LEX LOCALIS-JOURNAL OF LOCAL SELF-GOVERNMENT
ISSN:1581-5374 E-ISSN:1855-363X
VOL. 23, NO. S6(2025)

THE IMPACT OF STRATEGIES APPLIED BY THE UAE CYBERSECURITY COUNCIL AGAINST CYBERSECURITY THREATS WITHIN THE UAE GOVERNMENT ORGANIZATION AND ENTITIES

Saeed Mohamed Saeed Ali Alzaabi[1]*, Kamarul Zaman Haji Yusoff[2]

[1]*School of International Studies, Universiti Utara, Malaysia,06010 Sintok, Kedah- Malaysia.*
[2]*School of International Studies, Universiti Utara, Malaysia,06010 Sintok, Kedah- Malaysia.*

*Corresponding author E-mail: saeedmlialzaabi@gmail.com[1]

Abstract
Considering the increasing cybercrimes in the world and in the UAE, this study has been designed to explore the factors that have the potential to significantly control cybercrimes. The researcher conducted detailed literature review for identifying the factors and the laws that the government has made for the control of cybercrimes. Using the theoretical support of technology acceptance model, the framework of the study has been developed to cover the four key factors that have the potential to control cybercrimes. The data has been analyzed using SMART PLS 3. The findings revealed that all the variables have a significant positive impact over cyber security. The study ends up with theoretical and practical contributions along with highlighting the limitations of the current research and avenues for the future studies.

Keywords: *mobile cyber threats, phishing cyber threats, information cyber threats, banks cyber threats*

1. INTRODUCTION

In contemporary society, cyberspace has become an integral component of the everyday routines of individuals across many societal sectors, including business and governmental organizations. The ongoing advancement of Information and Communication Technologies (ICT), together with the proliferation of social media platforms (Ajina, Ali, Zamil, Khalid, & Sulaiman, 2024), the rise of internet-based commerce, and the widespread use of online banking, has not only fostered a robust economy, but has also facilitated the seamless global movement of information and media (Ta'Amnha, Alsoud, Asad, Magableh, & Riyadh, 2024). The realization of benefits from digital infrastructures in cyberspace is contingent upon the establishment of an environment characterized by trust security, safety, and reliability of such infrastructures (Damer, Al-Znaimat, Asad, & Almansour, 2021).

Furthermore, the interconnectedness of networks, inherent imbalance of cyber-threats, and ubiquity of the cyberspace across many domains need comprehensive strategies and collaborative endeavors from all parties involved to guarantee a sufficient degree of security in the UAE (Al Blooshi, et al., 2023). It is imperative for the government to establish a comprehensive structure that enables the coordination of all efforts aimed at enhancing the efficacy and efficiency of cyber security defenses, both inside and outside its various agencies. Consequently, it is imperative to involve a wide range of stakeholders from both the public and private sectors, as well as other global organizations, to address these concerns effectively (Shamsi, 2019).

Furthermore, there has been a significant surge in various forms of cyber assaults, such as malware, phishing, corrupted applications, password manipulation, computer session hijacking, and denial of service, inside the UAE and the Gulf Cooperation Council (GCC) in recent years (Shamsi, 2019). The rise in cyber security breaches targeting critical government and industry data may be partly attributable to many factors, including the abundance of data stored in data centers (AlDaajeh, et al., 2022). Official figures from the

Dubai police indicate a significant 88% surge in recorded occurrences of electronic crime in 2019 in comparison to the preceding years.

The topic of cyber security has garnered significant attention in scholarly discourse in recent years. According to the UAE Computer Emergency Response Team Website (2023), unauthorized individuals with advanced computer skills have managed to illicitly acquire ATM and credit card data from processing firms. Although UAE-based businesses are facing high levels of cybercrime, which includes 66% experiencing data breaches, the problem is not getting any better (Fearn, 2024). To mitigate the risk of fraudulent activities, it is essential for the government to enhance the security measures on both personal identification documents and business cards. One effective approach to do this is by integrating RFID blocking capabilities into these cards (Ameen, et al., 2021).

The UAE is well recognized for its robust conventional and cyber security measures, which are seen as crucial contributors to the high quality of life achieved in the country (Shamsi, 2019). The UAE has emerged as a destination where individuals from over two hundred nationalities reside, benefiting from the protection of the legal system that ensures their entitlement to serenity and harmony.

Mohamed Hamad Al Kuwaiti, the individual responsible for overseeing cyber security initiatives within the UAE government, emphasized the importance of aligning with the guidance provided by the country's wise leadership and the strategic objectives outlined for the next fifty years. Additionally, the UAE undertakes the responsibility of overseeing the level of compliance exhibited by the concerned authorities. The rapid advancement and wide-ranging nature of technology pose significant obstacles for the UAE government, necessitating increased attention to safeguard organizations against electronic attacks. Additionally, these attacks may also seek to pilfer highly significant information pertaining to bank clients (Ganeshbabu, Rajasekaran, & Ranganathan, 2024).

Cybercrimes are common throughout the world and Arab world (Damer, Al-Znaimat, Asad, & Almansour, 2021) especially UAE which has now become financial hub has no exception to it (Fadhel, Aljalahma, Almuhanadi, Asad, & Sheikh, 2022). However, cybercrimes are continues increasing on regular basis (Fearn, 2024). The UAE government, through the Supreme Council for Cyber security in the UAE, is working to confront electronic attacks that threaten the security of the government and the Emirati citizen. However, despite the measures taken by the UAE government and its Cyber Security Council, it continues to suffer from numerous forms of mobile cyber threats, phishing threats and attacks, information theft and identity theft, and attacks on banks, which are some of the most dangerous threats.

To improve internal security, the UAE government has created cyber-security council in November 2020 (Ameen, et al., 2021). The application of a sound government administration in enhancing cyber security leads to preparedness and response to suspicions posed by cyber security risks against government agencies in the UAE, which leads to an increase in awareness of the risks among senior employees, which leads to taking organizational measures to prevent such attacks (Al Blooshi, et al., 2023).

According to Mohammed Hamad Al Kuwaiti, the Chairman of the UAE Government Cyber Security Council, the Council, in collaboration with its partners, deals with a daily influx of over 50,000 cyber assaults that specifically target critical sectors inside the nation (UAE Cybersecurity Council, 2021). It is emphasized that proactive and efficient measures are taken to address these attacks with a high level of professionalism, aiming to strengthen the country's digital space against any malicious activities (Sky News, 2023).

Considerable number of governments worldwide are now contemplating the implementation of smart cities, which use cutting-edge technical advancements (Mijwil, Doshi, Hiran, Al-Mistarehi, & Gök, 2022). The Sheikh Mohammed bin Rashid Al Maktoum-sponsored Dubai Electronic Security Strategy sheds insight on the cyber threats and difficulties the UAE government faces (Ganeshbabu, Rajasekaran, & Ranganathan, 2024). These include assaults on banks, phishing scams, information theft, and identity theft as well as cyber

threats to mobile devices, cyber threats to mobile devices include sending a threat or committing a crime to any kind of electronic mobile device linked to the internet (Khan, Asad, Khan, Asif, & Aftab, 2021; Asad, Asif, Sulaiman, Satar, & Alarifi, 2023; Kanaan, Alsoud, Asad, Ta'Amnha, & Al-Qudah, 2024).

Phishing threats and assaults, information theft and identity fraud, and attacks on banks, cyber threats to mobile devices include sending a threat or committing a crime to any kind of electronic mobile device linked to the internet, phishing threats and assaults, information theft and identity fraud, and attacks on banks (Ameen, et al., 2021). Hence, the need to take certain steps to increase awareness of cyber security in the UAE which can significantly enhance cyber security, which calls for research in the field of cybersecurity.

Finally, the foremost challenge is related to banking cyber threats, UAE Computer Emergency Response Team Website (2023) stated that, hackers have been successful in acquiring credit card data from processing businesses and changing the available balances in these accounts. Other hackers in the targeted nations received these cards later and used them to withdraw substantial sums of money. Considering the issue and a continuous increase in these challenges there is a dire need for conducting research in the field of cybersecurity in the context of UAE.

2. LITERATURE REVIEW

Cyber-security encompasses the measures and protocols used to safeguard computer systems, networks, and internet-connected data against unauthorized access and potential damage. The rapid expansion of Information and Communication Technologies (ICT) inside the financial sector, namely in the domain of banking, has brought about a significant metamorphosis in the manner in which banks provide client services (Alkhuzaie, et al., 2024). According to Aldiabat et al. (2019), individuals engage in various banking activities, such as checking their account balances, making payments, applying for loans, and completing transactions, by using handheld devices inside the mobile banking model (Asad, Majali, Aledeinat, & Almajali, 2023). Furthermore, the use of mobile banking empowers clients to engage in financial transactions remotely, irrespective of their location and time constraints, by means of a portable handheld device and an active data plan (Asad, Aledeinat, Majali, Almajali, & Shrafat, 2024; Asad, et al., 2024). The use of digital banking services eradicates the limitations imposed by physical space and temporal factors that are often connected with conventional banking operations, such as the checking of account balances or the transfer of cash between accounts. Despite possessing several inherent advantages, mobile banking has encountered challenges in terms of low and sluggish client uptake (Ta'Amnha, Magableh, Asad, & Al-Qudah, 2023). Consequently, this topic has garnered significant attention from researchers worldwide, leading to a multitude of studies seeking to understand and elucidate its causes and implications (Aldiabat, Al-Gasaymeh, & Rashid, 2019).

The advent of the internet has significantly altered the manner in which individuals navigate their daily lives (Satar, Alharthi, Asad, Alenazy, & Asif, 2024). This transformation is evident in the way people establish connections with others via social networks and engage in commercial transactions using mobile devices (Allam, Asad, Ali, & Ali, 2021). Moreover, the impact of the internet extends to the realm of higher education, where it has brought about a substantial transformation in teaching techniques and the overall educational system. However, a significant number of individuals persistently encounter information security vulnerabilities stemming from a diverse array of potential hazards. Therefore, it is essential to prioritize the cultivation of cyber security awareness.

Additionally, on Sunday, November 29, 2020, the UAE announced the establishment of a Cyber security Council, which aims to prepare policies and legislation to enhance cyber security in the country and raise the readiness of all sectors to respond (UAE Cybersecurity Council, 2021). The announcement came while Sheikh Mohammed bin Rashid Al Maktoum, Vice President, Prime Minister and Ruler of Dubai, chaired, on Sunday, a Cabinet meeting at Qasr Al Watan in the Emirati capital, Abu Dhabi. Sheikh Mohammed bin Rashid wrote in a tweet on his Twitter account (Emirates News Agency, 2021).

In this context, Dr. Mohammed Al Kuwaiti, Chairman of the UAE Government Cyber-security Council, confirmed that the Council has succeeded in formulating an advanced cyber vision for the UAE that achieves maximum flexibility over the next fifty years, thus enhancing the country's global leadership and its ability to confront the increasing digital challenges and its readiness (UAE Cybersecurity Council, 2021).

The UAE possesses a sophisticated digital infrastructure and robust mechanisms to counteract malevolent electronic attacks directed at government sectors and institutions. As a result, it has achieved the fifth position globally in the Cyber security Index published by the International Telecommunication Union (ITU) of the United Nations. According to the official website of the UAE Government Cyber Security Council, issue of cyber security is a global concern. However, with an aim of the government to attract investors for businesses and employment creation it is necessary to increase cybersecurity (UAE Cybersecurity Council, 2021).

Cyber-attacks include a range of strategies used by persons who possess the capability to exploit vulnerabilities in electronic systems and networks, often with the aim of causing harm to these systems or gaining unauthorized access to and perusing confidential data (Mijwil, Doshi, Hiran, Al-Mistarehi, & Gök, 2022). Furthermore, they have been shown to impact a diverse range of businesses (Hasan & Al-Ramadan, 2021). Therefore, it is essential for enterprises to use a series of pragmatic strategies to effectively tackle the issue of cyber security. Cyber-attacks include malevolent actions directed at computer systems, networks, and devices over the Internet, with the intention of jeopardizing or causing harm to sensitive information (Mijwil, Doshi, Hiran, Al-Mistarehi, & Gök, 2022).

Unauthorized individuals find computer systems very appealing to manipulate due to the criticality of the information contained inside these systems. These assaults may be initiated by either an individual or a collective, driven by many factors such as monetary incentives, political agendas, or even personal motivations (AlDaajeh, et al., 2022). To mitigate these assaults, it is essential to adhere to the most effective strategies for ensuring online security, which include using robust passwords, refraining from engaging with emails originating from dubious sources, and regularly updating software and operating systems.

The achievement of this objective may be attained by staying informed about the latest threats and implementing effective security measures, while also formulating suitable tactics to counteract them (Bajao & Sarucam, 2023). Hence, considering the above discussion, the core issues that are causing the issues of cybersecurity are related to mobile cyber-threats, phishing cyber threats, information cyber threats, and banks cyber threats.

2.1 Mobile Cyber Threats

The spread of mobile phones has provided the unprecedented chance for financial inclusion of unbanked people in developing countries via innovations like mobile money (Akinyemi, Mushunje, & Feng, 2020). Commerce is a field of study that encompasses many activities related to the buying and selling of goods and services (Coulibaly, 2021). As Coulibaly (2021) claimed that it is essential to use Multimedia Messaging Service (MMS) for the purpose of conducting monetary transfers as well as facilitating the sending and receiving of payments (Abdul-Hamid, Shaikh, Boateng, & Hinson, 2019). Hence, the aim of this study is to explore the accessibility of unbanked individuals via mobile phone use, namely by establishing a network of physical transactional locations, often referred to as agents. Moreover, there is an increasing level of innovation, who are always seeking new methods and techniques (Asad, Asif, Sulaiman, Satar, & Alarifi, 2023). Hence, to ensure the efficacy of human-mediated cyber threat avoidance, it is essential that the countermeasures used be both resilient and capable of anticipating and averting such threats.

2.2 Phishing Cyber Attacks

Phishing attacks are widely recognized as one of the most severe forms of cyber-attacks within the realm of social networking platforms. These malicious activities have the potential to inflict significant and

detrimental damages. The assault against secure online transactions (Coulibaly, 2021). Attackers use several communication methods on social media platforms to reach out to individuals (Fearn, 2024). Furthermore, the severity level of attack vectors, or methods used to exploit vulnerabilities, also shows a continual increase (Ganeshbabu, Rajasekaran, & Ranganathan, 2024).

The phishing assault procedure operates on the assumption that the intended target will receive a fraudulent email. The attack begins by presenting a web service using a deceptive HTTP. In this process when the individual who has been targeted engages with the provided hyperlink and proceeds to interact with the form by inputting information. Once the necessary data is obtained, it becomes into the hands of the assailant (Hasan & Al-Ramadan, 2021). The assault in question involves deceiving consumers by creating a replica of a legitimate website, so luring them into a trap set by malicious actors. Hence, it is clear that the threat is significant and need proper research to understand for control the same.

2.3 Information Cyber Threats

The academic literature has identified several common mechanisms of illicit insider data theft and related crimes (IIDTRC) in retail companies, including botnets, coercion, collaboration, collusion, infiltration, and social engineering. Honest personnel may have heightened difficulties due to external pressures that coerce them into compromising their professional ethical standards and engaging in illicit activities, often referred to as "Intentional Illegal or Illicit Deviant Task-Related Conduct" (IIDTRC). Luo et al. (2020) constructed an extensive framework for understanding employee-engaged malicious computer misuse. One of the most challenging topics in the field of security research and practice is the prevention, detection, and response to data leakage caused by authorized individuals, also known as insider threats (Luo, Li, Hu, & Xu, 2020). The failure may be related to a deficient comprehension of the nature of the Internal Information and Data Theft Risk Control (IIDTRC) by crime prevention management, as well as a lack of clearly defined duties pertaining to internal data security.

Additionally, the principle highlights the importance of trust and security in e-commerce, as customers Commerce research include the dissemination of business knowledge, the cultivation of business connections, and the execution of commercial activities. Business transactions conducted via telecommunications refer to the exchange of goods, services, or financial transactions that occur remotely through electronic communication technologies. The topic of interest pertains to networks and need current attention.

2.4 Banks Cyber Threats

Information systems is the academic discipline that concentrates on the creation, advancement, execution, and administration of computer-based systems for managing information. In order to identify and mitigate harmful behaviour, it is essential for systems to maintain a continuous and effective process of monitoring, operating, and recording transactions. The achievement of this objective is contingent upon the use of cyber-resilient technology to safeguard information security (Kassa, James, & Belay, 2024). The inclusion of continuous monitoring is highly recommended as an integral part of insider risk management in order to provide comprehensive protection of sensitive and personal data inside a network. The safeguarding of internet systems against cyber-attacks is accomplished by the implementation of cyber security measures. Due to the potential negative consequences of breaches, including damage to a company's image and financial and non-financial damages to its customers, the implementation of cyber security measures is essential to mitigate such risks (Pashentsev & Babaeva, 2024).

Moreover, Artificial Intelligence (AI) has the capacity to profoundly alter human lives, potentially yielding both positive and negative outcomes. The potential of using it as a resource for public safety is now being examined via several approaches (Pashentsev & Babaeva, 2024). The use of biometrics in the financial sector includes the implementation of biometric payment methods. Fingerprint scans are often used in

tandem with this technology to authenticate transaction processes. However, all these measures need to be tested through research before formal implementation in any new society.

2.5 Underpinning Theory

2.5.1 Technology Acceptance Model (TAM)

Technology Acceptance Model (TAM) has been used in diverse fields (Alsyouf, et al., 2023). The TAM was first proposed by Davis in 1989, including two essential constructs: perceived utility (PU) and perceived ease of use (PEOU). This includes the exploitation of online library resources, digital libraries, and adherence to the Modern Language Association (MLA) standard. Additionally, Taherdoost (2022) performed a research whereby the author included the notion of system characteristic, especially system quality, inside the framework of the TAM. The objective was to evaluate users' behavioral intention towards e-library platforms (Taherdoost, 2022). Based on the research conducted by Taherdoost (2022), it was determined that various other variables incorporated in TAMexerted a noteworthy and positive influence on the fundamental constructs of TAM, particularly about the inclination to utilize mobile shopping services. Hence taking the underpinning support of TAM Figure 2.1 shows the relationship between the study variables, which are the independent variable Cyber Threats, which has four dimensions: Mobile Cyber Threats (MT), Phishing Cyber Threats (PT), Information Cyber Threats (IT), and Banks Cyber Threats (BT). The dependent variable is Cyber Security (CS).

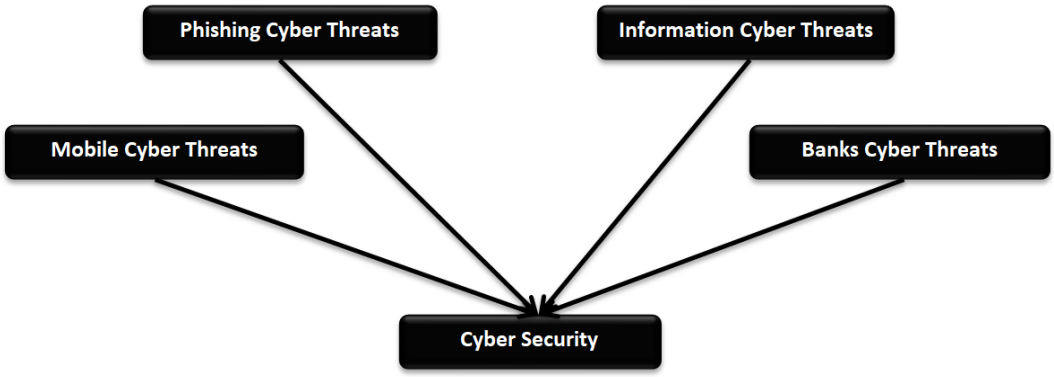

Figure 1 Conceptual Framework

The framework has been developed based on Technology acceptance model, because all the issues identified are related to technology. Technology at one time as it is increasing ease at the same time creating challenges for the organizations (Asad, Ahmad, Haider, & Salman, 2018). Researchers have widely used the Technology Acceptance Model (TAM) to investigate user behavior regarding the adoption of new information systems and technology in the setting of libraries. However, applying TAM over the use of this combination especially linking and extending the model to cybersecurity is the main aim of the study and the major theoretical contribution of the study.

2.6 Hypothesis Development

2.6.1 Cyber Security and Mobile Cyber Threats

Types of cyber threats vary depending on the means and tools by which cyber-attacks are carried out in order to complete crimes digitally. Specialists in this field have created forms and types of crimes and cyber security threats in several aspects and among these threats are cyber threats to mobile devices: This type focuses on delivering... A threat or crime against any type of electronic portable device connected to the Internet. It is considered one of the most dangerous and common threats because it is a common occurrence

due to the proliferation of portable devices around the world. Today, they are carried with every individual, young and old, and we rarely find a person who does not carry a mobile phone. Numerous previous studies have shown that this type of threats via mobile phones has an impact on the cyber security of governments and individuals, and among these studies (Mijwil, Doshi, Hiran, Al-Mistarehi, & Gök, 2022; Muhammad, Anwar, Saleem, & Shahid, 2023). But hardly any researchers have conducted research in the context of UAE, therefore, considering the gaps in the literature, the following hypothesis has been proposed for testing in the contextual setting of UAE.

H1: *Mobile cyber threats significantly impact cyber security services provided by the cyber security council.*

2.6.2 Cyber Security and Phishing Cyber Attacks Threats

The categorization of cyber threats is contingent upon the methodologies and instruments used in executing cyber assaults for the purpose of perpetrating digital crimes. Experts in the field have developed various categories and manifestations of cybercrimes and cyber security threats. One such threat is the Cyber Security and Phishing Cyber Attacks Threat, which specifically targets the delivery of malicious activities or crimes to any portable electronic device connected to the Internet. This particular threat is widely recognized as one of the most perilous and prevalent, owing to the widespread usage of mobile devices, computers, and social networking platforms worldwide. These devices have become ubiquitous among individuals of all ages, making them highly susceptible to such threats (Sulaiman, 2025). We encounter an individual who lacks possession of a mobile phone or other technical device enabling internet-based communication, rendering them susceptible to phishing attacks. Numerous prior investigations have shown the significant influence of phishing attacks on the cyber security of both governmental entities and people. Noteworthy research in this domain includes (Mijwil, Doshi, Hiran, Al-Mistarehi, & Gök, 2022; Muhammad, Anwar, Saleem, & Shahid, 2023). However, none of the above study has been conducted in the context of UAE, therefore, considering the gaps in the literature, the following hypothesis has been proposed for testing in the contextual setting of UAE.

H2: *Phishing Cyber Threats significantly impact cyber security services provided by the cyber security council.*

2.6.3 Cyber Security and Information and identity Theft Cyber Threats

The categorization of cyber dangers varies based on the methods and instruments used to perpetrate digital crimes. Experts in the domain have developed many categories and manifestations of criminal activities and cyber security risks (Awain, Asad, Sulaiman, Asif, & Shanfari, 2025). One such risk is the infringement upon cyber security, as well as the theft of information and identities. The topic of discussion pertains to cyber threats and their specific areas of concentration. This form of communication is employed to convey a threat or engage in criminal activities through any electronic device that is connected to the Internet. It is widely recognized as one of the most perilous and prevalent threats, owing to the ubiquitous presence of mobile devices, computers, and social networking platforms worldwide, as well as the availability of diverse and numerous techniques. In contemporary times, mobile devices equipped with in contemporary society, it is a rarity to encounter an individual, regardless of age, who does not own a mobile phone or lack access to technology devices enabling internet-based communication (Asad, Fryan, & Shomo, 2025). This widespread connectivity, however, exposes individuals to the inherent risks associated with information and identity theft. Numerous prior investigations have shown that the cyber security of both governments and people is adversely affected by the danger posed by data and personal identity theft. These investigations include the works of (Mijwil, Doshi, Hiran, Al-Mistarehi, & Gök, 2022; Muhammad, Anwar, Saleem, & Shahid, 2023). Moreover, the studies that have been conducted have not applied particularly information cyber threat in the context of UAE, therefore, considering the gaps in the literature, the following hypothesis has been proposed for testing in the contextual setting of UAE.

H3: *Information Cyber Threats significantly impact cyber security services provided by the cyber security council.*

2.6.4 Cyber Security and Banks Cyber Attacks

The classification of cyber dangers is contingent upon the methods and instruments used to perpetrate digital offenses. Experts in the field have developed various forms and categories of cybercrimes and cyber security threats. One such threat is Cyber Security and Banks Cyber Attacks, which specifically targets the delivery of threats or criminal activities to any electronic device connected to the Internet. This type of threat is widely recognized as one of the most perilous and prevalent due to the widespread use of mobile devices, computers, and social networking platforms worldwide. Additionally, the abundance of methods available for perpetrating such attacks contributes to their common occurrence. The ubiquity of portable devices among young individuals further exacerbates the prevalence of these threats. It is a rare occurrence to encounter an individual who does not own a mobile phone or lack access to technical devices facilitating internet communication. This renders them susceptible to the perils of cyber-attacks targeting financial institutions. Numerous prior investigations have shown that the occurrence of Banks Cyber Attacks has a significant influence on the cyber security of both governmental entities and people. These investigations include the works of (Mijwil, Doshi, Hiran, Al-Mistarehi, & Gök, 2022; Muhammad, Anwar, Saleem, & Shahid, 2023). Despite several studies, none of the above study has been conducted in the context of UAE, therefore, considering the gaps in the literature, the following hypothesis has been proposed for testing in the contextual setting of UAE.

H4: *Banks Cyber Attacks significantly impact cyber security services provided by the cyber security council.*

3. METHODOLOGIES

The research design encompasses a thorough strategy for gathering data in an experimental research endeavor with the objective of addressing research inquiries and examining hypotheses (Quinlan, Zikmund, Babin, Carr, & Griffin, 2018). To accomplish the research objective, a tailored questionnaire design is used in this quantitative approach as used by other similar studies in gulf countries (Sulaiman, Asad, Awain, Asif, & Shanfari, 2024). This study aims to investigate the causal relationship between variables. In this research the unit of analysis for this study is the offices of the Supreme Council for Cybersecurity in the UAE. The study population includes all employees working in federal institutions in the Emirates. The selection of the Cybersecurity Council as a coordination body is based on its exemplary role in protecting Emirati citizens from various cyber threats, as well as its extensive resources and capabilities to spread its vision. Based on data provided by the Federal Center for Competitiveness and Statistics (2023), the total study population, which is the UAE, is estimated at approximately 10,000. Estimating the sample size for both categorical and continuous data and using Cochran's "G*Power sampling program" power test (1977). It is therefore a sample size of 357 was collected. Using the technique of online collection via (e-mail or WhatsApp) to collect data was most convenient and suitable thus, the same technique has been applied. Finally, the data has been analysed using Smart PLS3 for applying structural equation modelling. The next section explains the analysis section.

4. ANALYSIS

This section includes all findings derived from the gathered data by using structural equation modeling using SMART PLS 3.0 (Sarstedt, M.Ringle, Smith, Reams, & F.HairJr, 2014). The study evaluated the measurement of reliability and validity of the constructs. The outer model posits that the research variables are unidimensional within the context of item analysis. Furthermore, after confirming as well as analyzing the data, the next stage is to evaluate the inner and outer models (Vinzi, Chin, Henseler, & Wang, 2010). Figure 2 represents the evaluation of measurement model.

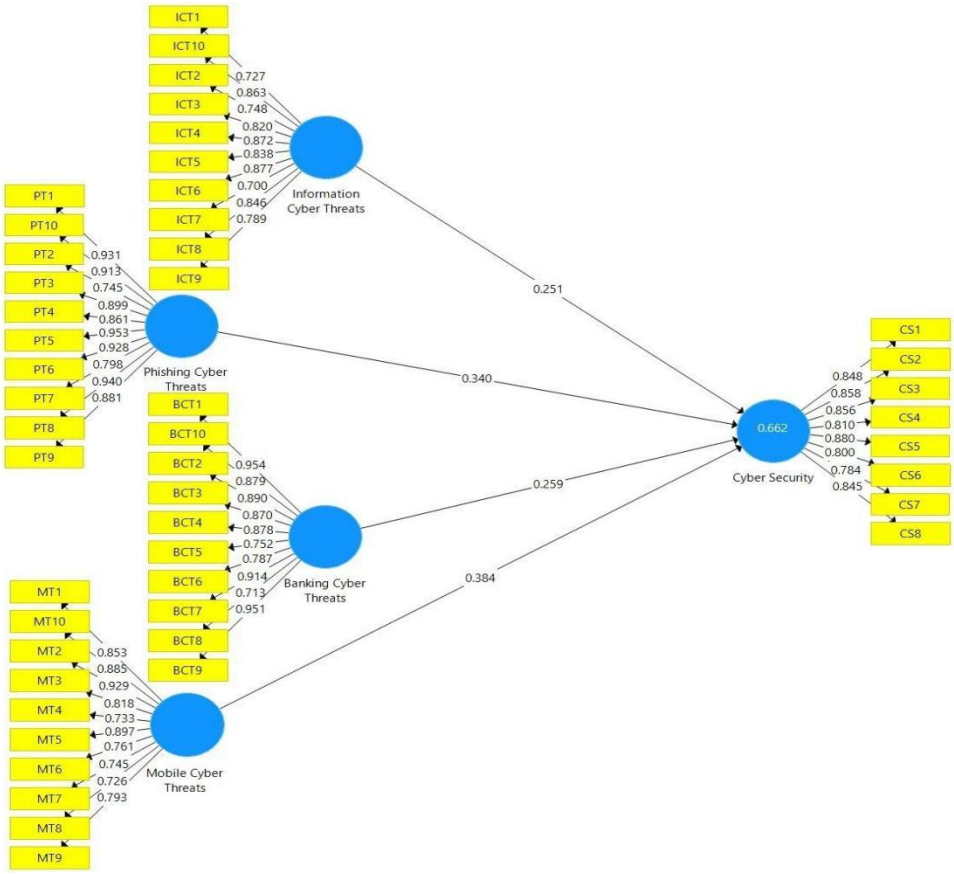

Figure 1Measurement Model

The study entails an investigation of Cronbach's Alpha, employed to evaluate the reliability and validity of all the variables using Cronbach's Alpha, Composite reliability and Average Variance Extracted (AVE) of all variables (Hair, Ringle, & Sarstedt, 2013), including Mobile Cyber Threats, Phishing Cyber Threats, Information Cyber Threats, Banks Cyber Threats, and Cyber Security, which are shown in Table 1.

Table 1: Reliability and Validity

Variables	Cronbach's Alpha	Composite Reliability	Average Variance Extracted (AVE)
Mobile Cyber Threats	0.936	0.946	0.640
Phishing Cyber Threats	0.966	0.971	0.772
Information Cyber threats	0.937	0.947	0.642
Banks Cyber Threats	0.953	0.961	0.715
Cyber Security	0.938	0.949	0.698

Above table showed that all the values are as per the threshold level and the variables hold sufficient reliability and validity. The study reveals the discriminant validity in which one speculative variable differed from another variable using Fornell-Larcker criterion (Chin, 2009). The results of discriminant validity by the Fornell-Larcker criterion are shown in Table 2.

Table 2 Discriminant Validity

	Banks Cyber Threats	Cyber Security	Information Cyber threats	Mobile Cyber Threats	Phishing Cyber Threats
Banks Cyber Threats	0.845				
Cyber Security	0.691	0.836			
Information Cyber threats	0.642	0.694	0.801		
Mobile Cyber Threats	0.641	0.736	0.636	0.8	
Phishing Cyber Threats	0.599	0.637	0.783	0.635	0.879

Discriminant validity has been known and ensured after confirming the reliability and validity of all variables in the structural model. After confirmation that all the variables are reliable and valid, an evaluation of the structural model examining the relationship between exogenous and endogenous latent variables has been performed. The bootstrapping results by applying the bootstrapping method of 5000 subsamples recognized that the relationships are significant as shown in table 3.

Table 3 Hypotheses Testing

	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (O/STDEV)	P Values
Mobile Cyber Threats->Cyber Security	0.384	0.360	0.096	3.978	0.000
Phishing Cyber Threats->Cyber Security	0.340	0.065	0.146	2.318	0.000
Information Cyber Threats->Cyber Security	0.251	0.254	0.086	2.897	0.000
Banks Cyber Threats->Cyber Security	0.259	0.253	0.091	2.816	0.001

The study also assesses a theoretical model to ascertain the prognostic significance at the construct level of Q^2 which is one of the criteria (Geisser, 2017). Cross-validated relevance findings of Q^2 values above zero indicate the predictive validity, a Q^2 value less than 0 indicates that the model lacks predictive relevance (Chin W. W., 1998), however, the calculated values are above 0.

Table 4 Construct Cross-validated Redundancy

	SSO	SSE	Q^2(=1-SSE/SSO)
Cyber Security	792.000	466.574	0.411

The above findings of the endogenous latent variable of Q^2 of cross-validated redundancy for cyber security (0.411) which specify that the structural model has a predictive influence.

5. CONCLUSIONS

The conclusions of the current study and the findings of the hypothesis revealed a highly significant indication of the increasing significance of the relationship between Mobile Cyber Threats, Phishing Cyber Threats, Information Cyber Threats, and Banks Cyber and Cyber Security. Additionally, despite various limitations, the current study was successful in addressing all research questions and research objectives. Consequently, numerous studies have been performed on the aspects that affect cybersecurity.

5.5.1 Theoretical Implications

The study results are anticipated to enhance the existing body of knowledge by confirming prior results. The first theoretical contribution from the examination of the Cyber Security during the declining performance of Cyber Security in that the individual setting has been largely ignored in previous studies. Consequently, most of the previous studies examine Cyber Security separately. Subsequently, other Cyber Security employees raising which are not aware of Cyber Security in UAE specifically, in the offices of the Supreme Council are also keen to learn from these empirical results. Likewise, the evaluation of the impact of Mobile Cyber Threats, Phishing Cyber Threats, Information Cyber Threats, and Banks Cyber Threats on the execution of Cyber Security is an additional contribution to enhancing the theoretical dimension within this framework.

5.5.2 Practical Implications

The government authorities, decision-makers, as well as policymakers have recognized that their decisions have a significant effect on cybersecurity. Consequently, it is crucial to demonstrate how government authorities and decision-makers could enhance cybersecurity among all employees working in the office of the Supreme Council. Furthermore, based on the literature, this research has recognized strategies for the Cyber Security lack of Cyber Security characteristics are the main cause among all employees working in the office of the Supreme Council. Thus, there is the fact that even those who are well-known do not manage their efforts well to guide the Cyber Security as well as correlate with the decision-makers and policymakers, and they are still not patronized.

5.6 Limitations and Recommendations

The first limitation is that even though there are various variables that affect the Cyber Security it is limited to Mobile Cyber Threats, Phishing Cyber Threats, Information Cyber Threats, and Banks Cyber Threats in study. The study suggests that future research might be conducted by using other factors to improve Cyber Security regarding the view of Mobile Cyber Threats, Phishing Cyber Threats, Information Cyber Threats, and Banks Cyber among all employees working in the office of the Supreme Council for Cybersecurity in the UAE who are involved in improving the Cyber Security to overcome the limitation of the study. Future research also considers government officials, decision makers or policymakers for all employees working in the office of the Supreme Council for Cybersecurity in the UAE.

Another limitation of the study is that data has been gathered from all employees working in the office of the Supreme Council for Cybersecurity in the UAE whereas, other officials of the government have not been added to the respondents. As this study is cross-sectional and longitudinal in nature whereas, future research could also be conducted on data collection over a longer or shorter period, or longitudinal or cross-sectional data collection individually.

Similarly, it involves the data collected in 2024-2025 that can be evaluated in a limited time due to time and the limitations of resources. The study has been conducted cross-sectionally and longitudinal because the competencies are not able to develop as well as they affect the relationship between variables over a longer period. A longitudinal study would be beneficial since it can illustrate the impact of policies over a longer

period, whereas Cross-sectional studies offer several notable advantages that make them popular in various fields, especially when quick, cost-effective, and broad data collection is needed.

Conclusion

This study examined how Mobile Cyber Threats, Phishing Cyber Threats, Information Cyber Threats, and Banks Cyber Threats influence the overall condition of cybersecurity at the Office of the Supreme Council for Cybersecurity in the United Arab Emirates. The research findings demonstrated a strong and positive relationship between these variables, highlighting the growing necessity of understanding the multidimensional nature of cyber threats in ensuring institutional performance and national security. Despite several limitations, the study successfully met its aims and research questions, contributing theoretically and practically to the developing debate on cybersecurity management.

Acknowledgement

The authors would like to thank their peers and colleagues for their insightful academic guidance and constructive criticism during the development of this research. They also thank the organizations and stakeholders in Qatar for their ongoing efforts to improve the performance of small and medium-sized businesses, which provided as an inspiration and source of information for our study. The authors also thank the contributions of previous researchers, whose writings on knowledge management, technological advancement, and entrepreneurial orientation provided the theoretical foundation for the current study.

References

Damer, N., Al-Znaimat, A. H., Asad, M., & Almansour, A. Z. (2021). Analysis of motivational factors that influence usage of Computer Assisted Audit Techniques (CAATs) auditors in Jordan. *Academy of Strategic Management Journal, 20*(Special Issue 2), 1-13.

Fadhel, H. A., Aljalahma, A., Almuhanadi, M., Asad, M., & Sheikh, U. (2022). Management of higher education institutions in the GCC countries during the emergence of COVID-19: A review of opportunities, challenges, and a way forward. *The International Journal of Learning in Higher Education, 29*(1), 83-97. doi:https://doi.org/10.18848/2327-7955/CGP/v29i01/83-97

Alkhuzaie, A. S., Asad, M., Mansour, A. Z., Sulaiman, M. A., Kayani, U. N., & Asif, M. U. (2024). Compliance with accounting standards by Jordanian SMEs. *Ikonomicheski Izsledvania, 33*(1), 89-107.

Fearn, N. (2024, January 12). *Cybersecurity Incidents Consistently Increase in UAE*. Retrieved from Drk Reading: https://www.darkreading.com/cyberattacks-data-breaches/cybersecurity-incidents-consistently-increase-in-uae

Asad, M., Ahmad, I., Haider, S. H., & Salman, R. (2018). A critical review of islamic and conventional banking in digital era: A case of Pakistan. *International Journal of Engineering & Technology, 7*(4.7), 57-59.

Allam, Z., Asad, M., Ali, A., & Ali, N. (2021). Visualization of knowledge aspects on workplace spirituality through bibliometric analysis. *2021 International Conference on Decision Aid Sciences and Application (DASA)* (pp. 446-450). Sakheer: IEEE. doi:10.1109/DASA53625.2021.9682372

Asad, M., Sulaiman, M. A., Awain, A. M., Alsoud, M., Allam, Z., & Asif, M. U. (2024). Green entrepreneurial leadership, and performance of entrepreneurial firms: Does green product innovation mediates? *Cogent Business & Management, 11*(1), 2355685. doi:https://doi.org/10.1080/23311975.2024.2355685

Asad, M., Majali, T., Aledeinat, M., & Almajali, D. A. (2023). Green entrepreneurial orientation for enhancing SMEs financial and environmental performance: Synergetic moderation of green

technology dynamism and knowledge transfer and integration. *Cogent Business & Management, 10*(3), 1-20. doi:https://doi.org/10.1080/23311975.2023.2278842

Asad, M., Aledeinat, M., Majali, T., Almajali, D. A., & Shrafat, F. D. (2024). Mediating role of green innovation and moderating role of resource acquisition with firm age between green entrepreneurial orientation and performance of entrepreneurial firms. *Cogent Business & Management, 11*(1), 2291850. doi:https://doi.org/10.1080/23311975.2023.2291850

Asad, M., Asif, M. U., Sulaiman, M. A., Satar, M. S., & Alarifi, G. (2023). Open innovation: The missing nexus between entrepreneurial orientation, total quality management, and performance of SMEs. *Journal of Innovation and Entrepreneurship, 12*(79), 1-13. doi:https://doi.org/10.1186/s13731-023-00335-7

Kanaan, O. A., Alsoud, M., Asad, M., Ta'Amnha, M. A., & Al-Qudah, S. (2024). A mediated moderated analysis of knowledge management and stakeholder relationships between open innovation and performance of entrepreneurial firms. *Uncertain Supply Chain Management, 12*(4), 2383-2398. doi:https://doi/10.5267/j.uscm.2024.5.028

Khan, A. A., Asad, M., Khan, G. u., Asif, M. U., & Aftab, U. (2021). Sequential mediation of innovativeness and competitive advantage between resources for business model innovation and SMEs performance. *2021 International Conference on Decision Aid Sciences and Application (DASA)* (pp. 724-728). Sakheer: IEEE. doi:10.1109/DASA53625.2021.9682269

Satar, M., Alharthi, S., Asad, M., Alenazy, A., & Asif, M. U. (2024). The moderating role of entrepreneurial networking between entrepreneurial alertness and the success of entrepreneurial firms. *Sustainability, 16*(11), 4535. doi:https://doi.org/10.3390/su16114535

Ta'Amnha, M. A., Magableh, I. K., Asad, M., & Al-Qudah, S. (2023). Open innovation: The missing link between synergetic effect of entrepreneurial orientation and knowledge management over product innovation performance. *Journal of Open Innovation: Technology, Market, and Complexity, 9*(4), 1-9. doi:https://doi.org/10.1016/j.joitmc.2023.100147

Ta'Amnha, M. A., Alsoud, M., Asad, M., Magableh, I. K., & Riyadh, H. A. (2024). Moderating role of technological turbulence between green product innovation, green process innovation and performance of SMEs. *Discover Sustainability, 5*, 1-16. doi:https://doi.org/10.1007/s43621-024-00522-w

Ajina, A. S., Ali, S., Zamil, A. M., Khalid, N., & Sulaiman, M. A. (2024). Unleashing the potential of social media celebrities to promote food waste reduction in educational institutions: Developing an extended model based on the value-belief-norm theory. *British Food Journal, 126*(7), 2787-2808. doi:https://doi.org/10.1108/BFJ-04-2023-0279

Ameen, N., Tarhini, A., Shah, M. H., Madichie, N., Paul, J., & Choudrie, J. (2021). Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce. *Computers in Human Behavior, 114*, 106531.

Al Blooshi, I. A., Alamim, A. S., Raed A. Said, Taleb, N., Ghazal, T. M., Ahmad, M., . . . Alshurideh, M. (2023). T Governance and Control: Mitigation and Disaster Preparedness of Organizations in the UAE. In *The Effect of Information Technology on Business and Marketing Intelligence Systems* (pp. 661-671). Cham: Springer.

Shamsi, A. A. (2019). Effectiveness of cyber security awareness program for young children: A case study in UAE. *International Journal of Information Technology and Language Studies, 3*(2), 8-29.

AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K.-K. R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security, 119*, 102754.

Ganeshbabu, R. O., Rajasekaran, M., & Ranganathan, C. S. (2024). CoT in Smart Cities. In *Cloud of Things* (pp. 90-106). Chapman and Hall/CRC.

UAE Cybersecurity Council. (2021, ~August 2). *UAE Cybersecurity Council*. Retrieved from The United Arab Emirates' Government portal: https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security/uae-cybersecurity-council

Sky News. (2023, May). *Sky News Arabia*. Retrieved from Sky news: https://www.skynewsarabia.com/middle-east

Mijwil, M., Doshi, R., Hiran, K. K., Al-Mistarehi, A.-H., & Gök, M. (2022). Cybersecurity challenges in smart cities: An overview and future prospects. *Mesopotamian Journal of Cybersecurity*, 1-4.

Aldiabat, K., Al-Gasaymeh, A., & Rashid, A. S. (2019). The Effect of Mobile Banking Application on Customer Interaction in the Jordanian Banking Industry. *International Association of Online Engineering, 13*(2), 37-49.

Emirates News Agency. (2021, January 28). *The Cybersecurity Council holds its first meeting "remotely."*. Retrieved from Emirates News Agency: https://www.wam.ae/ar/details/1395302905117

Hasan, M. F., & Al-Ramadan, N. S. (2021). Cyber-attacks and cyber security readiness: Iraqi private banks case. *Social Science and Humanities Journal, 5*(8), 2312-2323.

Bajao, N. A., & Sarucam, J.-a. (2023). Threats Detection in the Internet of Things Using Convolutional neural networks, long short-term memory, and gated recurrent units. *Mesopotamian journal of cybersecurity*, 22-29.

Akinyemi, B. E., Mushunje, A., & Feng, G. C. (2020). Determinants of mobile money technology adoption in rural areas of Africa. *Cogent Social Sciences, 6*(1), 1815963.

Coulibaly, S. S. (2021). A study of the factors affecting mobile money penetration rates in the West African Economic and Monetary Union (WAEMU) compared with East Africa. *Financial Innovation, 25*.

Abdul-Hamid, I. K., Shaikh, A. A., Boateng, H., & Hinson, R. E. (2019). Customers' perceived risk and trust in using mobile money services—an empirical study of Ghana. *International Journal of E-Business Research (IJEBR), 15*(1), 1-19.

Luo, X. R., Li, H., Hu, Q., & Xu, H. (2020). Why individual employees commit malicious computer abuse: A routine activity theory perspective. *ournal of the Association for Information Systems, 21*(6), 1-5.

Kassa, Y. W., James, J. I., & Belay, E. G. (2024). Cybercrime intention recognition: A systematic literature review. *Information, 15*(4), 263.

Pashentsev, D. A., & Babaeva, Y. G. (2024). Artificial intelligence in law-making and law enforcement: Risks and new opportunities. *Текст научной статьи по специальности «Право», 15*(2), 516-526.

Alsyouf, A., Lutfi, A., Alsubahi, N., Alhazmi, F. N., Al-Mugheed, K., Anshasi, R. J., . . . Albugami, M. (2023). The use of a technology acceptance model (TAM) to predict patients' usage of a personal health record system: the role of security, privacy, and usability. *International Journal of Environmental Research and Public Health, 20*(2), 1347.

Taherdoost, H. (2022). A critical review of blockchain acceptance models—blockchain technology adoption frameworks and applications. *Computers, 11*(2), 24.

Muhammad, Z., Anwar, Z., Saleem, B., & Shahid, J. (2023). Emerging cybersecurity and privacy threats to electric vehicles and their impact on human and environmental sustainability. *Energies, 16*(3), 1113.

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science, 43*(1), 115-135. doi:10.1007/s11747-014-0403-8

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2013). Editorial-partial least squares structural equation modeling: Rigorous applications, better results and higher acceptance. *Long Range Planning, 46*(1), 1-12.

Quinlan, C., Zikmund, W. G., Babin, B. J., Carr, J. C., & Griffin, M. (2018). *Business Research Methods* (2 ed.). London: Cengage Learning.

Sulaiman, M. A. (2025). Green product innovation as a mediator between green market orientation and sustainable performance of SMEs. *Sustainability, 17*(4), 1628. doi:https://doi.org/10.3390/su17041628

Awain, A. M., Asad, M., Sulaiman, M. A., Asif, M. U., & Shanfari, K. S. (2025). Impact of supply chain risk management on product innovation performance of Omani SMEs: Synergetic moderation of technological turbulence and entrepreneurial networking. *Sustainability, 17*(7), 2903. doi:https://doi.org/10.3390/su17072903

Sulaiman, M. A., Asad, M., Awain, A. M., Asif, M. U., & Shanfari, K. S. (2024). Entrepreneurial marketing and performance: Contingent role of market turbulence. *Discover Sustainability, 5*, 1-20. doi:https://doi.org/10.1007/s43621-024-00710-8

Asad, M., Fryan, L. H., & Shomo, M. I. (2025). Sustainable entrepreneurial intention among university students: Synergetic moderation of entrepreneurial fear and use of artificial intelligence in teaching. *Sustainability, 17*(1), 290. doi:https://doi.org/10.3390/su17010290

Vinzi, V. E., Chin, W. W., Henseler, J., & Wang, H. (2010). *Handbook of partial least squares* (Vol. 201). Berlin: Springer.

Sarstedt, M., M.Ringle, C., Smith, D., Reams, R., & F.HairJr, J. (2014). Partial least squares structural equation modeling (PLS-SEM): A useful tool for family business researchers. *Journal of Family Business Strategy, 5*(1), 105-115. doi:https://doi.org/10.1016/j.jfbs.2014.01.002

Chin, W. W. (2009). How to write up and report PLS analyses. In *In Handbook of Partial Least Squares: Concepts, Methods and Applications* (pp. 655-690). Berlin Heidelberg: Springer .

Geisser, S. (2017). *Predictive inference.* Chapman and Hall/CRC,.

Chin, W. W. (1998). The partial least squares approach to structural equation modeling.