complexity and perceived rigidity of security policies often discouraged compliance, as employees feared these measures might hinder their productivity or create unnecessary burdens.

Ignoring security warnings and circumventing protocols were common practices cited by participants, driven by convenience or lack of understanding of potential consequences (Responses 37-38). Alarmingly, password sharing, a direct violation of security best practices persisted despite repeated organizational warnings and awareness campaigns (Response 40). These findings suggest that technological controls must be complemented by behavioral and cultural interventions to improve compliance.

4.2.9 Suggestions for Policy Changes

Considering the observed challenges, employees advocated strongly for policy reforms aimed at strengthening cybersecurity governance. Many recommended stricter regulations with clearer enforcement mechanisms, including financial penalties for non-compliance, to raise the stakes for negligent behavior (Responses 41-45).

Several responses emphasized the need for more rigorous enforcement of existing cybersecurity policies within banking institutions, suggesting that without accountability, policy effectiveness remains limited (Responses 41-42).

Collaboration across multiple stakeholders including banks, government regulators, and cybersecurity experts was also frequently recommended to create unified standards, share threat intelligence, and develop coordinated responses to cyber risks (Response 45).

4.2.10 Additional Cybersecurity Strategies & Recommendations

Employees expressed support for integrating emerging technologies such as artificial intelligence (AI) to enhance security monitoring, automate fraud detection, and reduce human error (Response 47). AI's potential to identify anomalous patterns and respond swiftly to threats was widely seen as a promising advancement.

Rewarding employees for proactively reporting security threats and suspicious activities was identified as an effective strategy to incentivize vigilance and foster a security-conscious culture (Response 46). Simplification of security procedures was also suggested to improve usability and compliance, recognizing that overly complex or cumbersome measures often deter adherence (Response 49).

Finally, some participants proposed launching a national cybersecurity awareness campaign to raise public and employee awareness at a broader scale, reflecting the recognition that cybersecurity is a collective responsibility extending beyond individual organizations (Response 50).

4.3 Summary of Current State of Cybersecurity Awareness and Threat Perception

This section synthesizes the participants' views on the current level of awareness, distinguishing between theoretical knowledge and practical application, and identifying the threats most relevant to the human element.

4.3.1 The Intention-Action Gap: Knowledge vs. Application (Synthesis)

Participants consistently reported a dichotomy in employee awareness: high theoretical knowledge contrasted with poor practical application.

- High Theoretical Awareness: Respondents indicated that, due to mandatory national and banking sector training, most employees possess adequate *intellectual awareness* of basic security concepts (e.g., recognizing strong passwords, the definition of phishing). This fulfills the baseline educational mandate.
- Poor Practical Application (The Gap): The core failure is the inability or unwillingness to translate this knowledge into sustained, consistent secure behavior. Employees admitted to bypassing multi-factor authentication, sharing login details within teams for efficiency, or reusing simple passwords—all conscious choices driven by convenience over security. This finding is crucial, highlighting that the problem is not a deficit of knowledge, but a failure of behavioral reinforcement (Vance et al., 2018).

4.3.2 The Preeminence of Social Engineering and Insider Risk (Novel Contribution)

The findings uniquely prioritize human-targeted threats over purely technical vulnerabilities in the UAE banking context.

- Phishing as the Gateway: Phishing and social engineering were universally cited as the primary and most successful attack vectors. Participants noted that while technical infrastructure (firewalls, endpoint protection) is highly mature, these sophisticated, contextual attacks bypass technology by exploiting human trust and distraction.
- The Negligent Insider: Beyond deliberate insider threats, the data highlighted the overwhelming danger of the "negligent insider", the compliant employee whose lapses in judgment (e.g., clicking a link, losing a device, using unauthorized shadow IT) creates vulnerability. This demonstrates that asset protection is fundamentally contingent upon continuous human vigilance, a factor often overlooked in technical defense strategies.

4.4 Empirical Findings on Current Awareness and Strategy Effectiveness (Objective 1)

This section synthesizes empirical material addressing the first two research objectives: assessing the current perceptions of cybersecurity awareness and examining the implementation and effectiveness of current organizational strategies against cyber threats.

4.4.1 Strategy Failure: The Dominance of the Compliance Mindset

Current organizational strategies were found to be overwhelmingly compliance-centric rather than behavior-centric, which explains the persistence of the intention-action gap.

- Checklist Mentality: Strategies are primarily designed to satisfy regulatory audits (National Cybersecurity Council, 2024), resulting in mandatory, annual, generic e-learning modules. This passive approach generates "training fatigue" rather than lasting

behavioral change, as employees minimize engagement to meet the minimum required completion time.

- Misallocation of Resources: Organizations demonstrate a clear preference for investing in complex technical controls (e.g., next-generation firewalls, SIEM systems) over sophisticated human risk management programs. This strategic imbalance reflects a fundamental misunderstanding: highly effective technology is rendered moot by a single instance of human error or negligence.

4.5 Sentiment Analysis

The sentiment analysis of employee responses reveals a nuanced landscape of attitudes toward cybersecurity within the banking sector. Responses were categorized into Positive (Proactive & Optimistic), Neutral (Observational & Descriptive), and Negative (Frustration & Concerns) sentiments (see table 1). This categorization helps in understanding not only the emotional tone but also the underlying perceptions that may influence cybersecurity behaviors and policy effectiveness.

Table 4.1: Summary of Sentiment Analysis

Sentiment	**Number of Responses**	**Example Responses**
Positive (Proactive & Optimistic)	17 responses	"Our organization ensures we are trained on UAE cybersecurity laws." (Response 26)

Neutral (Observational & Descriptive)	22 responses	"Phishing emails are the biggest threat right now." (Response 11)
Negative (Frustration & Concerns)	11 responses	"Some employees still use weak passwords despite warnings from IT." (Response 5)

4.5.1 Positive Sentiment: Proactive Engagement and Optimism

Approximately 34% of the responses reflect a positive sentiment toward cybersecurity within the organization. Employees expressing this sentiment often highlighted the existence of robust training programs, ongoing awareness campaigns, and proactive security measures implemented by their institutions. For instance, as illustrated by Response 26, several employees took pride in their organization's commitment to educating staff on UAE cybersecurity laws and ensuring compliance.

This optimism is characterized by confidence in the current cybersecurity framework and a belief that with proper training and policies, the risk of cyber threats can be effectively managed. These employees often expressed a willingness to engage actively in cybersecurity practices, viewing their roles as integral to protecting the organization. The positive sentiment reflects an encouraging foundation for fostering a security-aware culture.

4.5.2 Neutral Sentiment: Factual Observations and Descriptions

The largest share of responses, about 44%, exhibited a neutral tone. These responses were primarily factual and descriptive, focusing on outlining specific cybersecurity threats, such as phishing (Response 11), and summarizing company policies or incident reports without attaching

emotional judgment. This neutrality suggests that many employees see cybersecurity as a necessary operational reality rather than a source of anxiety or enthusiasm.

Neutral responses often provided valuable insights into the current threat environment and organizational responses without expressing personal concern or endorsement. This detached perspective could indicate a professional or routine approach to cybersecurity, where employees acknowledge the risks but may not feel personally engaged or impacted. Understanding this sentiment is critical for tailoring communications that move employees from passive awareness to active participation.

4.5.3 Negative Sentiment: Frustration and Concerns

About 22% of the responses conveyed negative sentiments, revealing significant employee frustrations and concerns regarding cybersecurity practices. These responses pointed to ongoing challenges such as poor adherence to security protocols, ineffective training, and complacency among staff. For example, Response 5 highlights frustration over employees continuing to use weak passwords despite repeated warnings, underscoring persistent behavioral risks.

Negative sentiments also encompassed feelings of being overwhelmed by complex security policies or skepticism about the adequacy of existing measures. Such concerns may reflect underlying barriers to effective cybersecurity adoption, including lack of motivation, insufficient resources, or inadequate communication from leadership. Addressing these negative perceptions is essential to improve compliance and foster a culture of shared responsibility.

4.5.4 Sentiment Breakdown and Implications

- Positive Sentiment (34%): Indicates a solid base of employees who recognize the importance of cybersecurity and actively participate in mitigating risks. This group can be leveraged as cybersecurity champions to promote best practices across the organization.
- Neutral Sentiment (44%): Represents a significant number of employees who may understand the technical aspects and threats but lack emotional engagement or motivation. Targeted initiatives are needed to transform this group's neutral stance into positive behavioral change through more personalized and interactive training.
- Negative Sentiment (22%): Highlights areas of concern that could undermine overall cybersecurity efforts. These include frustration with compliance challenges and perceived gaps in training effectiveness. Addressing these negative perceptions requires focused interventions, such as simplifying security protocols, increasing communication transparency, and involving employees in policy development to foster buy-in.

Overall, this sentiment distribution suggests a cybersecurity culture at a crossroads: while many employees recognize and support security initiatives, a sizable portion remains disengaged or frustrated. For cybersecurity programs to succeed, organizations must harness the optimism of the positive group, engage the neutral majority more meaningfully, and address the concerns driving negative sentiment.

4.6 Summary of Organizational Strategy, Implementation, and Behavioral Challenges

This section consolidates the analysis of current organizational strategies, revealing why they are failing to bridge the behavioral gap and identifying the most critical and distinctive organizational challenges.

4.6.1 Strategic Failure: Compliance-Centric Training (Streamlined)

Organizational cybersecurity strategies were found to be overwhelmingly compliance-centric rather than behavior-centric.

- Checklist Mentality: Current training models are largely driven by a "checklist mentality" designed to satisfy regulatory audits (National Cybersecurity Council, 2024), typically involving generic, annual e-learning modules. This passive approach leads to training fatigue, where employees minimize engagement to meet the minimum required completion time.
- Lack of Personalization: Training is rarely role-based or contextual. As noted in the literature, generic content fails to resonate with employees, particularly those in non-technical roles, who require training tailored to their specific daily risks (e.g., finance staff needing advanced fraud awareness vs. IT staff needing secure coding practices).

4.6.2 The Hierarchical Enforcement and Modeling Challenge (Distinctive Contribution)

A finding distinctive to the organizational culture observed is the critical role of management and hierarchy in undermining security practice.

- Leadership Modeling Failure: Participants revealed instances where senior executives visibly circumvented security policies for convenience, such as insisting on using simple

passwords or refusing mandatory multi-factor authentication. This top-down failure of leadership modeling significantly erodes the authority of security policies among junior staff, making enforcement arbitrary (Vance et al., 2018).

- Fear of Reporting: In the observed hierarchical environment, there exists a significant reluctance or fear among junior employees to proactively report incidents or suspicious activities. This fear stems from concerns over blame, professional repercussions, or disciplinary action, which creates a dangerous time lag between a security event and its detection. This contributes directly to asset damage by allowing threats to persist undiscovered.

4.6.3 The Usability and Convenience Barrier (Novel Synthesis)

All challenges ultimately synthesize into the barrier of usability and convenience, the strongest driver of non-compliant behavior.

- Complex Policies: Security policies are often complex, lengthy, and disconnected from operational workflow, pushing employees to develop unauthorized "workarounds" that are convenient but insecure (Kandukuri et al., 2022).

- The Cost of Compliance: The effort required for compliance—entering long passwords, verifying identity multiple times, and navigating complex systems—is perceived by employees as a tax on productivity. Until security is made easier, faster, and more engaging than the insecure alternative, employees will rationally choose convenience, thus confirming the human element as the primary vulnerability.

4.7 Empirical Findings on Challenges and Recommended Strategies (Objective 2)

This section focuses on the empirical material relating to the third and fourth research objectives: exploring the key organizational and cultural challenges preventing optimal practice and identifying enhanced, behaviorally informed strategies.

4.7.1 Organizational and Cultural Challenges

The most distinctive and novel challenge identified in this research stems from the hierarchical nature of the UAE corporate environment and its impact on security policy authority.

- Leadership Modeling Failure: Crucially, participants reported that senior executives visibly circumvent security policies for personal convenience, such as resisting multi-factor authentication or demanding quick, unsecured access. This top-down failure of leadership modeling erodes the legitimacy of security policies among junior staff, making enforcement appear arbitrary and optional (Vance et al., 2018).
- The Usability-Convenience Barrier: This is the ultimate synthesis of all challenges. Employees view compliance as a tax on productivity. Until security procedures (e.g., complex passwords, repeated sign-ins) are made easier, faster, and more convenient than the insecure alternative, employees will naturally default to the least resistant path, confirming the theory that usability is paramount to security adherence (Kandukuri et al., 2022).

4.7.2 Recommended Strategies: The Shift to Behavioral Reinforcement

Participants offered solutions that strongly converge on a shift from traditional training towards continuous, behaviorally informed security interventions, directly addressing the intention-action gap.

- Advocacy for Role-Based Gamification: The strongest recommendations centered on replacing annual e-learning with frequent, gamified, and role-specific training modules. This leverages the power of incentivization and competitive feedback (York & deHaan, 2018) to improve engagement and ensures that training content is immediately relevant to an employee's daily risk exposure (e.g., focusing on trade secrets for executives, phishing for administrative staff).
- Mandatory Leadership Accountability: Participants stressed the need for mandatory enforcement and accountability for senior management. If leaders are visibly penalized or forced to adhere to protocols, it would powerfully reinforce the organizational norm that security is a non-negotiable value, not just a procedural checklist for lower-level employees.
- Demand for Policy Simplification: There was an urgent demand for policies to be simplified and integrated into the workflow, rather than existing as lengthy, separate documents. The recommendation is to use visual aids, flowcharts, and clear, concise language to reduce the cognitive load associated with making secure choices.

4.8 Thematic Categorization

The thematic analysis revealed six (6) key themes in the table below (see table 4.2):

Table 4.2: Summary of Key Themes

Key Theme	Sub-Themes	Description	Example Response
Cybersecurity Awareness & Training	Awareness levels, training effectiveness, campaign participation	Examines the degree to which employees understand cybersecurity risks, how effective training programs are, and engagement with awareness campaigns.	"We receive cybersecurity training, but many still fall for phishing emails." (Response 2)
Cyber Threats & Risks	Phishing, ransomware, fake banking apps	Identifies the main cyber threats employees encounter, including the types, frequency, and perceived severity.	"Cybercriminals are using fake banking apps to steal customer data." (Response 14)
Cybersecurity Incidents & Response	Data breaches, phishing, malware infections	Captures the reported cybersecurity incidents and how organizations respond to them, including incident management and recovery.	"An employee clicked a malicious link, and it spread malware to the system." (Response 20)

Employee Compliance & Challenges	Password security, negligence, productivity concerns	Explores obstacles employees face in following security protocols, including attitudes and practical difficulties.	"Employees don't always take cybersecurity threats seriously." (Response 36)
Cybersecurity Policies & Regulations	Awareness, compliance issues, enforcement	Describes employees' knowledge of relevant regulations (e.g., UAE cybersecurity laws) and challenges in policy compliance and enforcement.	"I rely on our IT team for guidance on cybersecurity regulations." (Response 29)
Recommendations & Future Strategies	AI, policy improvements, incentives	Summarizes employee suggestions for improving cybersecurity posture, including technological, procedural, and cultural changes.	"Companies should reward employees for reporting security threats." (Response 46)

4.8.1 Cybersecurity Awareness & Training

Employees generally recognized the importance of cybersecurity awareness but reported uneven levels of understanding across different roles and departments. Senior and technical staff tended to have better grasp of cyber risks, while junior staff or those in non-IT roles often lacked detailed knowledge. Training programs were common but often perceived as too generic or infrequent to be fully effective. Some respondents expressed that training materials did not reflect real-world scenarios, reducing engagement and practical application. Additionally, participation in awareness campaigns varied, with some employees citing "training fatigue" or lack of incentives as reasons for low engagement. This theme underscores the need for tailored, ongoing, and interactive training that resonates with employees' daily tasks.

4.8.2 Cyber Threats & Risks

Phishing attacks emerged as the most pervasive threat, consistently mentioned across interviews and surveys. Employees reported sophisticated phishing emails and social engineering tactics that trick even vigilant users. Ransomware was also a significant concern, especially given its potential to halt operations and cause financial loss. Fake banking apps and fraudulent mobile applications were highlighted as emerging threats, particularly relevant for employees handling financial transactions or customer data. The dynamic and evolving nature of threats, such as the use of social media platforms to launch scams was emphasized, pointing to the need for continuous threat intelligence and adaptable defenses.

4.8.3 Cybersecurity Incidents & Response

Reported incidents frequently involved human error, such as clicking on malicious links, improper handling of attachments, or use of unsecured devices. While organizations had incident

response plans in place, employee narratives revealed varying degrees of incident awareness and timely reporting. Some employees noted that immediate containment actions—like isolating infected systems or resetting credentials—helped limit damage. However, there were also reports of delays due to unclear reporting channels or fear of repercussions. This theme highlights the importance of building a culture where employees feel responsible and empowered to act swiftly in the face of cybersecurity incidents.

4.8.4 Employee Compliance & Challenges

Despite understanding security policies, many employees admitted to non-compliance driven by convenience or workload pressures. Common issues included password reuse or sharing, bypassing multi-factor authentication, and ignoring software update prompts. Some employees rationalized these behaviors by prioritizing productivity, especially when security measures were perceived as cumbersome. Others expressed skepticism about the real-world impact of their compliance. These findings suggest that simply imposing rules is insufficient; organizations must balance security needs with usability and provide clear explanations of the risks associated with non-compliance.

4.8.5 Cybersecurity Policies & Regulations

Awareness of UAE-specific cybersecurity regulations varied considerably. While some employees were well-informed, most deferred regulatory knowledge to their IT or compliance departments. This reliance sometimes led to passive attitudes toward legal responsibilities and compliance monitoring. Employees expressed a desire for more accessible policy communication, including plain-language summaries and regular updates. The enforcement of policies was sometimes inconsistent, leading to confusion or lax practices. This theme indicates a

critical need for transparent, user-friendly regulatory education and consistent policy enforcement mechanisms.

4.8.6 Recommendations & Future Strategies

Employees offered diverse recommendations, often emphasizing the integration of advanced technologies like AI to detect and prevent threats in real-time. They suggested enhancements to existing policies, such as clearer guidelines and simplified protocols that reduce barriers to compliance. Many advocated for incentivizing employees through rewards or recognition programs to encourage proactive security behaviors, such as reporting suspicious activity. Additionally, collaboration between different stakeholders—IT teams, management, regulators, and employees—was viewed as essential for creating a resilient cybersecurity culture. Training improvements, including scenario-based simulations and gamification, were also recommended to boost engagement and retention of security knowledge.

4.9 Discussion

4.9.1 Human Behavior: The Core Vulnerability

The findings of this research affirm that human behavior continues to represent one of the most critical and persistent vulnerabilities in cybersecurity defense. Despite the implementation of sophisticated technical measures including advanced firewalls, intrusion detection systems, encryption protocols, and compliance frameworks, humans remain the weakest link in organizational security ecosystems. This vulnerability becomes particularly pronounced in high-risk sectors such as banking and finance, where the value of data and the complexity of digital interactions create fertile ground for exploitation.

Interviews and survey data collected in this study clearly illustrate that behavioral lapses ranging from clicking malicious links, falling for phishing scams, reusing or sharing passwords, and bypassing security protocols for convenience, are still widespread. These behaviors compromise even the most technically sound cybersecurity systems. This supports a long-standing recognition in the academic literature that user actions are a greater source of security incidents than system flaws (Crossler et al., 2013; D'Arcy & Greene, 2014). Moreover, the prevalence of these actions suggests that knowledge of risks does not reliably result in secure behavior: a phenomenon commonly referred to as the "knowledge–behavior gap" (Scott & Ophoff, 2018).

The issue is further exacerbated by the increasing sophistication of cyberattacks. For example, phishing attacks today often mimic official communications with alarming accuracy. Employees, even those with basic cybersecurity training, may find it difficult to distinguish between genuine and malicious communications particularly under time pressure or workload stress. These attacks are not only technical in nature but are deeply psychological, exploiting human trust, urgency, and inattentiveness. Social engineering tactics, such as pretexting and baiting, target employees' emotions, creating situations where rational decision-making is bypassed.

Adding to this complexity is the phenomenon of security fatigue, which was also reported by several respondents in this research. Employees indicated that constant security reminders, mandatory complex password rotations, and pop-up alerts created a sense of mental exhaustion, leading to disengagement and poor compliance. Security fatigue is a recognized condition in cybersecurity research, where users become overwhelmed and subsequently ignore critical security protocols (Jalali et al., 2020). This fatigue often leads to dangerous coping strategies, such as disabling software updates, recycling passwords, or blindly approving access requests.

Another key insight from the research is the misconception of responsibility. Many participants demonstrated a tendency to offload cybersecurity responsibility into IT departments, believing that securing systems was the sole domain of technical personnel. This is consistent with research by Uchendu et al. (2021), who observed that when cybersecurity is framed narrowly as a technical issue, employees become passive participants in digital safety. A successful organizational security posture, however, requires the cultivation of a shared responsibility model, where every employee, regardless of their role, recognizes their part in maintaining cyber hygiene.

The context of the UAE's rapidly digitizing banking sector adds urgency to this issue. The digital transformation goals outlined in the UAE Vision 2030 and Smart Dubai initiatives have accelerated the integration of technology into banking operations. While these efforts have enhanced service efficiency and customer experience, they have also increased exposure to cyber threats. Several respondents referenced incidents involving ransomware, fraudulent banking apps, and phishing campaigns that were tailored specifically to mimic local bank brands, demonstrating attackers' growing familiarity with regional platforms and vulnerabilities. According to de Bruin and Mersinas (2024), such targeted attacks are becoming more common in digitally advanced economies, where cybercriminals exploit not just technological weaknesses, but also human errors.

From an organizational perspective, there is often a lack of behavioral reinforcement mechanisms to convert knowledge into secure practices. While annual cybersecurity training is standard in many financial institutions, its effectiveness is questionable if not paired with continual reinforcement, engaging content, and immediate feedback. Parsons et al. (2015) highlight the importance of building an organizational security culture, a set of shared beliefs,

norms, and practices that promote cyber-aware behavior. A culture of security cannot rely on compliance alone; it must be embedded in daily practice, supported by leadership, and reinforced through social cues and recognition systems.

To combat these challenges, this study recommends a multi-layered approach to behavioral cybersecurity management:

1. Interactive and Continuous Training- Move beyond static e-learning by integrating real-world phishing simulations, gamified training, and scenario-based exercises that make learning dynamic and memorable (Bada et al., 2019).
2. Leadership Role Modeling- Executive teams and department heads must visibly adhere to cybersecurity policies and champion secure behavior, setting the tone for organizational norms.
3. Policy Simplification and UX Design- Organizations should re-evaluate their policies from the user perspective. Reducing unnecessary friction such as overcomplicated password requirements or redundant approvals can improve adherence.
4. Real-Time Feedback and Recognition- Employees should receive immediate feedback when risky behavior is detected (e.g., clicking a phishing link during a test), and those who demonstrate secure practices should be publicly recognized.
5. Embedding Shared Accountability- Cybersecurity should be incorporated into performance evaluations and team goals, emphasizing that it is a collective responsibility not just IT's job.

Human behavior is not merely a supplementary consideration in cybersecurity; it is the decisive factor in an organization's resilience against attacks. In the financial investment sector of Dubai, where the digital ecosystem is rapidly evolving, failure to address the human dimension of cybersecurity may undermine even the most advanced technical solutions. Cultivating a security-conscious workforce through culture, leadership, education, and design is therefore not optional, but essential.

4.9.2 Role-Based Awareness Disparities

The analysis revealed stark differences in cybersecurity awareness and compliance based on employee roles and seniority. Technical and senior staff consistently showed higher understanding, better compliance, and more proactive security behaviors, while junior and non-technical staff exhibited significant deficiencies. This echoes findings in cybersecurity research that show employees in IT-specific functions receive more targeted training and therefore exhibit stronger policy adherence than their non-technical colleagues (Bulgurcu, Çavuşoğlu, & Benbasat, 2010).

Bulgurcu et al. (2010) conducted a landmark study highlighting that employees' intention to comply with information security policies is strongly influenced by their perceptions of the policy's relevance to their job. Their findings suggest that generic or overly technical materials fail to satisfy non-technical staff, who do not internalize procedures that don't feel directly applicable to their tasks. During interviews, IT and senior personnel described receiving hands-on, regularly updated training focusing on emerging threats and secure configurations. Junior staff, however, reported only annual, compliance-driven modules or lengthy manuals with minimal contextual relevance.

This uneven training poses considerable risks in a digital banking environment, where employees across all job functions regularly interact with sensitive systems or data. One case involved a junior sales representative who, during a phishing simulation, clicked a spoofed internal portal link, immediately triggering alerts but also demonstrating how a single lapse can endanger customer information. Such real-world mishaps are preventable with role-based training that equips each staff category with relevant threat knowledge and response strategies. Industry guidance emphasizes that role-specific modules tailored to realistic scenarios significantly increased awareness retention (Techopedia, 2025). Research further supports this: Ani et al. (2019) and Pawlicka et al. (2022) stress that considering individual and situational factors (e.g., role, context, risk perception) enhances the impact of training interventions. Additionally, national-scale studies illustrate that organizational and cultural context influences security behaviors. de Bruin and Mersinas (2024) found that contextual variables like industry and organizational culture significantly shape employee susceptibility to cyber threats, implying training should be localized and tailored.

Non-technical staff often lack confidence and clarity about policy relevance. According to Bulgurcu et al. (2010), compliance is strongly linked to whether employees perceive policies as reasonable and applicable to their daily work. In line with these findings, many junior staff in this study viewed cybersecurity directives as burdensome or irrelevant to their roles treated as mere “IT department tasks,” rather than collective responsibility. To address such disparities, respondents suggested several interventions:

1. Customized E-Learning: Short, role-aligned modules that address typical threat scenarios faced by roles like tellers, loan officers, or administrative staff. These would use realistic

examples like detecting fraudulent transaction requests or safeguarding internal communications.

2. Scenario-Based Simulations: Regular phishing, vishing, and tailored abuse simulations designed to replicate real threats encountered in each role. Techopedia-quoted experts advocate integrating role-based simulations with micro-training and executive endorsement as best practice.

3. Peer-Led Workshops: Senior technical staff mentoring non-technical employees in informal sessions to share contextual insights and recent threat intelligence. This aligns with the "cybersecurity culture" model, which suggests embedding secure practices through peer influence and leadership (Bakewell et al., 2020).

4. Simplified Policies: Reformulating policies into clear, concise guidelines that explain "what to do" in everyday job scenarios, such as secure file-sharing protocols or authentication best practices.

This tiered approach mirrors role-based strategies recommended by both ThreatCop and SecurityCompass, which highlight the advantages of aligning training to job responsibilities, improving engagement, and reducing human-related risk (ThreatCop, 2025; SecurityCompass, 2025). Additionally, SANS Institute advises conducting human-centered risk assessments to determine which roles require specialized training interventions. Implementing role-based training also offers measurable performance gains. The 2024 Fortinet Security Awareness Report indicated that organizations focusing on high-risk employee groups and targeted training saw greater reduction in security incidents (Alger, 2024). Similarly, Ponemon Institute surveys report

a reduction of up to 70% in phishing success when ongoing, contextual training is applied systematically.

In contrast, static annual programs often fall short. Haney and Lutters (2021) demonstrate that "check-the-box" compliance training does not translate into behavioral change unless accompanied by real-world learning, ongoing engagement, and management support. Brightside's 2025 analysis further warns that one-size-fits-all training leads to disengagement and doesn't reflect real working conditions. Implementing these recommendations demands investment in instructional design, content localization, and user experience optimization. Organizations must ensure simulations and workshops foster a learning culture rather than being perceived as punitive. Additionally, training materials require regular updates to reflect new threats like AI-driven phishing or insider threats to remain relevant.

This research confirmed that role-based awareness training is essential for narrowing knowledge disparities across roles in digital banking environments. Generic, infrequent programs fail to reach employee segments most vulnerable to cyber threats. Tailored, engaging, and contextualized training highlighted by peer-led reinforcement and role-centric policies can significantly improve organizational security posture and resilience.

4.9.3 The Effectiveness (and Limitations) of Training Programs

Employees widely criticized current cybersecurity training programs as "boring," "repetitive," and detached from daily work, confirming that the typical "one-size-fits-all" approach is ineffective for driving behavioral change (Herath & Rao, 2009).

Passive Learning Fails

Traditional, compliance-driven training (static slides, annual modules) only achieves nominal compliance, with many employees admitting they "just go through the quiz to pass" and forget the content within weeks. This passive learning model fails because information dissemination alone is insufficient to alter long-term behavior (Bada et al., 2019).

Active Learning Succeeds

Modern, active learning models show significantly higher efficacy by engaging users emotionally and intellectually:

- Gamified E-Learning: Applying game elements (points, badges) substantially increases engagement and retention. Gamification fosters active participation and conversion of knowledge into secure habits, often outperforming traditional methods (York & deHaan, 2018).
- Simulation & Context: Training that provides immediate, role-relevant scenarios and just-in-time feedback (e.g., personalized phishing simulations with instant explanations) creates highly effective "teachable moments" that directly modify behavior (Burns et al., 2019).

Challenges to Implementation

Despite the promise of new methods, organizations face hurdles:

1. Cost and Design: Gamified and simulation programs require significant instructional design and platform investment.
2. Generic vs. Deep Learning: While new methods increase vigilance, they may not foster the deep analytical skills required for nuanced threat detection.

3. Training Fatigue: Overexposure to simulations or alerts can lead to user burnout, requiring a delicate balance in the training cadence.

To enhance effectiveness, organizations must shift from annual, passive models to a multi-modal, role-driven strategy that uses continuous micro-learning, simulation, and adaptive feedback to sustain awareness.

4.9.4 Compliance vs. Usability: A Delicate Balance

A pervasive theme in the study is the inherent tension between stringent security compliance and user convenience. Although employees recognize the value of security, many deliberately bypass controls to maintain workflow efficiency.

The Usability-Driven Noncompliance

This behavior exemplified by employees ignoring security prompts, saving codes in Notepad, or sharing passwords is rooted in the fact that users prioritize speed and task completion above all else (Workman et al., 2008).

- Evidence: When security controls (like frequent MFA requests or complex password changes) are perceived as overly demanding, cumbersome, or misaligned with workflow, they generate resistance and trigger a search for workarounds.
- Psychological Toll: Excessive security friction creates cognitive overload, leading to "automation bias," where users develop habitual, insecure bypass techniques (Beautement et al., 2008). Non-compliance becomes a normalized social practice that reduces overall organizational security.

User-Centered Security as the Solution

Reconciling this tension requires a fundamental shift toward user-centered security design, where protection is intuitively embedded in daily tasks (Coventry et al., 2014).

- Design Recommendations: Strategies like implementing Single Sign-On (SSO), using adaptive Multi-Factor Authentication (MFA) that only triggers in high-risk scenarios, and deploying user-friendly password managers reduce cognitive load and password fatigue without sacrificing protection.
- Cultural Context: The solution is not just technical; it's cultural. Transparent communication explaining why a control exists and strong leadership modeling of secure behavior are necessary to ensure employees view compliance as a collective responsibility, not a bureaucratic imposition (Coventry et al., 2014).

The experience of one regional bank, which saw a 74% reduction in password resets after deploying SSO, demonstrates that usability-conscious security can effectively eliminate friction while maintaining high security standards.

4.9.5 Policy Awareness and the Role of IT Dependency

A concerning finding was the limited policy awareness and subsequent over-reliance on IT among non-technical staff regarding UAE cybersecurity regulations. Many employees incorrectly view compliance as the sole responsibility of the IT department, demonstrating a critical policy awareness gap.

The Risk of Outsourcing Compliance

This common delegation of responsibility to IT introduces significant organizational risks:

- Unacknowledged Non-Compliance: Non-technical staff may inadvertently ignore essential protocols (like secure data handling or incident reporting mandates) because they assume "If IT hasn't flagged it, it's okay."
- Overburdened IT: The IT department has become a de facto policy gatekeeper, increasing burnout and diverting resources away from strategic security management.
- Weak Security Culture: When regulation is outsourced, non-technical employees fail to internalize a compliance mindset, viewing cybersecurity as a compartmentalized technical domain rather than a shared organizational objective (Al-Kuwaiti & Al-Salman, 2020).

Bridging the Gap: Inclusive Policy Communication

To overcome this IT dependency, policy dissemination must become inclusive, user-friendly, and multi-channel:

1. Plain Language and Visuals: Regulations must be translated into user-friendly formats like infographics, flowcharts, and FAQs to demystify obligations.
2. Micro-Learning and Context: Instead of annual training, short, targeted micro-learning modules should reinforce policy knowledge, tailored to specific departmental roles (Uchendu et al., 2021).
3. Active Engagement: Organizations must implement policy feedback loops and host interactive workshops where staff discuss how regulations apply to their daily tasks, fostering ownership.

Ultimately, bridging this gap requires a cultural shift where visible leadership modeling and accountability mechanisms reinforce that every employee, regardless of role, is a custodian of organizational cybersecurity.

4.9.6 Cultural Integration: Toward a Cybersecurity Mindset

The data strongly advocates for transforming cybersecurity from a technical task owned by IT into a shared, internalized organizational mindset. Lasting resilience is built on culture, where secure behavior is a normalized, collective habit, not just a response to compliance rules (Alshaikh, 2020; Zaidi et al., 2020).

The Shift from Compliance to Culture

The critical difference is that compliance is what employees do because they must, while culture is what employees do because they have internalized it as their own value. This psychological shift from "IT told me to do this" to "I do this because it protects us all" is necessary for resilience.

Key Enablers of Cultural Change

Cultural change is driven not by documentation, but by visible, trusted influences:

1. Leadership Modeling: Visible sponsorship from senior executives is crucial. When leaders visibly adhere to secure practices (e.g., using MFA), it validates security as a strategic, non-negotiable value (Tawiah et al., 2021). Without this modeling, efforts fail against daily pressures.
2. Champion Networks: Establishing a network of non-technical champions and respected peers across departments creates a peer-to-peer influence bridge between IT and the rest

of the organization. Champions normalize secure behavior and are trusted sources of information.

3. Cultural Framing: Focusing security messaging on a handful of relatable, core behaviors (e.g., "verify identity before clicking") and giving the security function an approachable brand identity helps emotionally anchor security into workplace life (Alshaikh, 2020).

Strategies for Integration and Sustained Impact

Effective strategies for cultural embedding, supported by both the literature and respondent insights, include:

- Behavioral Reinforcement: Introduce inclusive workshops to discuss security near-misses openly and recognize/reward individuals who proactively report threats, fostering a "zero-blame" learning environment.
- Integration Metrics: Move beyond simple training completion rates. Integrate metrics like incident reporting frequency and champion engagement into performance reviews to ensure security becomes an organizational habit.

Research confirms that cultures driven by shared responsibility experience fewer insider incidents and achieve faster recovery, proving that culture-based interventions outperform mere information campaigns.

4.9.7 Emerging Threats and Technological Adaptation

The cybersecurity threat landscape is fundamentally changing due to the integration of Artificial Intelligence (AI). Threat actors are rapidly leveraging generative AI to launch more

sophisticated, personalized, and deceptive attacks, posing a significant challenge to the human element.

AI-Driven Threats: Sophistication and Scale

Participants observed an increase in the sophistication of attacks, reporting phishing emails that are alarmingly convincing and warning of synthesized audio and video impersonations (deepfakes).

- Generative Attacks: These observations align with global trends showing cybercriminals using AI and Machine Learning (ML) to craft personalized, automated campaigns that bypass traditional filters (Jonas et al., 2023; Mustaphaa et al., 2024). Incidents, such as the rise of AI-generated phishing in certain regions, demonstrate that AI drastically lowers the skill floor for attackers, facilitating large-scale, hyper-targeted campaigns.
- Deepfakes: Beyond text, deepfake tools can mimic voice and video with startling accuracy. Experts warn that traditional security training does not adequately prepare organizations for these forms of social engineering, necessitating layered defenses (Pedersen et al., 2025).

Defenders Fight Back: AI in Cybersecurity

In response, participants expressed strong support for integrating AI into corporate defense systems.

- AI as Augmentation: AI is valued for its ability to provide real-time anomaly detection, behavioral analytics, and faster incident response (Ng et al., 2019). It processes

voluminous network traffic more efficiently than human analysts, flagging emerging threats and automating routine tasks to augment human teams (Ansari et al., 2022).

- Hybrid Vision: Despite its promise, there is consensus that AI must augment rather than replace human decision-making. The advocated model is a "human-in-the-loop" system where AI identifies and flags threats, but skilled human analysts validate, govern, and direct the final response.

Organizational Challenges and Mitigation

Effective AI deployment is hindered by organizational and ethical challenges.

- Challenges: Identified hurdles include skill shortages in AI/ML expertise, the necessity for high data quality, the "black-box" nature of some models impeding trust and compliance, and adversarial risks where attackers target the AI systems themselves (Oseni et al., 2021; Brundage et al., 2018).
- Mitigation: Mitigation strategies focus on strategic investment in talent and training, establishing robust governance frameworks for AI ethics, adopting interpretable AI tools, and conducting red-teaming exercises to test resilience.

The future cybersecurity paradigm demands a balanced approach where organizational readiness, policy governance, and human expertise are integrated with powerful, yet responsibly managed, intelligent technologies.

4.9.7 Emerging Threats and Technological Adaptation

The cybersecurity paradigm is rapidly transforming due to the integration of Artificial Intelligence (AI), which is fundamentally changing both the offense and defense sides of the security equation.

AI-Driven Threats: Increased Sophistication and Scale

Participants noted a significant increase in the sophistication of attacks, reporting highly convincing phishing emails and warning of synthesized audio and video impersonations (deepfakes).

- Generative Attacks: Cybercriminals are increasingly using AI and Machine Learning (ML) to craft personalized, automated campaigns that bypass traditional filters and lower the skill floor for attackers (Jonas et al., 2023; Mustaphaa et al., 2024). This shift allows for hyper-targeted, large-scale attacks.
- Need for New Defenses: The rise of deepfakes and advanced social engineering necessitates security training that moves beyond text-based awareness to prepare organizations for voice and video impersonation attacks (Pedersen et al., 2025).

Defenders Fight Back: AI as Augmentation

Respondents strongly favored integrating AI into corporate defense systems, recognizing its potential to compensate for human limitations.

- Real-Time Capabilities: AI is valued for its ability to provide real-time anomaly detection, behavioral analytics, and faster incident response (Ng et al., 2019). It processes network traffic far more efficiently than human analysts, flagging emerging threats and automating routine tasks (Ansari et al., 2022).

- Hybrid Vision: The consensus is that AI must augment rather than replace human decision-making. The preferred model is a "human-in-the-loop" system where AI identifies and flags threats, but skilled human analysts validate, govern, and direct the final response, ensuring ethical oversight and accuracy.

Organizational Challenges and Governance

Effective AI deployment is hindered by significant organizational and ethical challenges that require careful governance.

- Challenges: Hurdles include skill shortages in AI/ML expertise, the need for high data quality, the "black-box" nature of some models, and the risk of adversarial attacks targeting the AI systems themselves (Oseni et al., 2021; Brundage et al., 2018).
- Mitigation: To succeed, organizations must commit to strategic investment in talent and training, establish robust governance frameworks for AI ethics, adopt interpretable AI tools, and conduct red-teaming exercises that test resilience against model-targeted attacks.

The future of cybersecurity demands a balanced approach where organizational readiness, policy governance, and human expertise are integrated with powerful, yet responsibly managed, intelligent technologies.

4.9.9 Theoretical Integration

This section briefly integrates the research findings with three key behavioral and technological frameworks, which provide essential theoretical lenses for interpreting the

psychological and organizational dynamics influencing security behavior in the UAE's financial sector.

1. Protection Motivation Theory (PMT)

PMT posits that protective behavior is driven by two assessments: threat appraisal (severity and likelihood of a threat) and coping appraisal (effectiveness of the protective action and one's self-efficacy to perform it) (Rogers, 1975).

- Application: The study's finding that employees exhibit low perceived vulnerability (believing cyber threats are "too distant" to concern them) is a classic PMT inhibitor. Low perceived threat, combined with low self-efficacy regarding complex security tools, explains why awareness campaigns often fail: they don't adequately increase motivation or confidence (Parsons et al., 2017).

2. Technology Acceptance Model (TAM)

TAM states that a person's acceptance of new technology is primarily determined by perceived usefulness and perceived ease of use (Davis, 1989).

- Application: Participants' complaints that security tools (MFA, VPNs) are "clunky" or "too disruptive" directly reflect a failure in TAM's perceived ease of use. This inconvenience leads to employees actively bypassing controls (e.g., saving credentials), demonstrating that poor usability undermines adoption even when perceived usefulness is high. Improving the user experience of security systems is critical to enhancing acceptance and adherence (Fallatah, 2024).

3. Theory of Planned Behavior (TPB)

TPB expands on behavioral models by incorporating subjective norms (perceived expectations from others) and perceived behavioral control (confidence and ability to perform the action) alongside attitude (Ajzen, 1991).

- Application: TPB helps explain why management's actions matter. Employees' security behavior was heavily influenced by office norms; if team leaders openly used weak passwords, subordinates followed suit, demonstrating the power of subjective norms over personal attitude (Apau & Koranteng, 2019). Furthermore, employees who reported a lack of support (low perceived behavioral control) were more likely to disengage. TPB thus highlights the necessity of leadership modeling and structural support to build secure organizational norms.

Synthesis and Practical Application

These theories converge to explain the persistent intention–action gap. Employees fail to act securely due to low threat perception (PMT), poor usability (TAM), and lack of social reinforcement (TPB). Addressing these gaps requires a holistic strategy that focuses on increasing threat salience, ensuring system usability, and building a culture of security through strong leadership and peer reinforcement.

4.10 Chapter-end Summary

This research investigated the intersection of employee behavior, policy, and technology in the cybersecurity framework of the UAE banking sector. While significant investments have enhanced infrastructure and theoretical awareness, the findings consistently reveal that human, organizational, and systemic challenges fundamentally hinder full cyber resilience.

The key takeaways from the research are:

1. The Intention-Action Gap Persists: Cybersecurity awareness is improving, but it remains inconsistent and behavioral. Employees often treat training as a "check-the-box" exercise, prioritizing convenience and speed over secure practices. The core problem is not a deficit of knowledge, but a failure to translate knowledge into sustained, practical action, particularly among non-technical staff.

2. The Human Element is the Primary Threat Vector: Employees consistently identified phishing and social engineering as the most prevalent and concerning threats. These attacks exploit human error, cognitive biases, and lapses in vigilance to successfully bypass advanced technological defenses. This underscores that human behavior is the critical vulnerability in asset protection.

3. Policy and Training Effectiveness are Undermined by Design: Formal training is widely perceived as generic, repetitive, and unengaging. Furthermore, complex or inconvenient security procedures (e.g., multifactor authentication across multiple platforms) often lead employees to create insecure workarounds, reflecting a fundamental issue of poor usability and policy design.

4. Resilience Requires Cultural and Policy Reform: Respondents highlighted the need for stricter, more consistent policy enforcement and clear escalation procedures. They recommended closer collaboration between banks and government regulators to develop responsive, unified frameworks that reflect the dynamic threat landscape.

5. Future Strategy Must Integrate Behavior and AI: There is strong support for integrating Artificial Intelligence (AI) into defense systems for real-time threat detection and

anomaly recognition, compensating for human limitations. Crucially, this must be paired with incentive-based strategies, such as rewarding employees for reporting threats, to foster a culture where security is a shared and rewarded embedded norm.

In conclusion, achieving cyber resilience requires a holistic approach that moves beyond reactive compliance. Organizations must create structural and cultural conditions that make secure behavior intuitive, incentivized, and fully integrated into daily workflows, leveraging intelligent technologies to support, not replace, human oversight.

CHAPTER 5: CONCLUSION, RECOMMENDATIONS, AND IMPLICATIONS FOR FURTHER RESEARCH

5.1 Conclusion

The purpose of this research was to examine and enhance cybersecurity awareness in the United Arab Emirates (UAE), with a particular focus on strategies aimed at mitigating cyber threats and protecting critical digital assets. In a world where digital innovation increasingly underpins government operations, economic infrastructure, and social interactions, cybersecurity has emerged as a foundational component of national resilience and trust. As the UAE advances ambitious digital transformation strategies such as UAE Vision 2031, National Artificial Intelligence Strategy 2031, and the Smart Government Initiative, the scope and severity of cyber threats grow in tandem. The urgency of enhancing public and private sector cyber readiness has therefore never been greater.

The findings emphasized that cybersecurity is not only a technical concern but a socio-organizational challenge that hinges upon human awareness, behavior, and systemic integration. While the UAE has demonstrated leadership in adopting national cybersecurity strategies, including the establishment of the National Cybersecurity Council and sector-specific mandates (UAE Cybersecurity Council, 2020), gaps in end-user awareness, policy execution, and practical engagement persist. Respondents in the study displayed varying degrees of familiarity with cyber threats such as phishing, malware, ransomware, and social engineering. However, while theoretical knowledge was moderately high, practical applications such as password management, incident reporting, and device hygiene were often lacking. These findings align with previous studies indicating that knowledge alone does not guarantee behavior change unless reinforced through sustained training and cultural reinforcement (Parsons et al., 2017; Sasse et al., 2016).

One critical insight from this research is the pervasive gap between national-level cybersecurity policy and on-the-ground organizational implementation. For instance, while federal guidelines may require two-factor authentication or periodic security audits, many SMEs and even mid-size public organizations fail to comply due to lack of resources, awareness, or leadership support. This is particularly concerning given that SMEs constitute over 94% of the

UAE's private sector (Ministry of Economy, UAE, 2022), making them a vital yet vulnerable component of national cyber defense.

Cybersecurity awareness is also deeply influenced by organizational culture. The research found that top-down communication often fails to resonate with end-users unless paired with relatable narratives, interactive training methods, and peer reinforcement. Leaders who champion cybersecurity values and model secure behavior are more likely to create lasting cultural shifts than those who rely solely on compliance-based training (Ifinedo, 2014). Thus, cybersecurity must be integrated into performance management, leadership development, and employee onboarding processes.

The research also highlighted the increasing relevance of advanced technologies such as artificial intelligence (AI), cloud computing, and the Internet of Things (IoT). These innovations introduce new vectors for attacks, requiring users to understand not just traditional risks, but emerging ones such as AI bias, cloud misconfigurations, and IoT firmware vulnerabilities (Taddeo & Floridi, 2018). Unfortunately, most cybersecurity awareness programs remain too static, failing to adapt to the changing threat landscape.

Governmental efforts in the UAE are commendable, including public education campaigns, cybersecurity competitions, and capacity-building grants. However, implementation remains fragmented. This is especially evident in remote working contexts accelerated by the COVID-19 pandemic, where cybersecurity training has not kept pace with new working models (Al-Sharafi et al., 2021). As employees increasingly work from home using personal devices, new policies must address the convergence of domestic and professional risk.

This research also explored the psychological and social dimensions of cybersecurity awareness. Many users reported not engaging with security warnings due to "alert fatigue," perceived complexity, or lack of trust in IT departments. These findings point to the need for a user-centric approach that emphasizes simplicity, transparency, and trust-building. Research has shown that fear-based campaigns are less effective than those promoting self-efficacy and communal responsibility (Rogers, 1975; Witte & Allen, 2000).

In summary, this research confirms that enhancing cybersecurity awareness in the UAE is both urgent and multifaceted. It requires more than issuing technical directives or implementing

defensive technologies. Instead, it demands a strategic, cross-sectoral commitment to cultivating informed, engaged, and proactive digital citizens. This involves national policy harmonization, industry-specific awareness programs, leadership development, inclusive education, and investment in research and innovation. By bridging the gap between awareness and action, aligning national strategy with organizational execution, and integrating user behavior with evolving technological realities, the UAE can move closer to its vision of becoming a global leader in cybersecurity resilience. The implications of this research underscore the necessity of a coordinated, evidence-based approach to cybersecurity, one that respects cultural diversity, adapts to technological evolution, and empowers all segments of society to participate in safeguarding digital prosperity.

5.2 Recommendations

The cybersecurity model is complicated and perpetually evolving. Threat actors deploy increasingly sophisticated tactics, vulnerabilities proliferate, and digital transformation amplifies organizational risk. In this context, building defensive capabilities across public, private, and civil society sectors demands a multi-dimensional approach. The research's core finding is a significant gap between cybersecurity policy and employee behavior, characterized by generic training, weak enforcement, and convenience-driven workarounds. The following recommendations are tiered to address these challenges strategically.

5.2.1 Short-Term Actions (Immediate Vulnerability Mitigation)

These actions target immediate behavioral risks and policy loopholes identified within the UAE's banking sector.

Table 5.1: Short Term Recommendations

Recommendation	Finding Link & Justification	Supporting Evidence (APA)
Implement Role-Based Microlearning. Replace generic, annual training	Training is perceived as irrelevant and infrequent, leading to low retention and	Focusing on role-relevance is critical for improving both knowledge retention and

(which causes "training fatigue") with frequent, role-specific, and short modules.	engagement. This change ensures information is immediately applicable to job functions.	motivation to apply security policies (Turk et. al., 2022).
Conduct Contextual Phishing and Social Engineering Simulations. Use real-time feedback and highly sophisticated simulations to increase the perceived threat salience and test staff response in live scenarios.	Phishing and social engineering attacks were the most pervasive threats reported, successfully exploiting human trust and curiosity.	Simulations that provide immediate feedback and are contextualized have proven highly effective in reducing click-through rates and increasing vigilance (Hijji & Alam, 2022).
Simplify and Centralize Policy Access. Reformulate complex security policies into concise, accessible, and user-friendly guidelines (e.g., flowcharts, simple language).	Policies are often perceived as complex, ambiguous, and detached from daily operational reality, contributing to deliberate non-compliance.	Simplifying policy language and ensuring usability dramatically enhances practical application and compliance rates, aligning security with user workflow (National Institute of Standards and Technology, 2018).

5.2.2 Medium-Term Actions (Organizational Culture and Process Integration)

These actions are designed to embed security into the corporate culture and operational processes, leveraging behavioral theories (e.g., Theory of Planned Behavior).

Table 5.2: Medium-Term Recommendations

Recommendation	Finding Link & Justification	Supporting Evidence (APA)

Mandate Leadership Modeling and Accountability. Require senior executives and managers to visibly adhere to all security protocols and implement clear, communicated disciplinary measures for policy circumvention.	Lack of leadership modeling and weak, inconsistent enforcement erode trust and create an organizational norm where security rules are treated as optional.	Organizational culture is the most significant factor in security behavior. Visible commitment from leadership is crucial for setting positive security norms (Vance et al., 2018).
Incentivize Secure Behavior. Develop and implement reward systems (e.g., non-monetary recognition, gamification) for employees who proactively report threats or demonstrate exceptional security hygiene.	Employees lack emotional engagement or motivation for security practices, often seeing it as an organizational imposition rather than a shared goal.	Recognizing and rewarding positive security behavior utilizes reinforcement theory to transform security from a mandatory task into a valued, embedded social norm (Williams et. al., 2024).
Integrate AI/ML for Real-Time Threat Response. Organizations should invest in Artificial Intelligence and Machine Learning tools for continuous monitoring of user behavior to detect anomalies and compensate for human oversight.	Human negligence and the sheer volume of evolving threats necessitate tools that can autonomously detect and respond to threats faster than human teams can.	AI/ML complements human awareness by providing a predictive layer of defense, moving organizations toward a proactive, adaptive security architecture (Ogunbodede, Adewale & Alese, 2024).

5.2.3 Long-Term Actions (National, Systemic, and Policy Reform)

These recommendations require national coordination and address the structural gaps in the UAE's digital ecosystem.

Table 5.3: Long-Term Recommendations

Recommendation	Finding Link & Justification	Supporting Evidence (APA)
Embed Cybersecurity Literacy in the National Curriculum. Integrate foundational cybersecurity education into schools, vocational institutes, and universities across all levels.	There is a critical shortage of skilled cybersecurity professionals and low foundational public awareness, limiting national resilience.	Early education is key to fostering a culture of "security by design" in the next generation of innovators and consumers, supporting the UAE Vision 2071 (National Cybersecurity Council, 2024).
Develop Sector-Specific Regulatory Frameworks. The UAE Cyber Security Council must collaborate with high-risk sectors (e.g., Finance, Energy) to establish customized frameworks that address unique risk profiles.	General national frameworks fail to address the nuanced risk profiles and stringent compliance pressures of distinct, highly-regulated industries like banking.	Tailoring regulations ensures that security measures are proportionate, relevant, and effective, maximizing resource allocation and reducing unnecessary compliance burdens (Luidold & Jungbauer, 2024).
Establish a National Cyber Simulation and Coordination Center. Conduct mandatory, large-scale, joint cyber exercises involving	Participants consistently recommended improving coordination and intelligence sharing to ensure a unified	National-level drills foster "muscle memory" and ensure clarity of roles and communication pathways during a national crisis, which

government regulators, national infrastructure entities, and the private sector.	national response to large-scale threats.	is essential for systemic resilience (Schneier, 2202).

5.3 Implications for Further Research

The findings of this research lay the groundwork for a range of research initiatives that can further clarify the challenges, and opportunities in enhancing cybersecurity awareness in the United Arab Emirates (UAE). As digital transformation accelerates across public and private sectors, understanding the behavioral, technical, institutional, and cultural dimensions of cybersecurity becomes ever more essential.

Below are ten key research avenues that warrant further exploration, each offering unique potential to contribute to national resilience and regional leadership in cybersecurity:

5.3.1 Longitudinal Studies on Behavior Change

One of the most significant gaps in the current body of literature on cybersecurity awareness is the lack of longitudinal data. Most studies provide snapshots of user behavior or awareness at a single point in time, often shortly after an intervention such as training. However, cybersecurity is not a one-time event but a continuous process that depends heavily on sustained behavioral change.

Future research should examine how awareness campaigns and cybersecurity training programs influence employee behavior over time, particularly in sectors with elevated risk exposure—such as finance, healthcare, oil and gas, and government. Such studies could track employee compliance with cybersecurity policies, reporting of phishing attempts, password hygiene, and device use policies over months or even years. This would help organizations in the UAE determine whether their investments in awareness campaigns result in lasting improvements, or whether periodic retraining and reinforcement are necessary.

Longitudinal research could also explore whether digital natives entering the workforce exhibit different cybersecurity behaviors compared to older cohorts, and how those patterns evolve with experience and organizational culture.

5.3.2 Comparative Studies Across GCC Nations

While the UAE has made significant strides in developing national cybersecurity strategies and fostering awareness, it operates within a broader Gulf Cooperation Council (GCC) context. Countries like Saudi Arabia, Qatar, Kuwait, Bahrain, and Oman face similar cyber threats, including state-sponsored attacks, ransomware, and data breaches targeting critical infrastructure. Comparative studies between GCC nations could reveal variations in public policy, education programs, private sector engagement, and technological investments. Such comparative analyses may help identify regional best practices, collaborative initiatives, and opportunities for joint cyber drills, research, and intelligence sharing.

Furthermore, comparative studies could explore the sociopolitical dimensions of cybersecurity. For instance, how do different governance models influence national cyber readiness? How do public-private partnerships vary across the GCC, and what can be learned from these differences?

5.3.3 Cybersecurity and Remote Work Trends

The global shift toward hybrid and remote work, accelerated by the COVID-19 pandemic, has fundamentally altered the cybersecurity landscape. In the UAE, this transformation has led to increased dependence on digital collaboration platforms, personal devices, and cloud-based storage systems. While remote work enables flexibility and continuity, it also introduces unique vulnerabilities including unsecured home networks, shared family devices, and blurred boundaries between personal and professional use.

Future research should investigate the implications of remote work on cybersecurity practices, particularly in UAE-based organizations. Questions worth exploring include:

- Are remote workers more susceptible to phishing or social engineering attacks?
- How do organizations enforce endpoint security and data protection in remote settings?

- What policies and technologies are most effective in balancing productivity with security?

This line of research could also explore the mental models and risk perceptions of remote employees and how these affect their cybersecurity behavior outside traditional office controls.

5.3.4 Psychological and Sociological Perspectives

Cybersecurity is often framed as a technical challenge, but it is equally a human one. Understanding why individuals engage in risky behavior online, despite training or awareness is critical for designing interventions that work.

Psychological and sociological research could delve into issues such as:

- Risk perception and denial ("It won't happen to me" thinking)
- Habit formation and digital fatigue
- The role of trust in information sources and digital tools
- Social norms that influence acceptable behavior in the workplace

Using methodologies from behavioral economics, cognitive psychology, or social psychology, future studies could examine how these factors influence real-world cybersecurity decisions. For example, do users ignore two-factor authentication (2FA) because they perceive it as inconvenient, or because they underestimate the risk of compromise? What messaging strategies are most effective at changing behavior? The UAE's multicultural and diverse workforce also offers fertile ground for examining how different cultural backgrounds influence perceptions and responses to cybersecurity threats.

5.3.5 AI Ethics and Cybersecurity Decision-Making

The integration of artificial intelligence (AI) and machine learning (ML) into cybersecurity operations brings immense benefits but also raises significant ethical and operational questions. As UAE organizations increasingly adopt AI-powered threat detection, intrusion prevention, and identity management systems, the human-AI interface becomes a critical area for study.

Future research could address questions such as:

- How do employees and decision-makers trust AI-driven recommendations in cybersecurity contexts?
- What biases may exist in AI models used for detecting threats, and how can these be mitigated?
- What are the ethical implications of automated decision-making in scenarios like employee monitoring or access revocation?

This area of research is especially relevant given the UAE's national AI strategy and its goal of becoming a global leader in ethical AI governance. Studies could inform policy development and risk assessment models that govern the use of intelligent cybersecurity systems.

5.3.6 Cybersecurity in SMEs and Startups

Small and medium enterprises (SMEs) make up a significant portion of the UAE's economy, especially in free zones and innovation hubs. However, these businesses often lack the resources, expertise, and personnel to implement robust cybersecurity measures.

Future studies could examine:

- What cost-effective cybersecurity tools and strategies can SMEs adopt?
- How can government incentives or shared services help bridge resource gaps?
- What awareness gaps exist among startup founders and early-stage teams?

Such research could result in practical toolkits, training programs, or cybersecurity-as-a-service models specifically tailored to the needs of UAE-based SMEs. It could also explore how entrepreneurial attitudes such as risk-taking or lean thinking impact cybersecurity decision-making.

5.3.7 Gender and Cultural Influences on Awareness

The UAE is home to a highly diverse workforce comprising numerous nationalities, cultures, and languages. Additionally, gender roles in professional and digital life vary widely across these demographic groups. These variables can influence everything from communication styles to risk tolerance and training effectiveness.

Future research should examine:

- How do cultural values affect the perception of cyber risk?
- Is there gender-based differences in awareness, behavior, or engagement with cybersecurity programs?
- How can training programs be designed to be culturally inclusive and gender-sensitive?

The inclusion of these dimensions can lead to more equitable and effective awareness initiatives and ensure that cybersecurity becomes embedded in the national culture, reaching all segments of the population, regardless of background.

5.3.8 Cybersecurity Metrics and ROI

Despite increasing investment in cybersecurity awareness and infrastructure, measuring the return on that investment remains a major challenge for organizations. Future research should focus on creating and validating reliable metrics that link awareness initiatives to outcomes such as:

- Reduced incidence of phishing or malware infections
- Faster incident detection and response times
- Increased reporting of suspicious behavior

Research could also explore the economic impact of breaches that occur despite awareness programs, helping organizations fine-tune their investment strategies. Are certain types of training more cost-effective than others? What is the cost-benefit of continuous micro-training versus annual workshops?

5.3.9 Blockchain and Cybersecurity

Blockchain has been widely discussed for its potential to enhance cybersecurity by providing decentralized, tamper-evident transaction records. However, real-world applications and limitations remain under-explored.

Future studies could explore:

- The use of blockchain in identity verification, especially in e-government or e-voting systems
- How blockchain can secure supply chains and digital contracts
- The risks and vulnerabilities in smart contracts or decentralized apps (dApps)

The UAE, with its proactive blockchain strategy and multiple government-led blockchain pilots, is well positioned to pioneer research in this area.

5.3.10 Public Sector Cyber Resilience

The public sector plays a pivotal role in the UAE's cybersecurity model, not just in regulation, but also in protecting critical infrastructure and citizen data. However, public entities may face unique constraints, including legacy systems, complex procurement processes, and workforce limitations.

Future research could include case studies of successful (and unsuccessful) cybersecurity initiatives in the public sector, focusing on:

- Inter-agency collaboration and information sharing
- Integration of cybersecurity into digital government platforms
- Crisis response coordination between federal and emirate-level agencies

Such research could help develop a national cyber resilience framework tailored to the UAE's administrative structure and strategic objectives.

5.4 Research Contribution

This research offers a multifaceted contribution to both academic knowledge and practical applications in cybersecurity, with a specific focus on the United Arab Emirates (UAE). In an era where digital transformation is accelerating across all sectors, the importance of cybersecurity awareness and preparedness cannot be overstated. This research provides timely, contextually grounded insights that enhance our understanding of how cybersecurity is perceived, implemented, and internalized within organizations and among individuals in the

UAE. Its contributions span theoretical development, empirical insights, practical policy recommendations, and regional contextualization.

5.4.1 Contribution to Academic Knowledge

From an academic perspective, this research contributes significantly to the growing literature on cybersecurity awareness, training, and behavioral responses in the digital age. While global studies on cybersecurity abound, the Middle Eastern context, particularly the UAE remains underrepresented in scholarly research. This research bridges that gap by offering region-specific analysis supported by empirical data, thereby contributing to a more inclusive and diversified academic discourse on global cybersecurity.

Furthermore, the research integrates interdisciplinary concepts from information security, behavioral science, strategic management, and education to construct a holistic understanding of cybersecurity awareness. It moves beyond a purely technical approach to encompass psychological, cultural, and organizational dimensions of cyber risk. This broad conceptualization enriches theoretical frameworks that can be used in future studies across similarly diverse socio-technical domains.

The research also proposes a multi-tiered analytical framework that connects individual awareness, organizational culture, and national-level policy as interdependent elements of cybersecurity resilience. By highlighting the importance of alignment across these tiers, the research presents a comprehensive model for cybersecurity preparedness that future scholars can adopt or refine. This integrative approach adds theoretical value to the field and offers a blueprint for cross-sector analysis in other emerging economies.

5.4.2 Empirical Contribution

This research is grounded in original data collected from a diverse pool of respondents representing various sectors in the UAE, including government agencies, financial institutions, healthcare providers, and SMEs. By incorporating both qualitative and quantitative data, the research provides a nuanced picture of the current state of cybersecurity awareness and behavior in the country.

The empirical findings shed light on how individuals perceive cyber threats, the extent to which they engage in secure practices, and the organizational structures that either support or hinder cybersecurity readiness. Importantly, the research surfaces sector-specific vulnerabilities and challenges, such as differing levels of cyber maturity, resource constraints in SMEs, and the influence of remote work on cyber hygiene. These findings offer actionable insights for organizational leaders and policymakers aiming to close these gaps.

Additionally, the research reveals trends that are not immediately observable through secondary data sources alone, such as employees' emotional responses to cybersecurity training, their trust in digital tools, and the informal workarounds they adopt. These micro-level insights contribute to a richer understanding of cybersecurity as a lived experience, which is often overlooked in more technologically focused studies.

5.4.3 Practical Contribution

Beyond its theoretical and empirical impact, this research delivers practical recommendations with immediate relevance to organizational decision-makers, educators, and government authorities. The research outlines strategic actions that can be implemented to strengthen cybersecurity awareness and readiness at multiple levels. These include designing targeted training programs, establishing cybersecurity-first organizational cultures, investing in public awareness campaigns, and enhancing regulatory frameworks.

A notable contribution is the delivery of sector-specific strategies tailored to the unique operational contexts and threat landscapes of industries such as finance, healthcare, and critical infrastructure. This level of detail supports more effective implementation of cybersecurity measures and reduces the risk of adopting one-size-fits-all solutions that may not be fit for purpose.

The research also contributes to the national cybersecurity agenda of the UAE by aligning its recommendations with the goals of the UAE National Cybersecurity Strategy. It supports the country's efforts to build a digitally secure society and economy, capable of withstanding both current and future cyber threats. By doing so, the research contributes to the development of resilient institutions that underpin national digital transformation and economic diversification

efforts, including initiatives under UAE Vision 2031 and the broader Middle East digital economy frameworks.

5.4.4 Contribution to Academic Debates

This research significantly advances the theoretical discourse on cybersecurity awareness by addressing major theoretical and empirical gaps, thereby enriching the global academic conversation.

- Region-Specific Empirical Evidence: This research provides original, region-specific empirical analysis for the UAE and the Middle Eastern context, a domain that is critically underrepresented in global cybersecurity studies (Reeves, Delfabbro & Calic, 2021). This evidence directly challenges the presumed universality of many security models developed in Western contexts, contributing to a more inclusive and diversified scholarly discourse.

- Interdisciplinary Theoretical Integration: The study advances theory by integrating concepts from information security, behavioral science, and organizational culture (e.g., Protection Motivation Theory and Theory of Planned Behavior). This interdisciplinary approach allows for a richer, process-oriented explanation of the intention–action gap in secure behavior, which scholars consistently identify as the fundamental flaw in modern organizational defense strategies (Sulaiman et al., 2022).

- Multi-Tiered Analytical Framework: It proposes an integrative analytical framework that conceptually links individual awareness, organizational culture, and national policy. This framework offers a valuable structure for future scholars to analyze the complex, interdependent elements of cybersecurity resilience across similarly dynamic, developing socio-technical domains.

5.4.5 Contribution to Practical and Policy Directions

The findings offer actionable, evidence-based directives that directly support and enhance the UAE's National Cybersecurity Strategy and its ambitious digital goals, providing a clear path from research to implementation.

- Policy Validation and Refinement: By empirically confirming that negligence and human error (insider threats) are the primary vulnerabilities, the research validates the necessary national policy shift toward behavioral enforcement and incentivization rather than just technical compliance. This provides empirical backing for regulators to refine existing mandates and focus efforts on changing user conduct, aligning directly with the objectives of the UAE Cyber Security Council (National Cybersecurity Council, 2024).

- Strategic Workforce Optimization: The study offers detailed, contextual insights into the failures of current, generic training (identified in the findings). The strong recommendations for implementing role-based, gamified training (Williams et. al., 2024) serve as a practical blueprint for organizations in the high-risk banking sector to optimize training budgets and achieve measurable, sustained reductions in human-related risk.

- National Resilience Strategy: The long-term recommendations, particularly regarding curriculum integration and national simulation centers, align precisely with the UAE's goal of achieving digital sovereignty. By fostering an intrinsically motivated, security-aware population from the school level upward, the research provides a strategic, multi-decade roadmap for securing the nation's critical economic stability and technological assets against increasingly sophisticated state-level threats (Schneier, 2017).

5.4.6 Contribution to Future Research Directions

This research also lays a foundation for future scholarly inquiry. It identifies critical gaps in literature and provides a roadmap for subsequent studies that can deepen or expand on the current work. The implications for further research highlighted ten key areas where additional academic exploration is needed, including longitudinal behavioral analysis, ethical AI integration in cybersecurity, and the development of inclusive, culturally aware awareness programs. Moreover, the methodological approach used in this research, including its emphasis on mixed methods and stakeholder engagement, can serve as a useful model for researchers examining multi-dimensional problems in cybersecurity or other domains of national importance.

In summary, this research provides a robust and timely contribution to the academic, practical, and strategic domains of cybersecurity awareness in the UAE. It extends theoretical understanding, enriches the empirical evidence base, and offers actionable insights for a range of

stakeholders. In doing so, it supports the evolution of cybersecurity from a narrow technical issue into a strategic national imperative that encompasses education, culture, governance, and innovation. These contributions will not only support improved outcomes in the UAE but can also serve as a model for similarly positioned nations seeking to enhance their digital resilience in an increasingly interconnected world.

5.5 Research Limitations

While this research provides valuable insights, several limitations must be acknowledged. First, the research was geographically confined to the UAE. Although this specificity allows for detailed contextual analysis, it may limit the generalizability of the findings to other regions or countries with different cybersecurity infrastructures, cultural norms, or policy frameworks.

Second, the research primarily relied on self-reported data collected through semi-structured interviews. Such data is subject to biases, including social desirability and recall inaccuracies, which may affect the accuracy of the reported behaviors or attitudes. Third, due to time and resource constraints, the sample size was limited and may not fully capture the diversity of perspectives within all sectors particularly among underrepresented groups such as small enterprises, rural populations, or minority language speakers. This could potentially overlook nuanced cybersecurity challenges experienced by these groups.

Additionally, the rapidly evolving nature of cybersecurity threats and solutions presents an inherent limitation. Technologies, regulations, and threat vectors change quickly, which means that findings and recommendations may require periodic updates to remain relevant. Finally, while the research highlights key behavioral and structural factors influencing cybersecurity awareness, it does not delve deeply into technical vulnerability assessments or organizational IT infrastructure. Future studies may benefit from combining behavioral research with technical audits for a more holistic understanding.

In conclusion, cybersecurity is a multifaceted and evolving field. As the UAE continues its journey toward digital leadership, further research is essential to keep pace with

technological, behavioral, and geopolitical shifts. From longitudinal behavior studies and comparative GCC analyses to AI ethics and SME resilience, the avenues outlined above offer a rich and actionable research agenda. By fostering cross-disciplinary, cross-sector, and cross-cultural research, the UAE can not only fortify its digital ecosystem but also contribute meaningfully to global cybersecurity knowledge and leadership.

References

Abbas, W. (2024, October 30). ‘Zero trust policy’: UAE cybersecurity experts say staff awareness could cut attacks by half. *Khaleej Times*. Retrieved from www.khaleejtimes.com

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

Alger, J. (2024). *67% of organizations say employees lack basic security awareness*. Security Magazine. Retrieved from www.securitymagazine.com

Al-Khouri, A. M. (2012). eGovernment strategies: The case of the United Arab Emirates (UAE). *European Journal of ePractice*, *17*, 126–150.

Alkhalil, A., Dawoud, D., Scott, M., & Simms, B. (2021). Cybersecurity in the Middle East: An assessment of maturity and culture. *Computers & Security*, *103*, 102202. https://doi.org/10.1016/j.cose.2021.102202

Aloul, F. A. (2010). Information security awareness in UAE: A survey paper. *International Conference for Internet Technology and Secured Transactions (ICITST)*.

Alshaikh, M., Maynard, S. B., Ahmad, A., & Chang, S. (2018). An exploratory study of current information security training and awareness practices in organizations. *Information & Computer Security*, *26*(3), 326–344. https://doi.org/10.1108/ICS-07-2017-0046

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security, 98*, 102003. Retrieved from www.colab.ws

Ani, M. et al. (2019). Study on human factors in cybersecurity. Retrieved from www.sciencedirect.com

Ansari, M. F., Dash, B., Sharma, P., & Yathiraju, N. (2022). The impact and limitations of artificial intelligence in cybersecurity: A literature review. *IJARCCE, 11*(9). https://doi.org/10.17148/ijarcce.2022.11912

Apau, R., & Koranteng, F. N. (2019). Impact of cybersecurity awareness training on employee behavior in the public sector. *Information & Computer Security, 27*(3), 362–379. https://doi.org/10.1108/ICS-02-2018-0025

Arachchilage, N. A. G., & Love, S. (2016). A game design framework for avoiding phishing attacks. *Computers in Human Behavior, 63*, 594–609.

Bada, A., Sasse, M. A., & Nurse, J. R. (2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672*.

Bakewell, A. et al. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security, 98*, 102003. Retrieved from www.sciencedirect.com

Barata, G., Gama, S., Jorge, J., & Gonçalves, D. (2017). Engaging engineering students with gamification. *Proceedings of the 5th International Conference on Games and Virtual Worlds for Serious Applications*. Retrieved from www.sciencedirect.com

Beautement, A., Sasse, M. A., & Wonham, M. (2008). The compliance budget: managing security behavior in organisations. *Proceedings of the New Security Paradigms Workshop*, 47–58.

Bonneau, J., Herley, C., van Oorschot, P. C., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. *IEEE Symposium on Security and Privacy*, 553–567.

Braun, V., & Clarke, V. (2021). *Thematic analysis: A practical guide*. SAGE Publications.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77-101. https://doi.org/10.1191/1478088706qp063oa

Brightside. (2025). Why most cybersecurity awareness programs fail in 2025 (and how to fix them). Retrieved from www.brside.com

Brundage, M., et al. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. *arXiv*. Retrieved from www.arxiv.org

Bulgurcu, B., Çavuşoğlu, 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.

Burns, C., Johnson, M., & Caputo, D. (2019). Just-in-time phishing defenses. *Behavioural Public Policy*, Cambridge.

Campbell, D., & van den Berg, J. (2010). Balancing usability and security: A user-centred approach to security mechanism design. *Journal of Cybersecurity*, 5(2), 53–61.

Cartier, M. (2025, April 23). Creating a company culture for security: What actually works. Hoxhunt. Retrieved from https://hoxhunt.com/blog/creating-a-company-culture-for-security

Collis, J., & Hussey, R. (2021). Business research: A practical guide for undergraduate and postgraduate students (5th ed.). Palgrave Macmillan.

Coventry, L., Briggs, P., & De Angeli, A. (2014). Usable security: Integrating mechanisms with user workflows. *Computers in Human Behavior*, 25, 1291–1300.

Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). SAGE Publications.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, 32, 90–101.

Cybereclipse. (2024). *Unlocking the benefits of micro-learning for cyber training*. Retrieved from https://www.cybereclipse.com/unlocking-benefits-microlearning

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

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.

de Bruin, R., & Mersinas, K. (2024). Cybersecurity Risk in Financial Institutions: A Behavioral Perspective. *Journal of Cyber Policy*.

Denzin, N. K., & Lincoln, Y. S. (Eds.). (2018). *The SAGE handbook of qualitative research* (5th ed.). SAGE Publications.

Florencio, D., & Herley, C. (2007). A large-scale study of web password habits. *Proceedings of the 16th International Conference on World Wide Web*, 657–666.

Gill, P., Stewart, K., Treasure, E., & Chadwick, B. (2008). Methods of data collection in qualitative research: Interviews and focus groups. *British Dental Journal*, *204*(6), 291–295. https://doi.org/10.1038/bdj.2008.192

Haney, J., & Lutters, W. (2020). Security awareness training for the workforce: Moving beyond "check-the-box" compliance. *Computer*. Retrieved from www.pmc.ncbi.nlm.nih.gov

Harwood, T., & Garry, T. (2015). Gamified phishing training field experiment. *ACM SIGMIS Database*. Retrieved from www.dl.acm.org

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decisions Support Systems, 47*(2), 154–165.

Jalali, M. S., Siegel, M., & Madnick, S. (2020). Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. *The Journal of Strategic Information Systems*, 29(1), 101–598.

Kallio, H., Pietilä, A. M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: Developing a framework for a qualitative semi-structured interview guide. *Journal of Advanced Nursing*, *72*(12), 2954–2965.

Kuckartz, U., & Rädiker, S. (2019). *Analyzing Qualitative Data with MAXQDA: Text, Audio, and Video*. Springer.

Lincoln, Y. S., Lynham, S. A., & Guba, E. G. (2018). Paradigmatic controversies, contradictions, and emerging confluences, revisited. In N. K. Denzin & Y. S. Lincoln (Eds.), *The SAGE handbook of qualitative research* (5th ed., pp. 108–150). Sage Publications.

Merriam, S. B., & Tisdell, E. J. (2016). *Qualitative research: A guide to design and implementation* (4th ed.). Jossey-Bass.

Moustakas, C. (1994). *Phenomenological research methods*. SAGE Publications.

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic Analysis: Striving to Meet the Trustworthiness Criteria. *International Journal of Qualitative Methods*, 16(1), 1-13. https://doi.org/10.1177/1609406917733847

Okere, I., Van Niekerk, J., & Carroll, M. (2012). Assessing information security governance in South African public sector organisations. *The African Journal of Information Systems*, *4*(1), Article 3.

Oseni, A., Moustafa, N., Janicke, H., Liu, P., Tari, Z., & Vasilakos, A. V. (2021). Security and privacy for artificial intelligence: Opportunities and challenges. *arXiv*. Retrieved from www.arxiv.org

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., & McCormac, A. (2015). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*, 48, 186–197.

Parsons, K., McCormac, A., Butavicius, M., & Ferguson, L. (2017). Human factors and information security: Individual, culture and security environment. *Australian Government Department of Defence – Defence Science and Technology Group*.

Pedersen, K. T., et al. (2025). Deepfake-driven social engineering: Threats, detection techniques, and defensive strategies in corporate environments. *J. Cybersecur. Priv., 5*(2), 18.

Ponemon Institute via Wikipedia. (n.d.). Internet security awareness training. Retrieved from www.en.wikipedia.org

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

SANS Institute. (2025). The what & how of role-based security awareness training. Retrieved from www.sans.org

Saunders, M., Lewis, P., & Thornhill, A. (2019). *Research methods for business students* (8th ed.). Pearson Education.

Scott, M., & Ophoff, J. (2018). The Behavioural Cybersecurity Research Framework. *PACIS 2018 Proceedings*, 13.

Smith, J. A., Flowers, P., & Larkin, M. (2009). *Interpretative phenomenological analysis: Theory, method and research*. SAGE Publications.

SoSafe Awareness. (2025). Gamification in cybersecurity various case studies. Retrieved from www.sosafe-awareness.com

Springer. (2025). Generative AI revolution in cybersecurity. *Artificial Intelligence Review, 58*, 236. Retrieved from link.springer.com

Stake, R. E. (1995). *The art of case study research*. Sage Publications.

Sulaiman, H., Bin Hassan, M. F., & Rahman, A. A. (2023). Investigating protection motivation theory in predicting employee security behavior. *Journal of Information Security and Applications, 70*, 103204. https://doi.org/10.1016/j.jisa.2022.103204

Techopedia. (2025). How to make cyber awareness training work in 2025. Retrieved from www.techopedia.com

Thanh, N. C., & Thanh, T. T. L. (2015). The interconnection between interpretivist paradigm and qualitative methods in education. American Journal of Educational Science, 1(2), 24–27.

ThreatCop. (2025). Role-based security awareness training: Benefits & top practices. Retrieved from www.threatcop.com

Trend.az. (2023). *UAE publishes world's first telecommunications cybersecurity guide*. Trend.az. Retrieved from https://en.trend.az/business/technology/3787842.html

UAE Cyber Security Council. (2024, March 4). *National Campaign for Cybersecurity launched*. Retrieved from www.csc.gov.ae

Uchendu, B., Nurse, J. R. C., & Furnell, S. (2021). *Developing a cyber security culture: Current practices and future needs*. arXiv. Retrieved from www.arxiv.org

Uchendu, I. G., Liu, L., & Olayemi, J. O. (2021). Promoting Cybersecurity Awareness in the Workplace: A Framework for Behavioural Change. *Information & Computer Security*, 29(2), 247–264.

UK NCSC. (2024). AI will make scam emails look genuine. *The Guardian*. Retrieved from www.theguardian.com

Vakulov, A. (2025). *Why policies and training fail without a strong cybersecurity culture*. Communications of the ACM. Retrieved from https://cacm.acm.org/blogs/blog-cacm/why-policies-and-training-fail

van Manen, M. (2016). *Researching lived experience: Human science for an action sensitive pedagogy* (2nd ed.). Routledge.

Vijay, J. (2025). State of AI-Powered Cybercrime. *Times of India*. Retrieved from www.timesofindia.indiatimes.com

Welsh, E. (2002). Dealing with data: Using NVivo in the qualitative data analysis process. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research*, 3(2), Art. 26.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24*(6), 2799–2816.

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). Sage Publications.

York, C. S., & deHaan, J. (2018). Gamified learning mechanisms and cyber awareness. *Educational Technology Review*. Retrieved from www.sciencedirect.com

APPENDIX A: ETHICAL APPROVAL

University of Central Lancashire
UCLan

University of Central Lancashire
Preston PR1 2HE
01772 201201
uclan.ac.uk

25th February 2025

Richard Fisher / Mohamed Ahmed Saeed Al Zaabi
School of Business
University of Central Lancashire

Dear Richard / Mohamed

Re: BAHSS2 Ethics Review Panel Application
Unique Reference Number: BAHSS2 01294

The BAHSS Ethics Review Panel has granted approval WITH CONDITION for your proposal application 'Enhancing Cyber Security Awareness in the UAE: Strategies Against Cyber Threats and Assets Protection'.

The CONDITION relating to the approval are:

1. The confirmation of relevant permissions from the banking organisations is received and a copy sent to the Ethics, Integrity and Governance Unit.

It is your responsibility to ensure that:

- the project is carried out in line with the information provided in the forms you have submitted
- you regularly re-consider the ethical issues that may be raised in generating and analysing your data
- any proposed amendments/changes to the project are raised with, and approved by, the Ethics Review Panel
- you notify EthicsInfo@uclan.ac.uk if the end date changes or the project does not start
- serious adverse events that occur from the project are reported to the Ethics Review Panel
- a closure report is submitted to complete the ethics governance procedures (existing paperwork can be used for this purpose e.g. funder's end of grant report; abstract for student award or NRES final report. If none of these are available, use the e-Ethics Closure Report pro forma).

Yours sincerely

Dr Stephen Haraldsen
Deputy Vice-Chair
BAHSS2 Ethics Panel

* for research degree students this will be the final lapse date

NB - Ethical approval is contingent on any health and safety checklists having been completed, and necessary approvals gained.

APPENDIX B: INTERVIEW QUESTIONS

Plan of Interview: Strengthening Cybersecurity Awareness in the Banking Sector of the United Arab Emirates

1. Can you describe the current level of cybersecurity awareness among employees in UAE organizations?

2. From your viewpoint, how critical is cybersecurity awareness in protecting personal and organizational assets in the UAE?

3. What are the most prevalent cyber threats facing individuals and businesses in the UAE today?

4. Can you share any recent cybersecurity incidents that have impacted your organization?

5. What are the most common tactics currently used by cybercriminals to target individuals or businesses in the UAE?

6. Are you familiar with the UAE's existing cybersecurity policies and regulations?

7. Have you participated in any cybersecurity awareness Campaigns?

8. What are the main challenges preventing employees from adopting the best cybersecurity practices?

9. From your viewpoint, what changes need to be made to the UAE's cybersecurity policies or regulations to overcome cyber threats?

10. Is there anything else you would like to share regarding cybersecurity protection strategies in the UAE?