applied sciences

MDPI

Article

Determinants of Cyberattack Prevention in UAE Financial Organizations: Assessing the Mediating Role of Cybersecurity Leadership

Nabil Hasan Al-Kumaim * and Sultan Khalifa Alshamsi *

Faculty of Technology Management and Technopreneurship, Universiti Teknikal Malaysia Melaka (UTeM), Durian Tunggal, Melaka 76100, Malaysia

* Correspondence: nabil@utem.edu.my or nhs1426@yahoo.com (N.H.A.-K.); p061820006@student.utem.edu.my (S.K.A.)

Abstract: Cyberattack prevention factors have a significant impact on the perception of social and moral values in the business context. Despite leaders' significant role in encouraging and enculturating cybersecurity practices in their organizations, there is a noticeable gap in the literature to highlight empirically how leaders and top management in organizations foster organizational cybersecurity. Therefore, this study aims to explore the role of cybersecurity leadership in financial organizations in preventing cyberattacks and investigate other human and non-technical factors related to the individual in financial organizations. Based on Protection Motivation Theory (PMT), the research framework was developed with the tallying of new variables focusing on the role of an organization's cybersecurity leadership, training frequency, and the role of government frequent alerting. This research employed a quantitative research method. The data were collected through a questionnaire from 310 financial executive officers from selected banks in UAE that use digital technology to enhance their daily banking operations. Using Structural Equation Modelling (SEM), the results indicated (1) a significant association between all investigated independent variables and cybersecurity leadership through hypothesis (H8–H14); (2) cybersecurity leadership mediates the relationship between investigated independent variables and cyberattack prevention, from hypothesis (H15, and H16–H22); (3) no significant association between investigated independent variables and cyberattack prevention from hypothesis (H1–H6), except hypothesis (H4 and H7), which show a significant association. The coefficient of cybersecurity leadership in this study is viewed as a prevention element against cyberattacks based on the findings. With greater cybersecurity leadership success, the implementation of cyberattack prevention increases. This study emphasizes the importance of cybersecurity leadership in a cyberspace environment that protects against cyberattacks and promotes cybersecurity awareness within financial organizations and society in UAE.

Keywords: cyberattack prevention; protection motivation theory; cybersecurity leadership; frequent training; government frequent alerting

check for updates

Citation: Al-Kumaim, N.H.; Alshamsi, S.K. Determinants of Cyberattack Prevention in UAE Financial Organizations: Assessing the Mediating Role of Cybersecurity Leadership. *Appl. Sci.* **2023**, *13*, 5839. https://doi.org/10.3390/app13105839

Academic Editor: Juan Francisco De Paz Santana

Received: 2 March 2023
Revised: 3 May 2023
Accepted: 5 May 2023
Published: 9 May 2023

1. Introduction and Research Gap

Cyberattacks are acts executed by a knowledgeable technologist whereby information is illegally accessed and stolen [1]. Moreover, a cyberattack destroys and corrupts the data files, which will impact the financial health of both the individual and the organization [2]. Many countries are affected by the dilemma of cybercrime or cyberattacks [3]. The rapid growth of the financial sector is an essential economic indicator of a country; however, it has made the UAE vulnerable to the threat of cyberattack [4]. The foundation of cyberattacks is linked to illegal activities by accessing private and sensitive data to threaten individuals or organizations or to gain profit by selling stolen information on the black market [5]. Moreover, the UAE has become a main target of cybercrime as a result of its booming economy and tourism [6]. Thus, its integral characteristics of technological development rate the UAE's digitalization and technological adoption level of awareness and knowledge of how to defend against identity theft and phishing [7].

Identity theft occurs due to individuals and organizations accessing digital technology on sharing information globally, which made the information susceptible to cyberattack activity [8]. Identity theft has arisen since the development of digital technology in its scope and breadth, attacking information stored online [9]. The identity theft phenomenon occurred rapidly in the UAE because the UAE is moving towards a digital hub for innovation and bringing innovative future technologies that focus on online access globally [6]. Identity theft usually occurs in the banking sector of the UAE, where fraudulent transactions occur through stealing money from an existing account and using personal information to initiate transactions.

In addition, phishing is a cyberattack that uses disguised email as a weapon to trick the email recipients into believing that the message is something they want or requested from their bank or their company [10]. According to Check Point Research, cyberattacks on organizations increased by 32% globally compared to the second quarter of 2021, while the UAE detected an average of 970 weekly attacks per organization in the second quarter of 2022, a massive 178% increase year-over-year [11]. Kaspersky's information revealed that phishing attacks and social engineering targeting individuals had increased by an alarming 230% in the UAE in the second quarter of 2022 [12]. The information is then used to access important accounts and can result in identity theft and financial loss. Globally, the UAE was ranked 9th after a higher number of phishing attacks on a bank [7]. Moreover, the UAE Banks Federation has rolled out warnings against fraud schemes, fake callers, and anonymous entities that resort to tricks to extort money from account users. Therefore, developing the conceptual framework of cyberattack prevention factors and cybersecurity awareness will reduce the damage to banking reputation, which leads to a reduction in profits, and affects relationships between parties vested in the business.

Hence, cyberattack prevention is still lacking in terms of deterrence for banking institutions that become victims of financial loss due to the identity theft of corporate information and financial information that generally incur associated costs [6]. Therefore, the efforts to develop a conceptual framework of cyberattack prevention and organizational cybersecurity culture are still in demand and can be used as guidance to prevent cyberattacks within the banking context and other similar financial organizations.

Furthermore, many organizations have implemented technical and physical cybersecurity measures as their source of preventing cyberattacks, where cyberattacks require a comprehensive approach that consists of improved security and risk management in the digital world on protocols, schemes, and standards [13,14]. Nevertheless, the majority of studies investigate factors to prevent cyberattacks from technical perspectives for the digital crime problem [15–17], but there are insufficient studies that investigate factors relevant to organizational factors and the role of leadership in cybersecurity awareness in leveraging cybersecurity behavior in banks and business organizations [18,19]. Therefore, this gap needs to be addressed in this research.

Moreover, cyberattack factors play a major role in showing evidence of the business impact on the world and society that is shaped by the influence of cyberattacks as a digital threat [20]. Furthermore, almost all businesses are starting to learn about technology transformation, focusing on the skills possessed by venture capitalists in the business innovative process for safety and protection [21]. Therefore, there is a need to study the role of skilled leaders in financial organizations in the UAE in preventing cyberattacks and investigate other human factors related to the individual in financial organizations in the UAE in preventing cyberattacks [1,16,22,23]. In line with that, this study has three bold research objectives. First, to propose a model of cyberattack prevention for financial organizations in UAE. Second, to identify and examine the factors that prevent individuals from being victims of cyberattacks in finance organizations in the UAE. Third, to examine the cybersecurity leadership mediating role between the investigated factors of cybersecurity protection and cyberattack prevention.

Substantially, in addition to employing and examining cyberattack preventive measures based on protection motivation theory, this research introduces and examines newly emerged cyberattack preventive measures, which are highly relevant to the banking sector and that can be generalized to other financial institutions and big business organizations. The new proposed preventive measure variables were derived from related research and will be presented in the next subsection in the form of three variables illustrated as follows: two independent variables, (a) frequent organizational training (b) frequent government alerting; and one mediating variable known as (c) cybersecurity leadership.

This paper is organized so that the next section of this article will include the background information on the research and related studies. Next is a description of how the research framework and hypotheses were developed. Then, the applied research method to develop and validate the instrument to collect data is presented. The analysis of the data and the findings are then presented and discussed. The study is ended with a conclusion and the implications of the research.

2. Research Background and Related Work

Cyberattacks are a type of harassing and anti-social behavior utilizing technology with a plan to cause someone mischief, distress, or personal loss [24]. This incorporates mobbing, stalking, and any type of misuse online. Cyberattack refers to unlawful acts wherein the computer is either a device or target or both [25].

2.1. Types and Classification of Cyberattacks

Cyberattacks are becoming widespread in the realm of technology today. Criminals attack internet users' information for their advantage. They are signed into the dark web to buy and sell illicit things and services [26]. Cybercriminals also have access to classified government data. Cyberattacks are rapidly high impacting, costing businesses and individuals billions of dollars annually [27]. Cyberattack targets organizations and individuals, where the attackers usually target businesses for straight financial benefit or to sabotage or undermine operations. They select individuals as a significant part of large-scale scams, or to deal with their devices and use them as a stage for criminal activity, as shown in Table 1.

Table 1. The types of cyberattacks.

Cyberattack Category	Types of Cyberattack	Classifying	References
Target networks or devices	Malware	Comprised of code created by cyber-attackers, intended to make broad harm to information and systems or to increase unauthorized access to a system through delivery as a connection or document over email and it is vital for the client to tap on the connection or open the record to execute the malware.	[4,28]
	Viruses	Computer programs that join themselves to or contaminate a system or documents and tend to move to other computers on a system by disrupting the computer activity and influencing the information stored by changing it or by erasing it.	[29,30]
	DoS Attacks	Used to make a web-based service unavailable and bring the model down by overpowering the webpage with traffic from a variety of sources and saving malware on users' computers for hacking into the system once the network is down.	[31,32]
Using devices in criminal activities	Phishing emails	Hackers send malicious email connections or URLs to clients to obtain access to their records or computer through emails that are not hailed as spam and clients are fooled into messages asserting that they must commute their secret key or update their data, offering criminals access.	[33,34]
	Identity theft	Accessing a user's personal information to take funds, obtaining confidential data for planning a criminal activity, and claiming government benefits from the user's name through discovering user's passwords by hacking, recovering individual data from web-based, or sending phishing messages.	[4,35]
	Cyberstalking	Includes online badgering, where the client is exposed to plenty of web-based emails and messages that threaten a user and impart fear by knowing them and causing the individual to feel afraid or worried about their safety.	[36,37]
Advanced threats in cloud and smart phone applications	Threats in the cloud system environment	It includes the most common threats in the cloud system, which are account hijacking, data sanitization, data control and malicious insider.	[38–40]
	Cyberattacks using smart phone and its applications	It includes (a) smartphone attacks at the physical device domain, (b) smartphone attacks at the network connectivity domain and (c) smartphone attacks at the application domain.	[41,42]

Based on Table 1, these types of cyberattacks caused a critical risk to the people who use the internet, with a great attack on user information. Cyberattacks are the greatest threat to every profession, every industry, and every organization that needs preventive measures encountering them.

Human factors are the weakest link in the rising number of cyberattacks, according to a previous literature review [19]. According to earlier studies in the field, hackers and other criminals targeted employees and support staff for mistakes to enable harmful incidents against an organization [43,44]. For instance, earlier research revealed that humans, either purposefully or unconsciously, were responsible for 95% of malware and ransomware attacks [45,46]. Although many researchers focused on internal human variables that intentionally encouraged cyberattacks, more recent research has revealed a rise in unintentional human factors that encourage cyberattacks. Unintentional human factors enhanced cyberattacks on organizations, according to the majority of qualitative studies [44,47–49] in various reviews. As an illustration, Kadena and Gupi [50] found that organizational management made the majority of unintended attacks on the organizations' information systems possible. For instance, not many individuals in leadership roles actively encouraged and promoted technology use among their staff. Aldawood and Skinner [51] found that employees' lack of use of technology hampered their capacity to detect social engineering trickery utilized by hackers. Rahman et al. [46], Ani et al. [52], and Nifakos et al. [53] all reported findings of a similar nature. According to Rahman et al. [46], many organizational staff members leave work without shutting off of their computers or use passwords that are too simple, making them vulnerable to hacking. Leaving laptops and computers unattended gives offenders the opportunity to install malware or disclose sensitive data. According to [52], making cybersecurity lessons and training mandatory will increase leaders' and employees' capacity for data security and make it easier for them to spot cyberattacks, hence reducing the risk of unintended data breaches. Rahman et al.'s [46] research also revealed that having the necessary skill set and a good attitude towards technology use reduced unintentional data breaches. According to Maalem Lahcen et al. [54] and Aldawood and Skinner [51], encouraging cutting-edge cybersecurity education not only increased awareness of cyberattacks and cybercrimes, but also encouraged creating passwords that were both strong and simple to remember. Users of technology were also allowed to log out each time they finished an activity to prevent unauthorized access thanks to increased employee and leader attention to the usage of technology and innovative education. Education would also assist leaders in addressing difficulties with exhaustion by encouraging technology use, inspiring their staff to develop their technological skills, and utilizing the same technology to address deliberate interruptions and complacency. In addition to training initiatives, Wong et al. [45] and Georgiadou et al. [47] noted the importance of organizational climate or culture in enforcing cybersecurity. While Hadlington [48] addressed enforcement through behavioral encouragement, Ramlo and Nicholas [49] supported the application of best practices, Randall and Allen [44] suggested alternative enforcement measures, including law enforcement agencies and the building of infrastructure.

2.2. Cyberattacks in UAE

The internet is the best creation and profoundly affects all parts of present-day living. It makes organizations and people vulnerable to cyberattacks [6]. Cyberattack rates are on the rise around the world. Most cybercrimes are related to financial and reputation damage, loss of privacy, and penetration of protected information [55]. The UAE has the most significant web-associated populace in the entire Middle East, with 85% of the population utilizing the web. The internet and social media are widely used in the UAE, and this is accompanied by an increase in instances of cyber victimization [6]. Additionally, these cyberattacks are difficult to demonstrate and criminals are ordinarily focused on the UAE occupants due to the overall economic status and the exceptionally high speed of utilizing advanced gadgets.

Available statistics and patterns highlight how serious the threat is: Cyberattacks increased by 50% globally and by a staggering 71% in the UAE in 2021 compared to levels in 2020. The average number of cyberattacks per company per week during the fourth quarter of 2021 was 925, compared to 408 in the UAE. The UAE had a 250% surge in cyberattacks in 2020 throughout the epidemic, including 1.1 million phishing attempts—the most common method for launching ransomware assaults. As a result, ransomware increased significantly, affecting 78% of UAE firms in 2020 (up from 66% in 2019) and being spread by more than 33% new ransomware threat groups [56]. In this manner, the UAE is facing malicious email assaults and is affected by phishing exercises. Moreover, scammers pose as bank agents and request the victim's bank information, because of credit card overcharge or blocked, where scammers can utilize the data to obtain access to the account's money. Additionally, a huge increase in the use of online payment and e-services has encouraged cybercriminals to select victims due to the low danger and possibility of high money available through cyberattacks.

2.3. UAE Initiatives to Prevent Cyberattacks

Technology is profoundly changing the desires of organizations and individuals. In UAE, the government has explicitly expressed that conventional procedures should be ceaselessly refreshed to guarantee proficiency and speed in government activity [57]. However, these technological advancements have come with greater security risks. UAE governments should integrate security with their developments and innovations [58]. Clients must be continuously aware of the wide extent of cyber threats because obtaining monetizable data is the essential goal of cyberattacks, and the Middle East is seeing a deluge in political and vital hacking.

The awareness of cybersecurity is still moderately poor in UAE [3]. With the enormous advancement of innovation and technology, cybercriminals can imitate the user's voice or signature to con others and take their money. Therefore, UAE is the first nation in the region to introduce a cyber-crime law to prevent cyberattacks, yet these laws should be regularly refreshed to coordinate the rapid advancement of technology [59]. In September 2017, the Dubai Cyber Security Strategy was launched by H. H. Sheikh Mohammed bin Rashid Al Maktoum, Vice President and Prime Minister of the UAE and Ruler of Dubai, to reinforce Dubai's situation as a world leader in advancement, security, and safety. The Dubai Cyber Security Strategy follows the innovative advancement change, and deal with difficulties and dangers in a way that is expected to prevent cyberattack scenarios [60].

The focus was on cybersecurity (strategy), which is expected to manufacture safe cyberspace by setting up controls to secure the credibility, protection, accessibility, and confidentiality of information. Moreover, the prevention emphasizes the cyber-smart nation (managerial), which means raising public awareness of the significance of digital security, guaranteeing a society that is completely mindful of the risks of cybercrime and cyber resiliency (operational) that keeps up the adaptability of the internet and guarantees the continuity and accessibility of cybersecurity in the event of any cyber-attacks.

2.4. Theoretical Background and Hypotheses Development

Underpinning Theory

The dominant variance for the theoretical argument of this research is derived from protection motivation theory, which serves to relate the reality of security threats to organizational end-users that convey actions in achieving the overall system security. Protection Motivation Theory (PMT) makes sense of the health evasion behavior that is connected with the impression of dangers and self-viability ability to make a successful move to reduce risk [61]. The assumption of the theoretical framework from the Protection Motivation Theory is to expand the proposed framework of cyberattack prevention. This is inevitably an indication of encouraging a healthy, safe and secure workplace environment. The Protection Motivation Theory explains a singular affinity to take part in willful secure behaviors [62], as expressed in Figure 1.

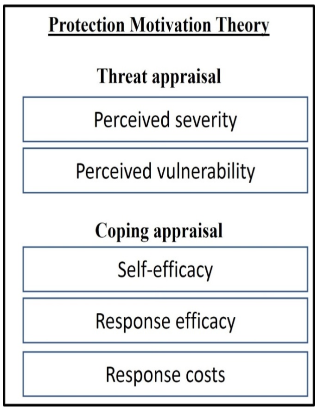

Figure 1. The Protection Motivation Theory, adapted from Rogers (1975) [62].

Based on Figure 1, the Protection Motivation Theory embodies five (5) appraisals underpinning those impacts: (1) perceived severity of the severe consequences that influence the likelihood of engaging in a potential cyberattack behavior, (2) perceived vulnerability can communicate the degree of cyberattack risk for a specific hazard if a current cyberattack behavior is continued, (3) self-efficacy estimate of the cyberattack threat behavior that complies with recommendations to detach the warning, (4) response efficacy reliance in the ability to implement the recommended coping cyber-attack behavior, and (5) response costs associated with carrying out the preventive coping response by completing the cyberattack behavior [61,63]. Derived from the literature review, the study has embraced these five (5) appraisals, as specified in Table 2.

Table 2. The protection motivation theory appraisals.

Appraisals	Specify	Definition	References
Perceived severity	Threat appraisal	An organization's perception of the seriousness of a cyber-attack is left untreated.	[61,64,65]
Perceived vulnerability		An organization's perception of risk contracting in a cyber-attack condition.	[61,66,67]
Self-efficacy	Coping appraisal	Confidence to continue the cybersecurity behavior and overcome temptations.	[61,68,69]
Response efficacy		The perceived effectiveness of taking action to improve cybersecurity.	[61,70,71]
Response costs		The perceived impediments to taking action to improve cybersecurity conditions.	[61,72]

The protection motivation theory will be a new approach to delivering cybersecurity awareness in the banking sector. Protection motivation theory is also one of the most interesting speculation theories that have been accentuated in the cybersecurity awareness setting. However, the theory demonstrates only two (2) measures while conveying a choice under threat, which are (1) threat appraisal that guarantees that security guidelines are reasonable and seen for the organizational climate and (2) coping appraisal that guarantees threat data are joined by useful data in deferring it, which is appropriate for this research setting in a banking climate. Consequently, embracing the Protection Motivation Theory for this research will demonstrate the serious threat that is likely to occur in a banking institution and can effectively reduce the danger through drawing in the anticipation conduct, which cautions the cyberattacks difficulty. Considerably, this research aimed to introduce and examine new additional cyberattack preventive measures that are highly relevant to financial and big banking and business organizations. The new proposed preventive measure variables were extracted from related studies and will be presented in the next subsections in the form of three variables illustrated as follows: two independent variables, (a) organization frequent training (b) government frequent alerting; and one mediating variable; (c) cybersecurity leadership.

2.5. New Proposed Cyberattack Prevention Factors

2.5.1. Organization Frequent Training (OFT)

Perhaps the most well-known way cybercriminals gain admittance to financial organizations' information is through their workers. Cybercriminals will dispatch false emails mimicking somebody in a financial institution and will either request individual information or access specific records [59]. Interfaces frequently appear to be authentic to an undeveloped eye and it is not difficult to fall into the trap. In this manner, employee mindfulness is crucial for a financial organization. Perhaps the most proficient method for safeguarding against cyberattacks and all types of data breaks is to train and alert financial institution employees on cyber-attack prevention and inform them of current cyberattacks [73]. Organizations should have frequent protection training against email phishing and scams performed by phishers, hacktivists, and cybercriminals through educating individuals about vulnerability to malware, ransomware, spam, and hacking. Organizations need to educate their employees on cybersecurity supposing that workers do not have the foggiest idea how to perceive a security danger, and how might they be supposed to keep away from it, report it, or eliminate it.

2.5.2. Government Frequent Alerting (GFT)

Moreover, workers need online cybersecurity training to protect themselves and the organization against cyber-attacks. The government also provides frequent alerts about possible major cyberattacks and take measures to prevent and minimize the impact of any such attack. These alerts focus on the punishment over data breaches and the sale of personal information of the public, which is now being used in scams. The government must always prioritize the safety of its IT infrastructure and critical systems and had outlined measures needed to secure these assets. Therefore, government frequent alerting will detect and prevent these attacks from compromising financial organizations' networks. Thus, in the context of cyberattack anticipation variables, government frequent alerting and organization frequent training can be included as indicators in creating cybersecurity awareness. Therefore, the new additional component of cyberattack prevention factors is shown in Table 3.

Table 3. Cyberattack prevention; new proposed and emerged factors.

Cyberattack Prevention Factors	Definition	Impacts on Organization	References
Organization frequent training	Cybersecurity training that assists workers to protect themselves and the organization from cyberattacks and threats.	Enhancing service efficiency and effectiveness in sustaining long-term viability in preventing cyber-attacks and threats.	[73–75]
Government frequent alerting	The government provides an assortment of data for clients in cyberattacks and alerts them.	Increase competitiveness capability in the government that obtains knowledge on the cyberattacks and threats.	[76–78]

2.5.3. Cybersecurity Leadership Role and Impact

In recent years, cybersecurity leadership was rarely highlighted in the research as an essential part of organization culture. This is because cybersecurity concerns were limited to certain technical people in the organization. Moreover, people inside the organization deal with cybersecurity as a technological issue [18]. However, with dramatic advancements in ICT, internet, knowledge of social engineering and their applications, cybersecurity is no longer solely a technological matter. Therefore, cybersecurity issues are no longer limited to technical measures to be followed in the organizations that involve users' sensitive financial information and data transactions [79,80]. We believe that cybersecurity is a sociotechnical issue and in some cases, irresponsible human related behavioral factors often represent the most breakable link in the chain in the organization that deter creating a safe digital environment. In other words, "cybersecurity is no longer the concern of just the IT department. Within organizations, it needs to be everyone's business including the organization leaders and top management" [81]. Cybersecurity is now an essential matter in every organization, not only those that are involved in money transactions, but also sensitive information flow, and leveraging cybersecurity awareness should be the responsibility of the organizations' top-level managers and leaders. Given that, cybersecurity leadership was defined in some previous studies as the role of organization leaders in mitigating risk and preventing organizational exposure to cyberattacks by leveraging cybersecurity awareness through setting, measuring and evaluating cybersecurity goals, strategies and policies within the organization [81–83]. As an authors of this research, we try to introduce the concept of cybersecurity leadership in a more simple and comprehensive way as the capability of organization's top-level managers to enculture cybersecurity awareness, technical skills and practical knowledge in the employees' mindset through setting, monitoring and evaluating some cybersecurity leadership indicators and components. Essential parts of these cybersecurity leadership components as shown in Table 4: first, setting the cybersecurity goal and strategy; second, positioning the cybersecurity functions; and third, implementing and evaluating the cybersecurity activity.

Cybersecurity leadership must take stronger and essential influential leadership positions inside their organizations during crisis conditions [84]. Additionally, cybersecurity leadership needs to be exceptional with basic information on arising patterns in cybercrime and the cybersecurity climate. Cybersecurity leadership plays a mediating role in risk exposure awareness that identifies continuity planning within the organization.

Numerous businesses are battling to build cybersecurity as a proactive piece of their day-to-day activity [55].

The financial organization has been a popular target for cybercriminals for a long time. According to Kaspersky (2019), in the past years alone, financial organizations suffered more than 1509 incidents with 184 confirmed data disclosures [85]. The high value of these data on the darknet makes these financial institutions an attractive target for cybercriminals. Additionally, progress in internet banking, mobile apps, and instant payments all require innovation that builds the financial business attack on new weaknesses. The present financial institution pioneers should be able to insert cybersecurity throughout their business activities in response to cyberattacks. They should have the option to lead by recruiting security chiefs that can foster abilities to prevent cyberattacks. Additionally, the financial institution needs cybersecurity leadership, especially Chief Information Security Officers, who are taking a strategic and stronger job inside their financial institution.

The overwhelming test for the leadership is to safeguard the financial institution's digital resources and foundation while guaranteeing activities without interference. For example, cybersecurity groups are currently changing their risk management and security programs to empower the reception of cloud services and online transaction instruments. With the digital ecosystem being a powerful climate, cyber dangers frequently develop before guidelines. Consistently, leaders settle on choices affecting security, and keeping the financial institution secure is everybody's liability. Security pioneers need to assist representatives with remaining secure by consistently preparing them to distinguish phishing endeavors, scammers, and online credit card frauds and proactively instructing them about new methods emerging in the digital world. Table 4 shows the elements of cybersecurity leadership components that can be used as a mediator in fostering the proposed research framework and cyberattack prevention. On the other hand, Cybersecurity leadership begins at the top, with the chief information officer (CIO) and chief information security officer. Cybersecurity leaders need to be up to speed on information security issues from a technical standpoint, understand how to implement security planning into the broader business objectives, and be able to build a longer-lasting security- and risk-based culture [19].

Table 4. The cybersecurity leadership components.

Components	Definition	Impacts on Organization	References
Setting the cybersecurity strategy.	Building the cybersecurity strategy that safeguards the business and reduces the risk of openness in their functional exercises.	Reorganizing the cybersecurity strategy to boost the way electronic documents are developed, kept, modified, stored, and obtained.	[84,86,87]
Positioning the cybersecurity functions.	Slotting cybersecurity inside the Information Technology purpose through the tasks, policy and advanced foundation that forestalls cyberattacks.	Access cybersecurity control is used to mitigate risk by regulating the number of people who can make, access, change or erase files saved in particular folders.	[20,88,89]
Implementing the cybersecurity activity.	Prioritizing cybersecurity specialized abilities that revamp the organization's advanced design and secure the information break from the cyber-attackers in their day-to-day activities.	Labeling cybersecurity activity documents constantly by subsequent collection events may considerably enhance the storage and access of records.	[73,86,90]

3. A proposed Cyberattack Prevention Framework and Hypothesis Development

3.1. Perceived Severity

According to [64] Briggs et al. (2017), integration changes bureaucratic structures, increasing the functional quality of cyberattacks and requiring appropriate flexibility inside the company to stop them. The perceived severity of a cyberattack as perceived by an enterprise is not addressed [61,64,65]. In terms of picking from the response obtained through back excitation, perceived severity is measured [67]. One can ask someone how they feel about the possibility of falling victim to cyberattacks, and responses such as "not stressed" or "very restless" are indications of how terrified they are of the threat. The perceived severity of the serious repercussions affects the propensity for a prospective cyberattack behavior. The unpleasant repercussions a person identifies with an event or result, such as a cyberattack behavior, are referred to as perceived severity. These effects may be related to a potential future occurrence, a present condition, such as a cyberattack issue, or both [65]. Although it goes by a more generic name, the idea of severity as a significant behavioral factor has been discussed in a variety of theories and across numerous academic areas [61,64,65]. Although the concept of severity might be viewed as an illustration of negative utility and negative valence, the phrase itself seems to have its origins in the Protection Motivation Theory. Some scholars have concluded that vulnerability, severity, and efficacy should multiply together so that if any one of these three factors has a value of zero, motivation will be zero [61,64,65]. Therefore, a hypothesis related to perceived severity can put forward as:

H1: *Perceived severity has a positive, significant relationship with cyberattack prevention.*

3.2. Perceived Vulnerability

Perceived vulnerability denotes a predetermined circumstance that reduces the perceived danger of a cyberattack and labels the places where an appropriate approach must be rethought each time [79]. According to [67], a cyberattack approach is one in which a company gains control over a previously perceived risk that is easier to view and avoid. In the aftermath of a cyberattack, an organization experiences [17,61,66,67]. The one conviction that is defenseless against a potential threat of a cyberattack is perceived vulnerability [71]. For instance, the person may be asked to provide information about their traits and finances through an email that serves as a genuine foundation to lure individuals in. If a certain hazard persists, perceived vulnerability can indicate the likelihood of a cyberattack for that risk. There are numerous operationalizations of perceived vulnerability (possibility, probability, likelihood), and no clear-cut measuring method or plan has yet been devised [71]. There are other techniques of assessment, though, and there are differences between them. These types of basic absolute vulnerability questions have the major flaw of confusing expectations, intentions, and current risk behavior, which leads to issues with cybersecurity [61,66,67]. Measures to reduce perceived vulnerability aim to make people think about expected or intended behavior in the future, preventing expectations, intentions, and current risky behavior from being confused with perceptions of susceptibility. As a result, conditional measures enable researchers to evaluate risk perceptions in individuals who are not presently engaged in the action, but may do so in the future. Additionally, they can be used to differentiate between perceived vulnerability under both preventive action and inaction. Accordingly, it can be hypothesized that:

H2: *Perceived vulnerability has a positive, significant relationship with cyberattack prevention.*

3.3. Self-Efficacy

Every time an effort is made to integrate cybersecurity aspects more deeply into the procedures of the organization's daily operation, self-efficacy underlines the critical cyberattack behavior [68]. A previous study [69] reported that cyberattack behavior happens when coworkers complete each other' jobs, which exposes important departmental interaction data and increases internal temptations. Self-efficacy is the confidence to maintain cybersecurity habits and resist pressure [61,68,69]. Self-efficacy is concerned with the conviction that one possesses the skills necessary to resist a cyberattack, which is assessed by a replies statement [91]. The self-efficacy assessment of cyberattack threats behavior involves adhering to advice to remove the warning. A person's self-efficacy relates to the confidence in their ability to carry out the behaviors required to achieve particular performance goals. The belief in one's capacity to exercise control over one's motivational behavior and social environment is known as self-efficacy [91]. The goals for which people strive, the amount of effort put out to obtain goals, and the possibility of achieving particular levels of behavioral performance are all influenced by these cognitive self-evaluations. Self-efficacy beliefs, unlike conventional psychological notions, are anticipated to change according to the operating domain and the environment in which an action occurs. These cyberattack effects could be explained by the lack of sufficient levels of challenge in efficacy measures that are relevant to the target sample [61,68,69]. Additionally, scoring procedures that limit the range of acceptable responses could result in abbreviated data. As a result, predictions of behavioral performance are limited due to the lack of sensitivity to variations in self-efficacy. Therefore,

H3: *Self-efficacy has a positive, significant relationship with cyberattack prevention.*

3.4. Response Efficacy

The key to ensuring shared cybersecurity components' long-term survival in the company is to take action with outstanding perceived effectiveness, which is the emphasis on response efficacy [70]. According to [71], increasing accessibility involves adopting yearly cybersecurity evaluations and organizational goals for self-improvement in cyberattack prevention. Response efficacy is the perceived value of making changes to increase cybersecurity [61,71]. Response efficacy is the conviction that adopting a particular activity will lessen the threat of a cyberattack [70]. Whether a response is effective depends on the user's capacity to carry out the advised countermeasures. Response efficacy is the perception that the suggested course of action will truly prevent the threat. The individual's conviction that the suggested activities will be successful in lessening or removing the perceived threat [61,70,71]. The goals that people pursue, the amount of effort put out to pursue goals, and the chance of achieving particular levels of behavioral performance are all influenced by these cognitive response efficacies. The Protection Motivation Theory has had a significant impact on clinical treatment, teaching, and research. Cyberattack prevention research frequently evaluates response efficacy, but the evidence for the association between response efficacy and risk behavior is conflicting [61,70,71]. A conclusion such as that, though, would probably be hasty. Bivariate relationships are attenuated and what is being measured is obscured by imprecise operationalization of response efficacy beliefs. Response efficacy significantly affects both the ability one has to tackle issues competently and the decisions one is most likely to make by identifying the beliefs one holds about their ability to alter situations. Therefore,

H4: *Response efficacy has a positive, significant relationship with cyberattack prevention.*

3.5. Response Costs

Response costs highlight the strategic nature of the infrastructure by enhancing the cybersecurity of the company to stop future intrusions [72]. According to Briggs et al. (2017) [64], an operational strategy is required for teaching and creating cybersecurity settings that make it simple for the organization to prevent cyberattacks. The obstacles that action-takers believe are preventing better cybersecurity conditions can be found in [61,64,72]. Response costs are concerned with the values one ascribes to the execution of a cyberattack strategy [64]. Response costs are associated with conducting a cyberattack to complete a preventive coping response [61,63]. In response cost, desirable items, points, tokens, or privileges are withheld in planned, progressive steps after engaging in unfavorable conduct or failing to achieve a predetermined objective. Removing reinforcement for unwanted or disruptive behavior is referred to as response cost. It is frequently employed in conjunction with a token economy and is most effective [72]. The individual loses something they already have or privileges they currently enjoy and anticipate having access to in the future when they behave incorrectly or unfavorably. In response cost, desired items, points, tokens, or privileges are gradually taken away after unwanted conduct or failure to achieve an objective. Response cost is a user's readiness to forego productivity in other areas in order to address a security problem [64]. Additionally, when we take away a reinforcement or a chance for a reinforcement from cybersecurity in reaction to challenging behavior, this is known as response cost. Many people believe that response cost is natural to include in the use of a reinforcement system since we are prone to taking things away as punishment for wrongdoing in our society. Therefore,

H5: *Response costs have a positive, significant relationship with cyberattack prevention.*

3.6. Organization Frequent Training

For a business to conduct its everyday operations, periodic training will teach employees the best practices and values for preventing cyberattacks in an extended cybersecurity environment [74]. According to Quader and Janeja (2021) [75], the majority of security awareness training initiatives concentrate on the most-recent network breaches and ongoing threats. Employees who receive cybersecurity training can better defend themselves and the company against online threats and attacks. An organization's frequent training improves service performance and efficiency to maintain long-term viability and stop threats and cyberattacks [73–75]. Organizations regularly train employees on email phishing scams used by hackers, hacktivists, and cybercriminals by letting them know how susceptible they are to a virus, spam, ransomware, and hacking. If workers don't have the slightest concept of how to identify a security risk and how they can be expected to avoid it, report it, or eliminate it, then organizations must teach them about cybersecurity. Organizational regular training will help employees recognize and eliminate cyberthreats and protect their most important assets [73]. Employees can therefore identify security breaches and prevent them by recognizing the threat level as spam, phishing, and malware, which are common occurrences in the workplace. Additionally, employees require online cybersecurity training to defend both themselves and the company from cyberattacks. Perhaps the most effective way to protect against cyberattacks and all forms of data breaches is to educate financial institution staff about how to prevent cyberattacks and keep them informed about recent hacks [73]. Employee mindfulness is essential for a financial business in this way. Therefore,

H6: *Organization frequent training has a positive, significant relationship with cyberattack prevention.*

3.7. Government Frequent Alerting

Government alerts will be sent frequently and will provide information on various cyberattacks that stress the many technical interests in swiftly preventing assaults [78]. According to Eichensehr (2019) [77], good governance would promote cybersecurity awareness in a community and organization by creating a cyberspace ecosystem that protects against cyberattacks. In cyberattacks, the government informs clients and gives a variety of data. Government frequent alerting boosts the government's ability to compete by providing knowledge of cyber threats and attacks [76–78]. People will be aware of current and real cyber threats because of the government's frequent alerts, which will affect their daily security framework [76] Additionally, it will set up core security measures so that people can defend themselves against such assaults. From the perspective of an association, cybersecurity leadership should understand their models and protect the company's data and financial information. In addition, the government regularly issues warnings about potential significant cyberattacks and takes action to stop and lessen the effects of any such attack. This warning focuses on the public's personal information being sold and how it is now being exploited in scams as payback for data breaches. The government has detailed the steps required to secure these assets and must always place a high priority on the security of its IT infrastructure and vital systems. Therefore, frequent government alerting will be able to identify and stop these attacks from compromising the networks of financial firms. Undeveloped eyes typically mistake interfaces for the real thing, and it is easy to be caught in the trap. Cybercriminals will send bogus emails pretending to be someone from a financial institution to either access certain records or request personal information [59]. Therefore,

H7: *Government frequent alerting has a positive, significant relationship with cyberattack prevention.*

3.8. Cybersecurity Leadership

In this study, the researchers anticipated a direct and indirect positive relationship between perceived severity, perceived vulnerability, self-efficacy, response efficacy, response costs, organization frequent training, and government frequent alerting as proposed independent variables (IVs) and cybersecurity leadership as a proposed mediating variable (MV). In addition, this study's researchers expected a direct positive relationship between cybersecurity leadership as a proposed mediating variable (MV) and cyberattack prevention as a dependent variable (DV). Thus, the analysis of the association between online security behaviors and the perceived severity of perceptions of cybersecurity hazards was aided [65]. According to Briggs et al. (2017) [64], it is now clearer how computer users view the benefits and drawbacks of using antimalware software. Therefore,

H8: *Perceived severity has a positive, significant relationship with cybersecurity leadership.*

The use of technology and the internet for daily operations has expanded, and as a result, both people and businesses are seen as being exposed to cybersecurity leadership [67]. According to Bada et al. (2019) [66], using technology frequently exposes people to many forms of cybersecurity leadership. Therefore,

H9: *Perceived vulnerability has a positive, significant relationship with cybersecurity leadership.*

Organizations must increase their self-efficacy in online security practices to develop training and policy materials that are effective [69]. According to Li and Shang (2020) [92], this knowledge was gathered to implement new regulations that support safe online conduct. Therefore,

H10: *Self-efficacy has a positive, significant relationship with cybersecurity leadership.*

Response efficacy looks into how consumers' attitudes around risk affect their online security behavior [71]. According to Alalehto (2018) [93], both organizations and individuals continue to struggle with cybersecurity leadership on knowledge protection. Therefore,

H11: *Response efficacy has a positive, significant relationship with cybersecurity leadership*.

To promote productivity and efficiency across the board and develop answers to the issues related to cybersecurity leadership, response costs have increased society's reliance on the internet [72]. The extent to which an organization member understands the importance of information security through cybersecurity leadership was mentioned by [65]. Therefore,

H12: *Response costs have a positive, significant relationship with cybersecurity leadership*.

Cybercriminals continue to prosper in their activities, which now involve targeting individual computer users in addition to corporations and organizations, despite constant training provided by organizations to staff members on how to secure digital assets [75]. According to Hamoud and Aimeur (2020) [74], enhancing security awareness will be more cost-effective than investing in technology. Successful and effective information security management relies on it. Therefore,

H13: *An organization's frequent training has a positive, significant relationship with cybersecurity leadership*.

Internet security has been under scrutiny due to an increase in data breaches caused by hacking incidents, which the government constantly warns against [77]. Internet users are aware of the potential cyber hazards, according to Abdalrahman and Varol (2019) [78], but they continue to connect to the internet using their laptops and other smart devices. Therefore,

H14: *Government frequent alerting has a positive, significant relationship with cybersecurity leadership*.

Maintaining business operations will depend on how cybersecurity functions are positioned, and cybersecurity leadership on new practices will lead to effective prevention measures [89]. The influence of moral leadership on behavioral outcomes is crucial in cyberattack prevention, according to Xue et al. (2021) [94]. Therefore,

H15: *Cybersecurity leadership has a positive, significant relationship with cyberattack prevention*.

Successful leadership management within an organization that prioritizes cybersecurity knowledge and plans prevention actions is necessary for cybersecurity leadership [87]. According to Cleveland et al. (2018) [86], operational excellence and the implementation of necessary cybersecurity measures require strategic alignment inside the business. Therefore,

H16: *Cybersecurity leadership has a positive, significant mediation effect between perceived severity and cyberattack prevention*.

Cybersecurity leadership provides real-time communication with the organization's leadership to strategically plan the course and objectives for methodically preventing intrusions [89]. According to Tounsi and Rais (2018) [88], a system of managerial procedures that produced cybersecurity awareness and tailored advice in practical steps against cyberattacks within a company can be classified. Therefore,

H17: *Cybersecurity leadership has a positive, significant mediation effect between perceived vulnerability and cyberattack prevention*.

The finest strategies and activities for resolving cyberattack challenges will be found in an organizational environment that prioritizes cyber awareness, according to cybersecurity leadership [86]. Managing cybersecurity-related risk, according to Lis and Mendel (2019) [90], will center on the infrastructure, direct the cybersecurity action plan, and improve the environment for preventing cyberattacks. Therefore,

H18: *Cybersecurity leadership has a positive, significant mediation effect between self-efficacy and cyberattack prevention.*

Leadership in cybersecurity will lead to a growth in the organization's reliance on its network for day-to-day operations, which requires a proper secure structure against cyberattacks that will impersonate both onsite and offshore network forces [95]. According to [73], to ensure that activities are uninterrupted by cyberattacks and to prevent them in the long run, executives must go beyond compliance monitoring. Therefore,

H19: *Cybersecurity leadership has a positive, significant mediation effect between response efficacy and cyberattack prevention.*

The event that stresses business continuity for cyberattack recovery operations that require a proper action plan and strengthens the affected cybersecurity aspects will be given priority by cybersecurity leadership [20]. According to [84], crucial layered cybersecurity components must be put into place in order to monitor and quickly respond to cyberattack behavior in an organizational setting. Therefore,

H20: *Cybersecurity leadership has a positive, significant mediation effect between response costs and cyberattack prevention.*

To stop threats and cyberattacks and sustain long-term survival, cybersecurity leadership must boost service effectiveness and efficiency [75]. Employees who obtain cybersecurity training can better protect themselves and the company against online dangers and attacks, according to Hamoud and Aimeur (2020) [74]. Therefore,

H21: *Cybersecurity leadership has a positive, significant mediation effect between the organization's frequent training and cyberattack prevention.*

Frequent alerting by the government boosts its competitiveness in learning about threats and cyberattacks [78]. According to [77], the government alerts citizens to cyberattacks and provides a range of information. Therefore,

H22: *Cybersecurity leadership has a positive, significant mediation effect between government frequent alerting and cyberattack prevention.*

3.9. Mediating Effect of Cybersecurity Leadership

Cybersecurity pioneers presently need to move past consistency screens and work towards shared risk proprietorship inside the business. The financial organization construction might have turned crossover; however, there is yet an enormous scope reception of online transaction advances and a lot more noteworthy use of cloud services than any time in recent memory potentially envisioned. Moreover, cybersecurity activities likewise confronted enormous new difficulties. This has made it more difficult for the leadership to keep an equilibrium and guarantee the well-being of their financial organization and instructive resources with online exchanges. Moreover, a cybersecurity model is needed for organizations and leaders must spike cybersecurity achievement [96]. However, focusing on cybersecurity and awareness to relieve potential cyberattacks for future threats requires a strategy.

According to [94], the effect of moral leadership on behavioral outcomes plays an important role in cybersecurity. Their findings showed that the data security environment fully mediates the relation between moral leadership and cybersecurity leadership perspective. However, Lehto and Limnéll (2021) [87] stated that setting the cybersecurity strategy as coordinating actions will manage extensive disruptions and implements a comprehensive security model. Therefore, cybersecurity leadership plays an important role as a mediator in their study to ensure cybersecurity achieves the set of actions as efficiently as possible. A study by Porter (2019) [97] shows that leadership style will be an approach to cybersecurity preventive measures, where the mediation role of cybersecurity leadership sets the tone to elevate cybersecurity dilemmas in an organizational context. Thus, positioning the cybersecurity functions will be substantial terms in the continuity of business operations and cybersecurity leadership on emerging practices will gain relevant prevention measures [89].

Therefore, exploring the mediating effect of cybersecurity leadership will create a new vision and planning for the transformation of behavioral changes to cybersecurity dilemmas [98]. Ogbanufe et al. (2021) [99], in their finding, stated that financial risks are connected with cybersecurity events, hence cybersecurity leadership mediates the consequences of organizational influences and risk management strategy. Consequently, implementing the cybersecurity activities will create a new cybersecurity infrastructure that prevents attacks and requires more attention in performing a supportive role [90]. Moreover, a mediating role of cybersecurity leadership is suggested, which compares leadership manners to cybersecurity functional domains and makes key decisions in the face of cyberattacks through implementing cybersecurity activities [86].

Based on Table 4, explained in Section 2.5.3 above, the cybersecurity leadership components are more important in securing the future threats to an organization's operation. Thus, cybersecurity leadership has not been tended to sufficiently both with regards to innovation and above all, concerning organizational leadership and strategy. In this research, the cybersecurity leadership will act as a mediator in the discovery of the relationship between Protection Motivation Theory and cyberattack prevention. Moreover, cybersecurity leadership will see cybersecurity hazards and influence assets to adjust the requirements for data security and functional security and safeguard against present and future cyber dangers.

3.10. Proposed Research Framework and Reemphasizing Research Gap

The study speculated that there are similar remarkable indicators or recognized elements of the Protection Motivation Theory based on cyberattack prevention as a case study. The proposed research framework begins within this study and discerns cyberattack prevention. This study determined the level of cyberattack prevention based on the Protection Motivation Theory. The study proposed research framework was clarified from the above theoretical and conceptualization evaluation from past studies. This proposed research framework will be related and pre-assessed together with the Protection Motivation measures as cyberattack prevention in a UAE case study, as specified in Figure 2.

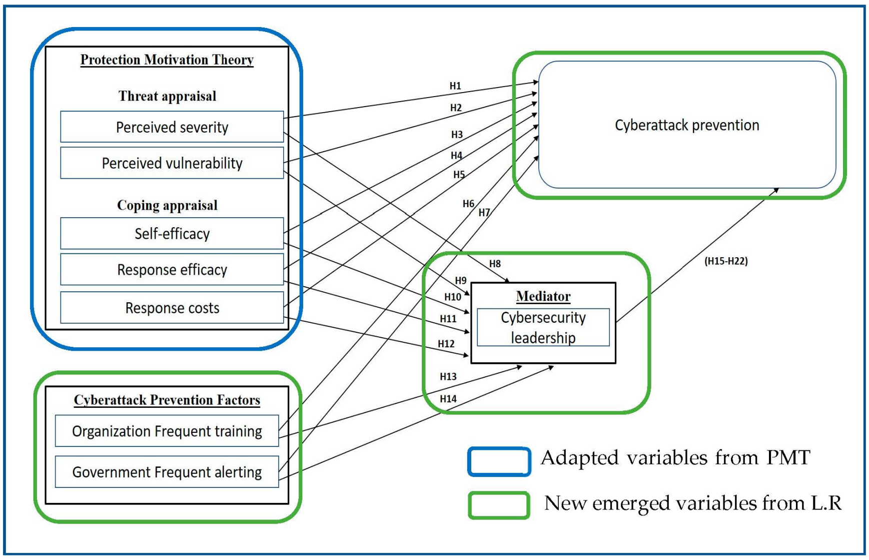

Figure 2. A proposed research framework.

3.11. Reemphasizing Research Gap

The UAE is rapidly becoming a digital innovation center and combining cutting-edge future technology with a global concentration on online access, which has resulted in the identity theft crisis [100]. Therefore, developing the conceptual framework of cyberattack prevention factors and cybersecurity awareness will reduce the damage to the banking reputation which leads to a reduction in profits and affect relationships between parties vested in the business. Nevertheless, the majority of studies investigate factors to prevent cyberattacks from technical perspectives as the digital crime dilemma [15–17,101], but there are insufficient empirical studies that investigate factors relevant to organizational factors and the role of leadership in cybersecurity awareness in the banking institution. Therefore, this is the gap that needs to be addressed in this research. Additionally, there is a need to study the role of skilled leaders in financial organizations in the UAE in preventing cyberattacks and investigate other human factors related to the individual in financial organizations in the UAE in preventing cyberattacks [1,16,22,102]. The study's proposed research framework was clarified from the above theoretical and conceptualization evaluation from past studies.

4. Research Methodology

The proposed research framework's determinants are measured and numerically analyzed using statistical techniques. The quantitative analysis examines the link between these determinants. The quantitative survey approach is used in this study to gather data from the intended respondents. We use random sampling techniques to assure generality, and a Smart PLS 3.0 is used to assess the survey data.

4.1. Instrument Development and Validation Process

4.1.1. Development of Questionnaire

To gather information from respondents, a questionnaire was created as a tool. Each question's content was derived from the prior research that was examined to make the question appropriate for testing the variable from the suggested theoretical framework. The questionnaire was created in English because the respondents for this study would be the financial executive officers from the commercial bank in the Central Bank, industrial bank in the Emirates Industrial Bank, a merchant bank in the Ajman Bank, and Islamic bank in the ADIB bank of the UAE that uses digital technology to enhance their daily banking operation. To ensure that each respondent could complete the questionnaire with the least amount of time and effort, structured questions were employed. To make it easier for respondents to react and analyze the data, the structured questionnaire was separated into listing questions and rating questions, as shown in Table 5.

Table 5. Structure of questionnaire.

No	Question	Measurement	Location of Questions in the Questionnaire	Items
1	Respondents Profile and Cyberattacks Levels and Controls	Multiple Choice Questions	Section 1: Q1–Q11	11
2	Protection Motivation Theory Related Measurements	5-point Likert Scale rating	Section 2: PS1–PS6	6
			Section 2: PV1–PV7	7
			Section 2: SE1–SE6	6
			Section 2: RE1–RE6	6
			Section 2: RC1–RC6	6
3	New Emerged Related Measurements	5-point Likert Scale rating	Section 3: OFT1–OFT6	6
			Section 3: GF1–GF6	6
4	Cybersecurity Leadership Related (CL) Measurements	5-point Likert Scale rating	Section 4: SCS1–SCS6	6 *
			Section 4: PSF1–PSF6	6 *
			Section 4: ICA1–ICA6	6 *
5	Cyberattack Prevention	5-point Likert Scale rating	Section 5: CP1–CP6	6
			Total Items	78

* Authors decided to use only the most tow highest internal consistency items form each construct.

4.1.2. Questionnaire Validation Process

A validity review is used to determine an instrument's validity, which is a measure of the instrument's precision and the degree to which it applies to what is systematic [103].

This research followed series of steps to validate the questionnaire as an instrument for data collection. Therefore, content validity took place to make sure questionnaire contents are relevant to the researched topic and free of linguistic errors. The content validity is performed through two ways, experts' review and pilot test. During experts' content validity, a fundamental component of a successful study design is measuring the survey questionnaire's validity and reliability and carrying out corrections (Hunt et al., 1982 [104]). For this reason, five (5) experts were surveyed, and in addition to using the items from the previous research as the basis for the survey, the survey's content and framework were validated by experts. These experts were academics who are regarded as subject matter experts since they had a Ph.D. in cybersecurity from a public university and have worked for at least five years in the field. The experts were asked to review every question in the questionnaire and make suggestions for changes based on their findings [103]. Following the completion of expert's instrument validation, the questionnaire was prepared for a pilot test. As a result, the study has produced a professional survey that is concisely written, straightforward, and simple to respond to. To confirm the reliability of the instrument, a pilot test was conducted through analyzing the data gathered from 30 bank employee participants, which showed that the value of Cronbach's alpha for all variables was acceptable, ranging from 0.744 for (self-efficacy) to 0.910 for (perceived severity), which indicates good reliability and adequate internal consistency of the measurements. Respondents were asked to rate how much they agreed or disagreed with each statement on a five-point Likert scale (1 = strongly disagreed; 2 = disagreed; 3 = neutral; 4 = agreed and 5 = strongly agreed). Additionally, the respondents were asked to identify any questions that they felt were cloudy or unclear. As a result, the study has produced a professional survey that is concisely written, straightforward, and simple to respond to. Through this pilot test, the questionnaires' content validity was established.

4.2. Sampling Method and Data Collection

Probability random sampling was selected to avoid bias in the research and to ensure that samples are representative of the target population. The printed survey was prepared and handed to targeted financial executive officers to be distributed. We succeeded in distributing more than 368 questionnaires. However, a total of 58 questionnaires were considered defective responses and hence discarded since some respondents returned incomplete responses. As a result, 310 questionnaires were used for the analysis.

5. Analysis and Results

5.1. Respondent Profile and Cyberattacks Levels and Controls

The descriptive statistics of the respondents for the current sample are listed as shown in Table 6. Questions (1–8) were about respondents' profile and demographic information, while questions (9–11) concerned specific information on types of cyberattack encountered, rating level of cyberattack leadership practices and rating levels of success of cyberattack prevention among individuals working in financial organizations.

Table 6. Respondent profile.

Variables (Question Items)	Response	Number	%
1. Gender	Male	263	85%
	Female	47	15%
2. Age	18–24	13	4.2%
	25–34	120	38.7%
	35–44	128	41.3%
	45–54	45	14.5%
	55–64	4	1.3%

Table 6. *Cont.*

Variables (Question Items)	Response	Number	%
3. Work Experience	Less than 5 year	50	16.1%
	5–10	223	71.9%
	11–20	15	4.8%
	More than 20	22	7.1%
4. Nationality	UAE Citizen	45	14.5%
	Non- UAE Citizen	265	85.5%
5. Banking sector	Public Sector	150	48.4%
	Private Sector	160	51.6%
6. Bank category	Commercial Bank	75	24.2%
	Industrial Banks	45	14.5%
	Merchant Banks	30	9.7%
	Islamic Banks	160	51.6%
7. Qualification	Graduate Diploma	55	17.7%
	Bachelor's degree	160	51.6%
	Professional Qualification	33	10.6%
	Master degree	57	18.4%
	Doctor of Philosophy (Ph.D.)	5	1.6%
8. Current position	Senior Executive	44	14.2%
	Executive Level	78	25.2%
	Officer Level	166	53.5%
	Clerical Level	22	7.1%
9. Frequent cyberattacks encountered in your work	Malware	79	25.5%
	Viruses	120	38.7%
	DoS Attacks	33	10.6%
	Phishing emails	33	10.6%
	Identity theft	22	7.1%
	Cyberstalking	23	7.4%
10. Rating the level of [cybersecurity leadership practice] used in your work	Level 1: Less than 20%	55	17.7%
	Level 2: 20–40%	45	14.5%
	Level 3: 41–60%	75	24.2%
	Level4: 60–80%	82	26.5%
	Level 5: More than 80%	82	26.5%
11. Success rate of cyberattack prevention in your work	Less than 20%	50	16.1%
	Between 20–40%	40	12.9%
	Between 41–60%	75	24.2%
	Between 61–80%	92	29.7%
	Between 81–100%	53	17.1%

As shown in Table 6, the total number of male respondents was 263 (85%), and the number of females was 47 (15%). Most of the respondents belonged to the age group between 35–44 years old with a frequency of 128 (41.3%), while 120 respondents (38.7%) were 25–34 years old, 45 respondents were 45–54 years old (14.5%), 13 respondents were 18–24 years old (4.2%) and the remaining 4 respondents were 55–64 years old (1.3%). The majority of the respondents, 223, were reported to have working experience between 5–10 years (72%). Most of the respondents were non-UAE citizens with a frequency of

265 (85.5%) who work in the banking sector, while only 45 respondents (14.5%) were UAE citizens. The number of workers in Islamic banks were the most dominant number of respondents with a frequency of 160 (51.6%), followed by commercial banks, 75 (24.2%), industrial banks, 45 (14.56%), and merchants banks, 30 (9.7%). The results revealed that the investigated financial organizations suffer high rate of several cyberattacks. Viruses and malware attacks represented the most common cyberattacks with a rate of (38.7%) and (25.5%), respectively, followed by DoS and phishing emails attacks each with similar rate of (10.6%), then lastly identity theft and cyberstalk attacks with rate of (7.1%) and (7.4%), respectively. Respondents declared a variety of responses about assessing the rate of applying cybersecurity leadership practices in their financial organizations. However, almost one third of the respondents, nearly (35%) in total, stated that the rate of practicing cybersecurity leadership concept is approximately less than 50%. As a result, such a low rate of practicing the cybersecurity leadership concept was reflected in the responses to the next question, which showed no high rate of cyberattack prevention among individuals in financial organizations.

5.2. Path Model Assessment

In this research work, structural equations were modelled on a variance basis using Smart PLS 3.0. The moderately complex model that was utilized in this investigation consists of seven independent variables, one mediation variable, and one dependent variable. In order to analyze the measurement and structural model, this work employed Partial Least Square-Structural Equation Modelling (PLS-SEM) with SmartPLS v. 3 [105] as a statistical tool. As survey research is not normally distributed, this approach is especially well-suited for this paper because it allows for smaller sample sizes without making normality assumptions [106]. Therefore, it is necessary to evaluate both the measurement model and the structural model. While the structural model addresses the presumption that the hypotheses are accepted or rejected, the measurement model uses the PLS Algorithm to assess the consistency, convergence, and discriminating validity of the model.

5.2.1. Assessment of Measurement Model

Measurement model assessment includes measuring the internal consistency reliability, convergent validity and discriminatory validity. According to Hair Jr and Sarstedt [107], the measurement model stipulates evaluating the reliability (internal consistency reliability) and validity (convergent and discriminatory validity) of each construct in the model. Measurements of internal consistency, reliability, convergent validity, and discriminatory validity are part of the assessment of measurement models.

- Construct Reliability

The measurement scales for internal correlation among items for the specified latent construct is referred to as reliability [107]. A contract's reliability is determined by assessing the scale measurement's consistency and reliability. Cronbach's alpha and composite reliability are two measures that can be used to assess construct reliability. The Cronbach's alpha coefficient measures how effectively a scale's items are positively correlated with one another. It is calculated as the mean of the correlations between the items used to measure the concept [108]. A Cronbach's Alpha value of 0.7 or higher indicates construct reliability [109]. An alternative internal consistency reliability measure, called composite reliability (CR), can be used more effectively because Cronbach alpha has limitations in the population [110]. It is acceptable to have a construct reliability value of 0.70 or greater [111]. The construct reliability values for each construct are displayed in Table 7. With composite reliability ratings ranging from 0.835 to 0.929 and Cronbach's Alpha values ranging from 0.753 to 0.908, the reliability of all constructs is acceptable.

Table 7. Construct reliability and internal consistency measures.

Construct		Cronbach's Alpha	Composite Reliability
Cybersecurity Prevention	(CP)	0.887	0.917
Government Frequent Alerting	(GF)	0.824	0.873
Organization Training	(OFT)	0.845	0.906
Perceived Severity	(PS)	0.753	0.835
Perceived Vulnerability	(PV)	0.864	0.900
Response Cost	(RC)	0.895	0.922
Response Efficacy	(RE)	0.757	0.838
Cybersecurity Leadership	(CL)	0.908	0.929
Self-Efficacy	(SE)	0.875	0.911

- Construct Validity

The degree to which a construct captures the intended or desired effect is known as its construct validity [112]. The convergent validity and discriminant validity components of construct validity are assessed [111,113]. According to Hair Sarstedt, Jr. [113], convergent validity refers to the degree of strong correlation between measures of the same constructs, whereas discriminant validity refers to how dissimilar one construct is from another.

Convergent validity addresses loading and average variance extracted (AVE) of construction and assesses the degree of correlation of same-definition measurements [113]. The larger outer loading of the indicator indicates that there is a high degree of agreement between the connected measurements or that items used to test the same definition are coherent with the construct [113]. Factor loadings above 0.7 are thought to be extremely important [63]. According to Table 8, all of the loadings were higher than the suggested threshold of 0.7. However, there were a few items eliminated because of low outer loadings (between 0.50 and 0.60) as shown in Table 9. Additionally, the average variance extracted (AVE) value should be 0.5 or greater, indicating that constructs often account for more than half of the variance in their indicator. On average, there are more errors in measurement items with AVE below 0.5. Table 4 displays the AVE results as well as the initial outer loadings of the measurements.

Table 8. Convergent validity measurement results.

Construct	Items	Loadings	Average Variance Extracted (AVE)
Cybersecurity Prevention	CP1	0.809	0.688
	CP2	0.837	
	CP3	0.850	
	CP5	0.818	
	CP6	0.834	
Government Frequent Alert	GF1	0.751	0.535
	GF2	0.768	
	GF3	0.785	
	GF4	0.783	
	GF5	0.666	
	GF6	0.621	
Organization Training	OFT1	0.849	0.762
	OFT3	0.906	
	OFT4	0.864	

Table 8. *Cont.*

Construct	Items	Loadings	Average Variance Extracted (AVE)
Perceived Severity	PS2	0.691	0.504
	PS3	0.757	
	PS4	0.767	
	PS5	0.734	
	PS6	0.587	
Perceived Vulnerability	PV1	0.818	0.606
	PV2	0.832	
	PV3	0.824	
	PV4	0.808	
	PV5	0.501	
	PV6	0.832	
Response Cost	RC1	0.856	0.704
	RC2	0.840	
	RC3	0.821	
	RC4	0.853	
	RC5	0.825	
Response Efficacy	RE1	0.745	0.514
	RE2	0.733	
	RE4	0.822	
	RE5	0.718	
	RE6	0.533	
Cybersecurity Leadership	CL1	0.830	0.686
	CL2	0.872	
	CL3	0.837	
	CL4	0.812	
	CL5	0.813	
	CL6	0.804	
Self-Efficacy	SE1	0.818	0.672
	SE2	0.843	
	SE4	0.861	
	SE5	0.885	
	SE6	0.676	

Table 9. List of eliminated items.

Items	Indicator Loading	Items	Indicator Loading
CP4	0.436	PS1	0.435
OFT2	0.462	RC6	0.352
OFT5	0.429	SE3	0.343
OFT6	0.495	CE3	0.349

Table 9 lists the items with low outer loadings (between 0.50 and 0.60), which were eliminated due to low values. These items are CP4, OFT2, OFT5 and OFT5, RC6, PS1, SE3 and CE3. The researcher eliminated these items one by one to examine how their elimination affects the AVE. Eliminating items with the lowest indicator values had increased the AVE to exceed the threshold value (0.50).

In contrast, discriminant validity implies that measurements of constructs that, according to theory, should not be associated are not shown to have a strong correlation with one another [113]. According to [107], the Fornell–Larcker criterion can be used to test discriminant validity. The square root of AVE values is supposed to be bigger than the value of correlations with other constructs, according to the Fornell–Larcker criterion [113,114]. Each latent construct's square root of the AVE is greater than its connection with the other constructs (see Table 10).

Table 10. Fornell–Larcker criterion.

	(CP)	**(GF)**	**(OFT)**	**(PS)**	**(PV)**	**(RC)**	**(RE)**	**(CL)**	**(SE)**
(CP)	0.830								
(GF)	0.522	0.732							
(OFT)	0.483	0.482	0.873						
(PS)	0.372	0.423	0.340	0.710					
(PV)	0.301	0.315	0.466	0.228	0.779				
(RC)	0.488	0.485	0.712	0.256	0.437	0.839			
(RE)	0.554	0.505	0.451	0.598	0.337	0.432	0.717		
(CL)	0.710	0.601	0.636	0.443	0.481	0.622	0.624	0.828	
(SE)	0.448	0.408	0.531	0.427	0.522	0.488	0.523	0.616	0.820

Cybersecurity Prevention (CP), Government Frequent Alerting (GF), Organization Training (OFT), Perceived Severity (PS), Perceived Vulnerability (PV), Response Cost (RC), Response Efficacy (RE), Cybersecurity Leadership (CL), Self-Efficacy (SE).

5.2.2. Assessment of Structural Model

The structural model is evaluated following the validation of the measurement model or outer model as a valid and reliable model. The method would include assessing the model's likelihood for prediction as well as the correlations between the variables [113]. To examine the model's hypothesized relationships, the structural model is essentially assessed. The coefficient of determination (R^2) of endogenous constructs, effect size (f^2), and path coefficients are the three parameters that determine how well the model can predict the future. The R2 score shows how much variance in dependent variables the related model can explain. The R^2 ranges from 0 to 1, with values of 0.75, 0.50, and 0.25 denoting considerable, moderate, and weak predictive accuracy, respectively, in accordance with Hair Jr., Sarstedt [113]. Table 11 presents the results of the PLS algorithm analysis. It could be observed that 64.7% of the variance in Cybersecurity Leadership is explained by SE, GF, OFT, CR, PV, SR, and RE. Moreover, 53.9% of the variance in cyberattack prevention is explained by CL, SE, GF, OFT, CR, PV, SR, and RE. In addition to determining the endogenous construct's R^2 values, the latent predictor construct's effect size was calculated. Table 11 below presents the R^2 value for each endogenous construct.

Table 11. Result of coefficient of determination (R^2).

Variable	**R^2**	**Result**
Cyberattack Prevention	0.539	Substantial
Cybersecurity Leadership	0.647	Substantial

To evaluate whether the omitted construct significantly affects the endogenous constructions, the effect size (2) is used. Cohen [65,115] stated that values of 0.02–0.14, 0.15–0.34, and larger than 0.35, respectively, imply modest, moderate, and substantial impacts. The f^2 value for each path is displayed in Table 12 below. The effect size varies from a low of 0.005 (Perceived seventy → Cybersecurity prevention) to a maximum value of 0.089 (Self-Efficacy → Cybersecurity prevention).

Table 12. Result for effect size (f^2).

Path	Cyber Security Prevention	Cyber Security Leadership	Effect Size
Government Frequent	0.052	0.073	low
Organizational Training	0.087	0.030	low
Perceived seventy	0.005	0.040	low
Perceived Vulnerability	0.068	0.054	low
Response Cost	0.079	0.035	low
Response Efficacy	0.077	0.082	low
Self-Efficacy	0.089	0.055	low

The path coefficient is also used to assess the strength and significance of the proposed relationships among latent constructs. Estimates are obtained for relationships between structural models with standardized values between 1 and +1, with coefficients closer to +1 denoting a strong positive link and coefficients closer to −1 indicating a strong negative association. Figure 3 displays the path coefficients of the model. The bootstrapping approach is employed to examine the relevance of correlations. The t-value path coefficients for each relationship are reported in the output. The findings of the hypothesis testing are summarized in Table 13.

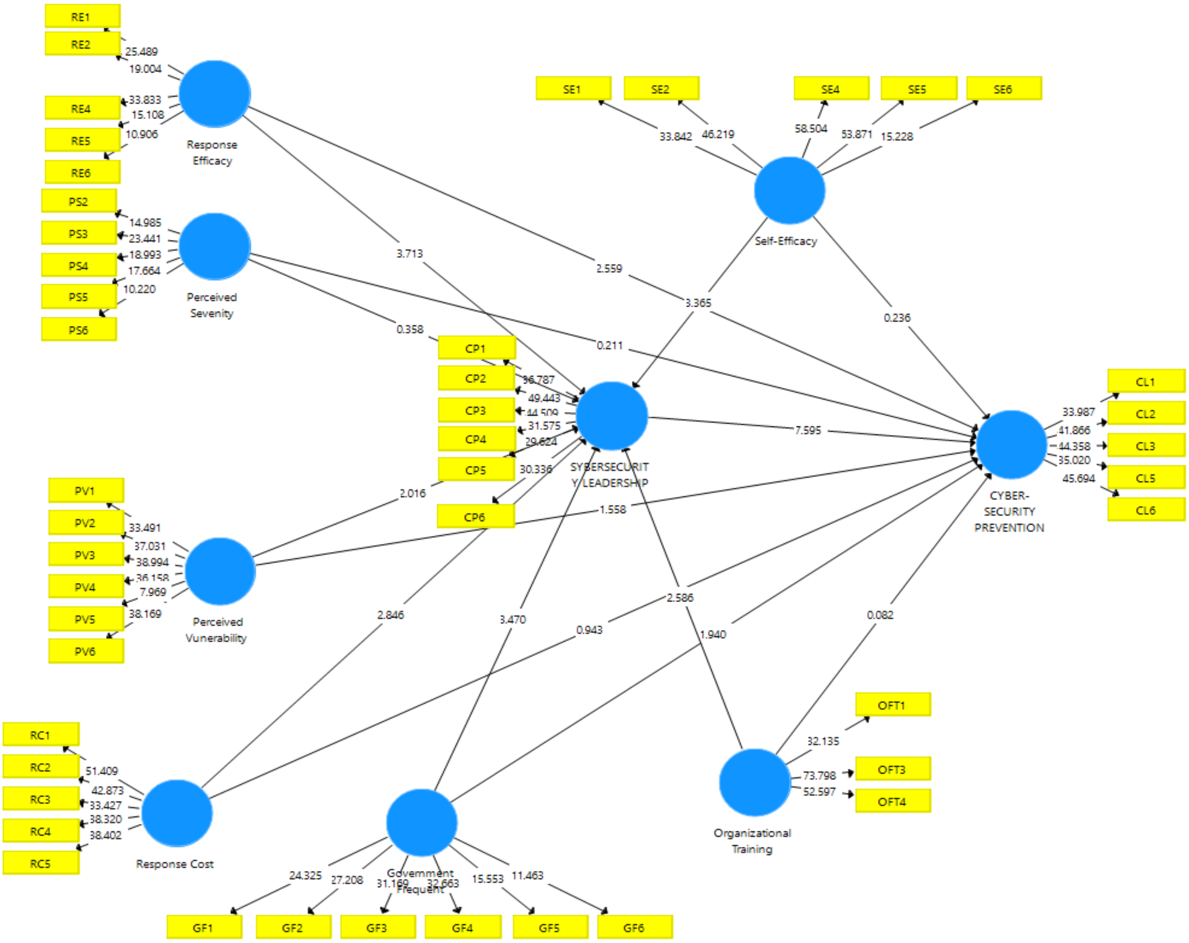

Figure 3. Structural model for path coefficients and *p*-value.

Table 13. Table of hypothesis testing (direct effect).

Hypothesis	Path	Original Sample (O)	Standard Deviation (STDEV)	T Statistics (∣O/STDEV∣)	*p* Values	Results
H1	PS → CP	−0.007	0.045	0.211	0.833	Rejected
H2	PV → CP	−0.069	0.046	1.558	0.120	Rejected
H3	SE → CP	−0.013	0.048	0.236	0.813	Rejected
H4	RE → CP	0.161	0.063	2.559	0.011	Accepted
H5	RC → CP	0.055	0.057	0.943	0.346	Rejected
H6	GF → CP	0.105	0.056	1.940 *	0.053	Accepted
H7	OFT → CP	0.003	0.062	0.082	0.935	Rejected
H8	PS → CL	0.019	0.047	0.358	0.721	Rejected
H9	PV → CL	0.09	0.043	2.016	0.044	Accepted
H10	SE→ CL	0.178	0.057	3.365	0.001	Accepted
H11	RE → CL	0.241	0.065	3.713	0.000	Accepted
H12	RC → CL	0.170	0.059	2.846	0.005	Accepted
H13	OFT → CL	0.156	0.061	2.586	0.010	Accepted
H14	GF → CL	0.202	0.059	3.470	0.001	Accepted
H15	CL→ CP	0.554	0.073	7.595	0.000	Accepted

* Significant at level 0.01. Cyberattack Prevention (CP), Cybersecurity, Leadership (CL), Self-Efficacy (SE) Government Frequent Alerting (GF), Organization Training (OFT), Perceived Severity (PS), Perceived Vulnerability (PV), Response Cost (RC), Response Efficacy (RE).

6. Mediating Variable Analysis

Hypotheses 16–22 state that CL mediates the relationship between H16: PS → CL → CP, H17: PV → CL → CP, H18: SE → CL → CP, H19: RE → CL → CP, H20: RC → CL → CP, H21: OFT → CL → CP, and H22: GF → CL → CP. In this regard, the two-step empirical investigations were conducted in PLS to examine the mediating effect based on the indirect effect between independent and dependent variables via a mediating variable. The first step involves applying path coefficients, t-statistics, and *p*-value to verify the significance of direct and indirect effects. According to [116], full mediation occurs when the mediated effect is significant, but not the direct effect, while partial mediation occurs when a mediator variable partially explains the relationship between an exogenous and an endogenous construct in the presence of a significant direct effect. Therefore, and as shown in Table 14, Cybersecurity Leadership (CL) has a full indirect mediating effect between the dependent variable Cyberattack Prevention (CP) and the five independent variables Self-Efficacy (SE), Perceived Severity (PS), Perceived Vulnerability (PV), Response Cost (RC) and Organization Training (OFT). Further, Cybersecurity Leadership (CL) has a partial mediation effect between Cyberattack Prevention (CP) and only two independent variables, Response Efficacy (RE) and Government Frequent Alerting (GF).

Table 14. Table of mediating hypothesis testing (indirect effect).

	Path	T Values	*p* Values	Results	Type of Mediation
H16	PS → CL → CP	6.366	0.000	Accepted	Full
H17	PV → CL → CP	4.571	0.000	Accepted	Full
H18	SE → CL → CP	2.115	0.035	Accepted	Full
H19	RE → CL →CP	6.458	0.000	Accepted	Partial
H20	RC → CL →CP	2.31	0.037	Accepted	Full
H21	OFT → CL →CP	3.25	0.029	Accepted	Full
H22	GF → CL →CP	2.020	0.044	Accepted	Partial

Cyberattack Prevention (CP), Cybersecurity, Leadership (CL), Self-Efficacy (SE), Government Frequent Alerting (GF), Organization Training (OFT), Perceived Severity (PS), Perceived Vulnerability (PV), Response Cost (RC), Response Efficacy (RE).

7. Discussion

Based on Figure 2 and theoretical foundation explained in Section 3, this study model was developed via proposing seven independent variables and one mediation variable named as cybersecurity leadership and coded as (CL) and one dependent variable named as cyberattack prevention and coded as (CP). In accordance, the researchers of this study proposed twenty-two hypotheses to be examined.

Regarding the first seven direct hypotheses (H1–H7), the empirical findings in this study indicated that there is no significant direct relationship between the seven proposed hypotheses except two hypotheses (H4 and H7). Therefore, the results for testing threat appraisal revealed that perceived severity (PS) and perceived vulnerability (PV) have no significant relation with cyberattack prevention in hypothesis H1 (PS → CP) and H2 (PV → CP) of the structural model and were thus rejected. The results in (Table 13) for perceived severity (PS) and perceived vulnerability (PV) indicate that the related p-value for (PS) was 0.833, which was more than the threshold value of $p > 0.05$, and the related p-value for (PV) was 0.120, which was more than the threshold value of $p > 0.05$. These results provide sufficient empirical evidence to reject hypothesis H1 and H2. Although the result appears to be at odds with both theoretical predictions and the results of several other investigations [61,64,65] from various contexts, it is in line with findings from earlier research that has shown similar findings, where the perceived severity (PS) and perceived vulnerability (PV) did not predict secure behavior [65,117]. As repeatedly reported by previous PMT research [118–120], threat appraisal is a poor predictor of both security behavioral intentions and safety behaviors. This may be interpreted by considering the mediating effect that is already proved to be existed or the users feel that sufficient technical preventive measures have already been undertaken regarding perceived vulnerability.

In addition, for coping appraisal direct hypotheses (H3, H4 and H5) the results show that H3 (SE → CP) and H5 (CR → CP) were rejected, while only H4 (RE → CP) was accepted with a low significance level where bootstrap was based on two tailed critical value test commonly used, which consider t-value 1.65 significance level at (10%), 1.96 significance level (5%), and 2.65 significance level (1%) [121].

The p-value associated with hypothesis H3 (SE → CP), which determines the relationship between self-efficacy and cyberattack prevention, was 0.813, indicating that self-efficacy (SE) is not a significant predictor for cyberattack prevention (CP). This was in line with some previous studies [67,122] that reported self-efficacy to be an insignificant predictor for protective motivation behavior, especially in association with the effect intervention of other variables.

Furthermore, the results indicated that the relationship between response efficacy and cyberattack prevention (RE → CP), as in hypothesis (H4) in the structural model, was significant. The path coefficient for H4 was reported as p-value 0.011, with a t value of 2.559, which was more than the threshold point of $t > 1.96$. This is consistent with the results of [117,123], which confirmed the positive correlation between response efficacy and cyberattack prevention among the total sample of users. For the last hypothesis in coping appraisal, the results indicated that the relationship between response cost and cyberattack prevention (RC → CP), as in hypothesis (H5) in the structural model, was not significant. The path coefficient for H5 was reported as p-value 0.346, with a t-value of 0.943, which was less than the threshold point of $t > 1.96$. This result is in line with the results of [123,124], which confirmed the response cost was not a significant predictor of protection motivation among the total sample of users. Furthermore, the result for the newly emerged H6 and H7 indicated the acceptance of H6 as the government frequent alerting has a significant positive relationship on cyberattack prevention (GF → CP) with t-value 1.94 significance level at (10%). Based on our research, we could not find an empirical and quantitative study that confirms similar results of H6. However, many other non-empirical studies confirm the necessity of government support to enact regulations and frequent alerts to protect their citizens and organizations from cyberattacks [125–127]. Governments should therefore take a lead in employing cybersecurity concepts by encouraging standard-setting and certification, raising knowledge and awareness at all levels of organizations, including top management, and conducting cybersecurity events. On the other hand, the results for H7 indicated that the path coefficient for H7 was reported as a p-value of 0.935, with a t value of

0.082, which was less than the threshold point of $t > 1.96$. Therefore, organization frequent training has no direct significant effect on cyberattack prevention (OFT → CP). This result contradicted the previous research results [128–131], which confirmed the existence of a relationship between cybersecurity organization training and individuals' cybersecurity protective behavior. A possible explanation for this result is that the participants may not be fully aware of the available cybersecurity training and those who are aware might not be fully satisfied with the current level of cybersecurity training. Therefore, financial and other business organizations need to improve current training programs and design effective interventions to increase information security awareness and compliance.

Regarding the hypotheses (H8–H14) that were proposed to test the relationship between all seven independent variables (IVs) and cybersecurity leadership (CL) as the mediation variable, the empirical findings in this study indicated that significant relationships exist between all the proposed hypotheses and cybersecurity leadership (CL), except H8 (PS → CL). This is because the result for testing perceived severity (PS) in relation with cybersecurity leadership (CL) indicated that the related p-value for (PS → CP) was 0.721, which was more than the threshold value of $p > 0.05$. This result provides sufficient empirical evidence to reject hypothesis H8.

H9: Perceived vulnerability (PV) has a positive, significant relationship with cybersecurity leadership (CL). The result shows that the path coefficient value between PV → CL is 0.090. As the t-value is 2.016, higher than the critical value of 1.96 as well as the p-value of 0.044, which is smaller than the threshold of 0.05, the results show that the path coefficient is significant. Hence, there is a significant positive relationship between PV and CL. This result provides sufficient empirical evidence to accept hypothesis H9. Although the result appears to be consistent with both theoretical predictions and the results of several other investigations [61,66,67] from various contexts, it is in line with findings from earlier research that has shown similar findings [67], where the use of technology and the internet for daily tasks has risen, making people and businesses more vulnerable to cybercrime.

H10: Self-efficacy (SE) has a positive, significant relationship with cybersecurity leadership (CL). The result shows that the path coefficient value between SE and CP is 0.187. As the t-value is 3.365, higher than the critical value of 1.96, as well as the p-value of 0.001, which is smaller than the threshold of 0.05, the results show that the path coefficient is significant. Hence, there is a significant positive relationship between SE and CL. This result provides sufficient empirical evidence to accept hypothesis H10. Although the result appears to be consistent with both theoretical predictions and the results of several other investigations [61,68,69] from various contexts, it is in line with findings from earlier research that has shown similar findings [69], where the organizations must increase their self-efficacy in online security behaviors to develop training and policy materials that work.

H11: Response efficacy (RE) has a positive, significant relationship with cybersecurity leadership (CL). The result shows that the path coefficient value between RE and CL is 0.241. As the t-value is 3.713, higher than the critical value of 1.96, as well as the p-value of 0.000, which is smaller than the threshold of 0.05, the results show that the path coefficient is significant. Hence, there is a significant positive relationship between RE and CP. This result provides sufficient empirical evidence to accept hypothesis H11. Although the result appears to be consistent with both theoretical predictions and the results of several other investigations [61,70,71] from various contexts, it is in line with findings from earlier research that has shown similar findings [71], where the response efficacy looks into how user behavior affects their perception of risk when it comes to online security.

H12: Response costs (RC) have a positive, significant relationship with cybersecurity leadership (CL). The result shows that the path coefficient value between RC and CP is 0.170. As the t-value is 2.846, higher than the critical value of 1.96, as well as the p-value of 0.005, which is smaller than the threshold of 0.05, the results show that the path coefficient is significant. Hence, there is a significant positive relationship between RC and CP. This result provides sufficient empirical evidence to accept hypothesis H12. Although the result appears to be consistent with both theoretical predictions and the results of several other investigations [61,64,72] from various contexts, it is in line with findings from earlier research that has shown similar findings [72], where the response cost represents an important element to promote secure transactions and organization safe performance in the presence of an effective cybersecurity leadership.

H13: Organization frequent training (OFT) has a positive, significant relationship with cybersecurity leadership (CL). The result shows that the value of the path coefficient between OFT and CP is 0.156. As the t-value is 2.586, higher than the critical value of 1.96 as well as the *p*-value of 0.001, which is smaller than the threshold of 0.05, the results show that the path coefficient is significant. Hence, there is a significant positive relationship between OFT and CP. This result provides sufficient empirical evidence to accept hypothesis H13. The result appears to be consistent with both theoretical predictions and the results of several other investigations [73–75] from various contexts, and is in line with findings from earlier research that has shown similar findings, where the organization frequently trains staff to secure digital assets because cybercriminals continue to prosper in their operations, and now target both business and organizations as well as individual computer users [75].

H14: Government frequent alerting (GF) has a positive, significant relationship with cybersecurity leadership (CL). This study found that the path coefficient between GF and CP is 0.202, with a t-value of 3.470 and a *p*-value of 0.001. As the t-value is higher than the critical value (1.96) and at the significance value lower than the threshold of 0.05, the path coefficient is significant. Thus, there is a significant positive relationship between GF and CP. This provides substantial empirical evidence to accept hypothesis H14. The result appears to be consistent with both theoretical predictions and the results of several other investigations [76–78] from various contexts, and it is in line with findings from earlier research that has shown a similar finding [77], where the government issues periodic warnings regarding internet security as a result of the growth in data breaches brought on by hacking incidents.

H15: Cybersecurity leadership (CL) has a positive, significant relationship with cyberattack prevention (CP). The result shows that the path coefficient value between CP and CL is 0.554. As the t-value is 7.595, higher than the critical value of 1.96, as well as the *p*-value of 0.000, which is smaller than the threshold of 0.05, the results show that the path coefficient is significant. Hence, there is a significant positive relationship between CP and CL. This result provides sufficient empirical evidence to accept hypothesis H15. The result appears to be consistent with both theoretical predictions and the results of several other investigations [84,86,87] from various contexts, and it is in line with findings from earlier research that has shown similar findings [89], where putting cybersecurity functions in the right positions will be essential for maintaining business operations, and cybersecurity leadership on new practices will lead to successful prevention measures.

Hypotheses 16–22 show the results of indirect mediation effect between all seven proposed independent variables (IVs) and dependent variables (DV) through cybersecurity leadership (CL) as the mediating variable. According to [116], full mediation occurs when the mediated effect is significant but not the direct effect, while partial mediation occurs when a mediator variable partially explains the relationship between an exogenous and an endogenous construct in the presence of a significant direct effect. Therefore, and as shown in Table 14, Cybersecurity Leadership (CL) has a full indirect mediating effect between the dependent variable Cyberattack Prevention (CP) and the five independent variables Self-Efficacy (SE), Perceived Severity (PS), Perceived Vulnerability (PV), Response Cost (RC) and Organization Training (OFT) because none of these five constructs have a direct significant effect on cyberattack prevention as a DV, but there was significant direct effect through cybersecurity leadership as a mediating variable. Meanwhile, Cybersecurity Leadership (CL) has a partial mediation effect between Cyberattack Prevention (CP) and only two independent variables, Response Efficacy (RE), and Government Frequent Alerting (GF). This is because these two constructs have a significant direct effect on cyberattack prevention as a DV, and significant direct effect through cybersecurity leadership as a mediating variable at the same time. These findings confirmed the importance of cybersecurity leadership (CL) as a mediator that leverages and boosts cyberattack preventive behavior among individuals in financial and business organizations. Many recent studies in the cybersecurity field have emphasized the importance of cybersecurity leadership [19,83,132,133]. Despite the significance of leaders in encouraging cybersecurity practices, there is a lack of empirical research on the role of these leaders as a human factor that fosters organizational cyberattack prevention among individuals. Thus, the findings of the testing hypotheses (H16–H22) filled this gap by revealing an empirical result on the importance of cybersecurity leadership as a mediating variable that facilitates higher cyberattack prevention among individuals in the organization.

8. Research Conclusions

This study investigated the factors that contribute to cyberattack prevention in financial organizations in UAE. A general perception of this study was to propose a research framework for cyberattack prevention in the UAE by employing the Protection Motivation Theory and adding new variables focusing on the mediation role of an organization's cybersecurity leadership, and the role of both organization frequent training, and government frequent cybersecurity alerting. A proposed theoretical framework and 22 hypotheses were constructed to guide this study. This research employed a quantitative research method. The data were collected from 310 different financial organization in the UAE that use digital technology to enhance their daily banking operation through survey questionnaires. Subsequently, the data were analyzed using Structural Equation Modelling (SEM) as a statistical methods and techniques approach. The results indicated a significant association between all investigated independent variables and cybersecurity leadership (H8–H14), and cybersecurity leadership mediates the relationship between the investigated independent variables and cyberattack prevention (H15–H22). Meanwhile, no significant association was found between investigated independent variables and cyberattack prevention (H1–H6), except (H4 and H7), which show a significant association.

According to the research finding of this study, cybersecurity leadership is viewed as an important prevention element against cyberattack attempts. With greater cybersecurity leadership success, the implementation of cyberattack prevention increases. This study emphasizes the importance of cybersecurity leadership in a cyberspace environment that protects against cyberattacks and promotes cybersecurity awareness within financial organizations and society in UAE.

9. Implications and Suggestion for Future Research

First, in terms of managerial implications, this study identified a few essential managerial implications that could be practiced by leaders in the managerial levels of financial and business organizations and serve as guidelines for managers and decision-makers to enhance cybersecurity awareness among individuals in the financial organization and reduce or eliminate the expected future risk of cyberattacks. Reaffirming the role played by successful cybersecurity leadership, the role of leaders in the financial organizations lies in several important tasks, including: (a) strategic planning that ensures the protection of the organization and its personnel from cyberattacks, (b) continuous evaluation and monitoring of expected security gaps within financial organization or among individuals of the organization, (c) enculturation of cybersecurity awareness, technical skills and cybersecurity practical knowledge in the employees' mindset through setting, monitoring and evaluating some cybersecurity indicators and components, (d) the effective contribution of leaders and decision-makers in the financial organization in the development of financial organization cybersecurity policy and regulation, which are directly concerned with promoting awareness of cybersecurity among individuals within the financial organization and, and (f) frequent support for cybersecurity training programs and supervising the implementation of training programs among members of the financial organization. Second, regarding theoretical implications, in addition to employing and examining protection motivation theory-based cyberattack preventive measures, this research also introduces and examines newly emerging cyberattack preventive measures that are highly relevant to the banking industry and that can be applied to other financial institutions and large business corporations. The new proposed preventive measures variables, which were derived from related studies presented in three variables, are as follows: two independent variables, (a) frequent organization training, (b) frequent government alerting, and (c) cybersecurity leadership as a mediating variable. Future research could also predict new correlation and interaction among similar factors proposed in this study or suggest some additional relevant factors to be examined in similar context and different research environment.

The third practical contribution, regarding the proposed and validated research framework beside testing and implementing motivation protection theory MPT, highlighted the importance of the three emerged variables named as government frequent alerting, organization cybersecurity frequent training and leadership cybersecurity to be in practice. Therefore, leaders who lead financial or business organizations are encouraged to exercise and learn some cybersecurity basic measures and skills to leverage and foster a more secure environment in their organizations. As an external protection measure, and in addition to their ongoing efforts to establish well-protected and -secured organizations, government should follow up the well-developed and updated policies that ensure all financial organizations and business organizations are practicing safe and secure work operations and transactions. Additionally, as an internal protection measure, leaders who lead financial or business organizations should encourage conducting more up-to-date cybersecurity frequent training among individuals in financial organizations on how to protect personal and related work data from being abused or misused through cyberattack practices.

Although this study addressed a very essential concept about the cyberattack prevention model from an organizational and behavioral perspective, a few limitations might open other directions for more related future research. First, the context and scope of this study was limited to only some selected banks in the UAE with a focus on the role of the cybersecurity leadership role, government and organization frequent alerting and training. Future research might conduct comparative or cross-sectional investigations that include more than one country and focus on other cybersecurity concepts. Second, this study was more focused on organizational and individual behavior toward boosting more cyberattack prevention practices among individuals in UAE financial organizations; other research might address some pure cybersecurity technical issues or other relevant cybersecurity social engendering traps to be rectified. Finally, this study adopted motivation protection theory as the underpinning theory to develop the proposed research framework. In the same context, we encourage researchers to conduct similar research based on cognitive theory, or through using psychological theories, or recent advances in behavioral theories.

Author Contributions: N.H.A.-K., writing—original draft, conceptualization, formal analysis, methodology, project administration, and supervision. S.K.A., resources, validation, writing—review and editing. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Local ethics committees (Universiti Teknikal Malaysia Melaka) ruled that no formal ethics approval was required in this particular case. This study has been performed in accordance with the Declaration of Helsinki.

Informed Consent Statement: Informed consent for participation was obtained from respondents who participated in the survey. The respondents who participated in the survey, were asked to read the ethical statement (There is no compensation for responding nor is there any known risk. To ensure that all information will remain confidential, please do not include your name. Participation is strictly voluntary and you may refuse to participate at any time) and proceed only if they agree. No data was collected from anyone under 16 years old.

Data Availability Statement: Data available on request due to privacy or ethical restrictions.

Acknowledgments: The authors are grateful to the SOLVE research group for guidance, and are thankful to CRIM for the financial support and Universiti Teknikal Malaysia Melaka for providing facilities in this study.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Lemieux, F. Criminal Intelligence. In *Intelligence and State Surveillance in Modern Societies*; Emerald Publishing Limited: Bradford, UK, 2018; pp. 95–119. [CrossRef]
2. Zabyelina, Y. *The Role of Major Intergovernmental Organizations and International Agencies in Combating Transnational Crime*; Cambridge University Press: Cambridge, UK, 2019; pp. 305–310. [CrossRef]
3. Ferguson, R.I.; Renaud, K.; Wilford, S.; Irons, A. PRECEPT: A framework for ethical digital forensics investigations. *J. Intellect. Cap.* 2020; *ahead-of-print*. [CrossRef]
4. Younies, H.; Al-Tawil, T.N. Effect of cybercrime laws on protecting citizens and businesses in the United Arab Emirates (UAE). *J. Financ. Crime* **2020**, *27*, 1089–1105. [CrossRef]
5. Smith, K.T.; Jones, A.; Johnson, L.; Smith, L.M. Examination of cybercrime and its effects on corporate stock value. *J. Inf. Commun. Ethics Soc.* **2019**, *17*, 42–60. [CrossRef]
6. Alwasmi, M. Cybercrime, a global and severe transnational problem in UAE and Globally—A Comparative Study. *Res. Sq.* **2022**, 1–17. [CrossRef]
7. Dempere, J.; Malik, S. Consumer financial fraud in the United Arab Emirates. *J. Financ. Crime* **2021**, *28*, 1193–1209. [CrossRef]
8. Ratten, V. The effect of cybercrime on open innovation policies in technology firms. *Inf. Technol. People* **2019**, *32*, 1301–1317. [CrossRef]
9. Adu, K.K.; Adjei, E. The phenomenon of data loss and cyber security issues in Ghana. *Foresight* **2018**, *20*, 150–161. [CrossRef]
10. Siyam, N.; Hussain, M. Cyber-Safety Policy Elements in the Era of Online Learning: A Content Analysis of Policies in the UAE. *TechTrends* **2021**, *65*, 535–547. [CrossRef]
11. CXODX. Check Point Research: Cyber Attacks Increased by 32% Globally and by 178% in the UAE. 2022. Available online: https://cxodx.com/check-point-research-cyber-attacks-increased-by-32-globally-and-by-178-in-the-uae/ (accessed on 4 February 2023).
12. Cunnington, S. The Underestimated Impact of Enterprise Cyberattacks on Individual Consumers. 2022. Available online: https://gulfbusiness.com/the-underestimated-impact-of-enterprise-cyberattacks-on-individual-consumers/ (accessed on 4 February 2023).
13. ElYacoubi, D. Challenges in customer due diligence for banks in the UAE. *J. Money Laund. Control*, 2020; *ahead-of-print*. [CrossRef]
14. La Torre, M.; Dumay, J.; Rea, M.A. Breaching intellectual capital: Critical reflections on Big Data security. *Meditari Account. Res.* **2018**, *26*, 463–482. [CrossRef]
15. Kumar, S.; Carley, K.M. Approaches to understanding the motivations behind cyber attacks. In Proceedings of the 2016 IEEE Conference on Intelligence and Security Informatics (ISI), Tucson, AZ, USA, 28–30 September 2016; pp. 307–309.
16. Teymourlouei, H. Quick reference: Cyber attacks awareness and prevention method for home users. *Int. J. Comput. Syst. Eng.* **2015**, *9*, 678–684.
17. Bada, M.; Nurse, J.R.C. The social and psychological impact of cyberattacks. In *Emerging Cyber Threats and Cognitive Vulnerabilities*; Academic Press: Cambridge, MA, USA, 2020; pp. 73–92. [CrossRef]
18. Nobles, C. Stress, Burnout, and Security Fatigue in Cybersecurity: A Human Factors Problem. *HOLISTICA–J. Bus. Public Adm.* **2022**, *13*, 49–72. [CrossRef]
19. Triplett, W.J. Addressing Human Factors in Cybersecurity Leadership. *J. Cybersecur. Priv.* **2022**, *2*, 573–586. [CrossRef]
20. Islam, M.S.; Farah, N.; Stafford, T.F. Factors associated with security/cybersecurity audit by internal audit function: An international study. *Manag. Audit. J.* **2018**, *33*, 377–409. [CrossRef]
21. Mahto, R.V.; McDowell, W.C. Entrepreneurial motivation: A non-entrepreneur's journey to become an entrepreneur. *Int. Entrep. Manag. J.* **2018**, *14*, 513–526. [CrossRef]
22. Malik, M.S.; Islam, U. Cybercrime: An emerging threat to the banking sector of Pakistan. *J. Financ. Crime* **2019**, *26*, 50–60. [CrossRef]
23. Teichmann, F.M.; Falker, M.-C. Money laundering through banks in Dubai. *J. Financ. Regul. Compliance*, 2020; *ahead-of-print*. [CrossRef]
24. Yar, M. E-Crime 2.0: The criminological landscape of new social media. *Inf. Commun. Technol. Law* **2012**, *21*, 207–219. [CrossRef]
25. Aggarwal, S.; Duan, Z.; Kermes, L.; de Medeiros, B. E-Crime Investigative Technologies. In Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008), Waikoloa, HI, USA, 7–10 January 2008; p. 486.
26. Meland, P.H.; Sindre, G. Cyber attacks for sale. In Proceedings of the 2019 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 5–7 December 2019; pp. 54–59. [CrossRef]
27. Alzoubi, H.M.; Ghazal, T.M.; Hasan, M.K.; Alketbi, A.; Kamran, R.; Al-Dmour, N.A.; Islam, S. Cyber Security Threats on Digital Banking. In Proceedings of the 2022 1st International Conference on AI in Cybersecurity (ICAIC), Victoria, TX, USA, 24–26 May 2022. [CrossRef]

28. Chandra, G.R.; Sharma, B.K.; Liaqat, I.A. UAE's Strategy Towards Most Cyber Resilient Nation. *Int. J. Innov. Technol. Explor. Eng.* **2019**, *8*, 2803–2809. [CrossRef]
29. Trabelsi, Z.; Barka, E. A Basic Course Model on Information Security for High School IT Curriculum. In Proceedings of the 2019 IEEE Global Engineering Education Conference (EDUCON), Dubai, United Arab Emirates, 8–11 April 2019; pp. 63–70.
30. Maisikeli, S. UAE Cybersecurity Perception and Risk Assessments Compared to Other Developed Nations. In Proceedings of the 2020 3rd International Conference on Information and Computer Technologies (ICICT), San Jose, CA, USA, 9–12 March 2020; pp. 432–439.
31. Trabelsi, Z.; Zeidan, S.; Saleous, H. Teaching Emerging DDoS Attacks on Firewalls: A Case Study of the BlackNurse Attack. In Proceedings of the 2019 IEEE Global Engineering Education Conference (EDUCON), Dubai, United Arab Emirates, 8–11 April 2019; pp. 977–985.
32. Ali, L. Cyber Crimes-A Constant Threat For The Business Sectors And Its Growth (A Study Of The Online Banking Sectors In GCC). *J. Dev. Areas* **2019**, *53*, 267–279. [CrossRef]
33. Paliath, S.; Qbeitah, M.A.; Aldwairi, M. PhishOut: Effective Phishing Detection Using Selected Features. In Proceedings of the 2020 27th International Conference on Telecommunications (ICT), Bali, Indonesia, 5–7 October 2020; pp. 1–5.
34. Qbeitah, M.A.; Aldwairi, M. Dynamic malware analysis of phishing emails. In Proceedings of the 2018 9th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, 3–5 April 2018; pp. 18–24.
35. Bani-Hani, A.; Majdalweieh, M.; AlShamsi, A. Online Authentication Methods Used in Banks and Attacks Against These Methods. *Procedia Comput. Sci.* **2019**, *151*, 1052–1059. [CrossRef]
36. Kaur, P.; Dhir, A.; Tandon, A.; Alzeiby, E.A.; Abohassan, A.A. A systematic literature review on cyberstalking. An analysis of past achievements and future promises. *Technol. Forecast. Soc. Chang.* **2021**, *163*, 120426. [CrossRef]
37. Abaido, G.M. Cyberbullying on social media platforms among university students in the United Arab Emirates. *Int. J. Adolesc. Youth* **2020**, *25*, 407–420. [CrossRef]
38. Al Nafea, R.; Amin Almaiah, M. Cyber Security Threats in Cloud: Literature Review. In Proceedings of the 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021; pp. 779–786. [CrossRef]
39. Ahmad, W.; Rasool, A.; Javed, A.R.; Baker, T.; Jalil, Z. Cyber security in IoT-based cloud computing: A comprehensive survey. *Electronics* **2022**, *11*, 16. [CrossRef]
40. Ghelani, D.; Kian Hua, T.; Kumar, S.; Koduru, R. Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking. *Am. J. Comput. Sci. Technol.* **2022**. [CrossRef]
41. Bubukayr, M.A.S.; Almaiah, M.A. Cybersecurity Concerns in Smart-phones and applications: A survey. In Proceedings of the 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021; pp. 725–731. [CrossRef]
42. Muheidat, F.; Tawalbeh, L. *Artificial Intelligence and Blockchain for Cybersecurity Applications*; Springer International Publishing: Cham, Switzerland, 2021; ISBN 9783030745745.
43. Dawson, J.; Thomson, R. The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *Front. Psychol.* **2018**, *9*, 744. [CrossRef]
44. Randall, R.G.; Allen, S. Cybersecurity professionals information sharing sources and networks in the U.S. electrical power industry. *Int. J. Crit. Infrastruct. Prot.* **2021**, *34*, 100454. [CrossRef]
45. Wong, W.P.; Tan, H.C.; Tan, K.H.; Tseng, M.L. Human factors in information leakage: Mitigation strategies for information sharing integrity. *Ind. Manag. Data Syst.* **2019**, *119*, 1242–1267. [CrossRef]
46. Rahman, T.; Rohan, R.; Pal, D.; Kanthamanon, P. Human Factors in Cybersecurity: A Scoping Review. In *IAIT2021: The 12th International Conference on Advances in Information Technology*; Association for Computing Machinery: New York, NY, USA, 2021. [CrossRef]
47. Georgiadou, A.; Mouzakitis, S.; Askounis, D. Detecting Insider Threat via a Cyber-Security Culture Framework. *J. Comput. Inf. Syst.* **2022**, *62*, 706–716. [CrossRef]
48. Hadlington, L. The "human factor" in cybersecurity: Exploring the accidental insider. In *Psychological and Behavioral Examinations in Cyber Security*; IGI Global: London, UK, 2018; pp. 46–63. [CrossRef]
49. Ramlo, S.; Nicholas, J.B. The human factor: Assessing individuals' perceptions related to cybersecurity. *Inf. Comput. Secur.* **2021**, *29*, 350–364. [CrossRef]
50. Abulencia, J. Insider attacks: Human-factors attacks and mitigation. *Comput. Fraud Secur.* **2021**, *2021*, 14–17. [CrossRef]
51. Aldawood, H.; Skinner, G. Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review. In Proceedings of the 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE), Wollongong, Australia, 4–7 December 2018; pp. 62–68. [CrossRef]
52. Ani, U.D.; He, H.; Tiwari, A. Human factor security: Evaluating the cybersecurity capacity of the industrial workforce. *J. Syst. Inf. Technol.* **2019**, *21*, 2–35. [CrossRef]
53. Nifakos, S.; Chandramouli, K.; Nikolaou, C.K.; Papachristou, P.; Koch, S.; Panaousis, E.; Bonacina, S. Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors* **2021**, *21*, 5119. [CrossRef]
54. Maalem Lahcen, R.A.; Caulkins, B.; Mohapatra, R.; Kumar, M. Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity* **2020**, *3*, 10. [CrossRef]
55. Chandra, A.; Snowe, M.J. A taxonomy of cybercrime: Theory and design. *Int. J. Account. Inf. Syst.* **2020**, *38*, 100467. [CrossRef]

56. Harika, M.; Campbell, E. Ransomware in the UAE: Evolving Threats and Expanding Responses | Middle East Institute. July 2022. Available online: https://www.mei.edu/publications/ransomware-uae-evolving-threats-and-expanding-responses (accessed on 24 February 2023).
57. Aboul-Enein, S. *Cybersecurity Challenges in the Middle East*; GCSP: Geneva, Switzerland, 2017; ISBN 9782889471003.
58. Aloul, F.A. The Need for Effective Information Security Awareness. *J. Adv. Inf. Technol.* **2012**, *3*, 176–183. [CrossRef]
59. Rajan, A.V.; Ravikumar, R.; Shaer, M. Al UAE cybercrime law and cybercrimes—An analysis. In Proceedings of the 2017 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), London, UK, 19–20 June 2017. [CrossRef]
60. Dubai, E. DUBAI CYBER SECURITY STRATEGY Establishing Dubai as a Global Leader in Innovation, Safety and Security. *Dubai.Ae*. 2017. Available online: https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/government-services-and-digital-transformation/dubai-cyber-security-strategy (accessed on 24 February 2023).
61. Rogers, R.W. A Protection Motivation Theory of Fear Appeals and Attitude Change. *J. Psychol.* **1975**, *91*, 93–114. [CrossRef]
62. Rogers, R.W. Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In *Social Psychophysiology: A Sourcebook*; Cacioppo, J.T., Petty, R., Eds.; Guilford: New York, NY, USA, 1983; pp. 153–177.
63. Kothe, E.J.; Ling, M.; North, M.; Klas, A.; Mullan, B.A.; Novoradovskaya, L. Protection motivation theory and pro-environmental behaviour: A systematic mapping review. *Aust. J. Psychol.* **2019**, *71*, 411–432. [CrossRef]
64. Briggs, P.; Jeske, D.; Coventry, L. Behavior Change Interventions for Cybersecurity. In *Behavior Change Research and Theory. Psychological and Technological Perspectives*; Academic Press: Cambridge, MA, USA, 2017; pp. 115–136. [CrossRef]
65. van Bavel, R.; Rodríguez-Priego, N.; Vila, J.; Briggs, P. Using protection motivation theory in the design of nudges to improve online security behavior. *Int. J. Hum. Comput. Stud.* **2019**, *123*, 29–39. [CrossRef]
66. Bada, M.; Sasse, A.M.; Nurse, J.R. Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv* **2019**, arXiv:1901.02672.
67. Vrhovec, S.; Mihelič, A. Redefining threat appraisals of organizational insiders and exploring the moderating role of fear in cyberattack protection motivation. *Comput. Secur.* **2021**, *106*, 102309. [CrossRef]
68. Li, L.; Xu, L.; He, W.; Chen, Y.; Chen, H. Cyber Security Awareness and Its Impact on Employee's Behavior. In *Research and Practical Issues of Enterprise Information Systems*; Springer: Cham, Switzerland, 2016; pp. 103–111.
69. Ophoff, J.; Lakay, M. Mitigating the Ransomware Threat: A Protection Motivation Theory Approach. In Proceedings of the Information Security: 17th International Conference, ISSA 2018, Pretoria, South Africa, 15–16 August 2018; pp. 163–175.
70. White, J.K. Impact of Protection Motivation Theory and General Deterrence Theory on the Behavioral Intention to Implement and Misuse Active Cyber Defense. Ph.D. Thesis, Capella University, Minneapolis, MN, USA, 2017.
71. Choi, H.; Young, K.J. Practical Approach of Security Enhancement Method based on the Protection Motivation Theory. In Proceedings of the 2021 21st ACIS International Winter Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD-Winter), Ho Chi Minh City, Vietnam, 28–30 January 2021; pp. 96–97.
72. Hassandoust, F.; Techatassanasoontorn, A.A. Understanding users' information security awareness and intentions. In *Cyber Influence and Cognitive Threats*; Elsevier: Amsterdam, The Netherlands, 2020; pp. 129–143.
73. McCrohan, K.F.; Engel, K.; Harvey, J.W. Influence of awareness and training on cyber security. *J. Internet Commer.* **2010**, *9*, 23–41. [CrossRef]
74. Hamoud, A.; Aïmeur, E. Handling User-Oriented Cyber-Attacks: STRIM, a User-Based Security Training Model. *Front. Comput. Sci.* **2020**, *2*, 25. [CrossRef]
75. Quader, F.; Janeja, V.P. Insights into Organizational Security Readiness: Lessons Learned from Cyber-Attack Case Studies. *J. Cybersecur. Priv.* **2021**, *1*, 638–659. [CrossRef]
76. Tsagourias, N. Cyber attacks, self-defence and the problem of attribution. *J. Confl. Secur. Law* **2012**, *17*, 229–244. [CrossRef]
77. Eichensehr, K.E. Decentralized Cyberattack Attribution. *AJIL Unbound* **2019**, *113*, 213–217. [CrossRef]
78. Abdalrahman, G.A.; Varol, H. Defending Against Cyber-Attacks on the Internet of Things. In Proceedings of the 2019 7th International Symposium on Digital Forensics and Security (ISDFS), Barcelos, Portugal, 10–12 June 2019; pp. 1–6.
79. Uchendu, B.; Nurse, J.R.C.; Bada, M.; Furnell, S. Developing a cyber security culture: Current practices and future needs. *Comput. Secur.* **2021**, *109*, 102387. [CrossRef]
80. Jeong, J.; Mihelcic, J.; Oliver, G.; Rudolph, C. Towards an improved understanding of human factors in cybersecurity. In Proceedings of the 2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC), Los Angeles, CA, USA, 12–14 December 2019; pp. 338–345. [CrossRef]
81. Rothrock, R.A.; Kaplan, J.; Friso, V.D.O. Boards Role in Managing Cyber Risk. 2018. Available online: https://www.proquest.com/docview/1986317468?pq-origsite=gscholar&fromopenview=true (accessed on 26 February 2023).
82. Klimoski, R. Critical Success Factors for Cybersecurity Leaders. *People Strateg.* **2016**, *39*, 14–18. Available online: http://search.ebscohost.com/login.aspx?direct=true&AuthType=shib&db=buh&AN=112590899&site=ehost-live&custid=s8501869 (accessed on 26 February 2023).
83. Huang, K.; Pearlson, K. For what technology can't fix: Building a model of organizational cybersecurity culture. *Proc. Annu. Hawaii Int. Conf. Syst. Sci.* **2019**, *2019*, 6398–6407. [CrossRef]
84. Hathaway, M.E. Leadership and responsibility for cybersecurity. In *Georgetown Journal of International Affairs*; The Johns Hopkins University Press: Baltimore, MD, USA, 2012; pp. 71–80.

85. Nair, D. UAE Sees More Than 600,000 Phishing Attacks in Q2. *N-Business*. 22 August 2020. Available online: https://www.thenationalnews.com/business/money/uae-sees-more-than-600-000-phishing-attacks-in-q2-1.1065830 (accessed on 23 February 2023).
86. Cleveland, S.; Cleveland, M. Toward cybersecurity leadership framework. In Proceedings of the Thirteenth Midwest Association for Information Systems Conference, St. Louis, MO, USA, 17–18 May 2018.
87. Lehto, M.; Limnéll, J. Strategic leadership in cyber security, case Finland. *Inf. Secur. J. A Glob. Perspect.* **2021**, *30*, 139–148. [CrossRef]
88. Tounsi, W.; Rais, H. A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Comput. Secur.* **2018**, *72*, 212–233. [CrossRef]
89. Culot, G.; Fattori, F.; Podrecca, M.; Sartor, M. Addressing Industry 4.0 Cybersecurity Challenges. *IEEE Eng. Manag. Rev.* **2019**, *47*, 79–86. [CrossRef]
90. Lis, P.; Mendel, J. Cyberattacks on Critical Infrastructure: An Economic Perspective. *Econ. Bus. Rev.* **2019**, *5*, 24–47. [CrossRef]
91. Salehi, S. Analysis of Environmental Behaviors of Rural People by Applying Protection Motivation Theory. *J. Rural Res.* **2021**, *11*, 662–673. [CrossRef]
92. Li, Y.; Shang, H. Service quality, perceived value, and citizens' continuous-use intention regarding e-government: Empirical evidence from China. *Inf. Manag.* **2020**, *57*, 103197. [CrossRef]
93. Alalehto, T. Crime prevention in terms of criminal intent criteria in white-collar crime. *J. Financ. Crime* **2018**, *25*, 838–844. [CrossRef]
94. Xue, B.; Xu, F.; Luo, X.; Warkentin, M. Ethical leadership and employee information security policy (ISP) violation: Exploring dual-mediation paths. *Organ. Cybersecur. J. Pract. Process People* **2021**, *1*, 5–23. [CrossRef]
95. Zegzhda, D.; Lavrova, D.; Pavlenko, E.; Shtyrkina, A. Cyber Attack Prevention Based on Evolutionary Cybernetics Approach. *Symmetry* **2020**, *12*, 1931. [CrossRef]
96. Amer, F.; Abdulrahim, H.; Juma, S.; Rajan, A.V.; Ahamed, J. Shopping online securely in UAE. In Proceedings of the 2013 International Conference on Current Trends in Information Technology (CTIT), Dubai, United Arab Emirates, 11–12 December 2013; pp. 153–160.
97. Porter, J., Sr. Transformational Leadership and Its Approach to Cybersecurity Implementation. Ph.D. Thesis, Capitol Technology University, Laurel, MD, USA, 2019.
98. Philip, J. Viewing Digital Transformation through the Lens of Transformational Leadership. *J. Organ. Comput. Electron. Commer.* **2021**, *31*, 114–129. [CrossRef]
99. Ogbanufe, O.; Kim, D.J.; Jones, M.C. Informing cybersecurity strategic commitment through top management perceptions: The role of institutional pressures. *Inf. Manag.* **2021**, *58*, 103507. [CrossRef]
100. Afifi, M.A. Ethical Responsibilities for Assessment of Techniques and Legal Framework to Minimize IT Crimes in UAE. 2019. Available online: https://www.researchgate.net/publication/339003848_Ethical_Responsibilities_for_Assessment_of_Techniques_and_Legal_Framework_to_Minimize_IT_Crimes_in_UAE (accessed on 26 February 2023).
101. Gandhi, R.; Sharma, A.; Mahoney, W.; Sousan, W.; Zhu, Q.; Laplante, P. Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political. *IEEE Technol. Soc. Mag.* **2011**, *30*, 28–38. [CrossRef]
102. Teichmann, F.M.J.; Falker, M.-C. Money laundering through exchange offices. *J. Money Laund. Control*, 2020; *ahead-of-print*. [CrossRef]
103. Lawshe, C.H. A quantitative approach to content validity. *Pers. Psychol.* **1975**, *28*, 563–575. [CrossRef]
104. Hunt, S.D.; Sparkman, R.D.; Wilcox, J.B. Survey Preliminary Findings Pretest. *J. Mark. Res.* **1982**, *19*, 269–273. [CrossRef]
105. Ringle, C.M.; Sarstedt, M.; Mitchell, R.; Gudergan, S.P. Partial least squares structural equation modeling in HRM research. *Int. J. Hum. Resour. Manag.* **2020**, *31*, 1617–1643. [CrossRef]
106. Chin, W.W.; Marcolin, B.L.; Newsted, P.R. A Partial Least Squares Latent Variable Modeling Approach for Measuring Interaction Effects: Results From a Monte Carlo Simulation Study and Voice Mail Emotion/Adoption Study. *Inf. Syst. Res.* **2003**, *14*, 189–217. Available online: https://apps.dtic.mil/sti/pdfs/ADA441817.pdf (accessed on 26 February 2023). [CrossRef]
107. Hair, J.F., Jr.; Sarstedt, M.; Ringle, C.M.; Gudergan, S.P. *Advanced Issues in Partial Least Squares Structural Equation Modeling*; SAGE Publications: Southend Oaks, CA, USA, 2017.
108. Awang, M.M.; Kutty, F.M.; Ahmad, A.R. Perceived social support and well being: First-year student experience in university. *Int. Educ. Stud.* **2014**, *7*, 261–270. [CrossRef]
109. Sultana, N.; Amin, S.; Islam, A. Influence of perceived environmental knowledge and environmental concern on customers' green hotel visit intention: Mediating role of green trust. *Asia-Pac. J. Bus. Adm.* **2022**, *14*, 223–243. [CrossRef]
110. Kasunic, M. *Designing an Effective Survey*; Software Engineering Institute-Carnegie Mellon University: Pittsburgh, PA, USA, 2005; Available online: https://apps.dtic.mil/sti/citations/ADA441817 (accessed on 26 February 2023).
111. Alzahrani, A.; Stahl, B.; Prior, M. Developing an instrument for e-public services' acceptance using confirmatory factor analysis: Middle east context. *J. Organ. End User Comput.* **2012**, *24*, 18–44. [CrossRef]
112. Brown, R.P. Measuring individual differences in the tendency to forgive: Construct validity and links with depression. *Personal. Soc. Psychol. Bull.* **2003**, *29*, 759–771. [CrossRef] [PubMed]
113. Hair, J.F.; Sarstedt, M.; Hopkins, L.; Kuppelwieser, V.G. Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research. *Eur. Bus. Rev.* **2014**, *26*, 106–121. [CrossRef]

114. Henseler, J.; Ringle, C.M.; Sarstedt, M. Using Partial Least Squares Path Modeling in Advertising Research: Basic Concepts and Recent Issues. In *Handbook of Research on International Advertising*; Edward Elgar Publishing: Cheltenham, UK, 2012. [CrossRef]
115. Cohen, J. *Statistical Power Analysis for the Behavioral Sciences*; Routledge: Abingdon, UK, 2013.
116. Zhao, X.; Lynch, J.G.; Chen, Q. Reconsidering Baron and Kenny: Myths and truths about mediation analysis. *J. Consum. Res.* **2010**, *37*, 197–206. [CrossRef]
117. Sulaiman, N.S.; Fauzi, M.A.; Hussain, S.; Wider, W. Cybersecurity Behavior among Government Employees: The Role of Protection Motivation Theory and Responsibility in Mitigating Cyberattacks. *Information* **2022**, *13*, 413. [CrossRef]
118. Hodgkins, S.; Orbell, S. Can protection motivation theory predict behaviour? A longitudinal test exploring the role of previous behaviour. *Psychol. Health* **1998**, *13*, 237–250. [CrossRef]
119. Maddux, J.E.; Rogers, R.W. Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *J. Exp. Soc. Psychol.* **1983**, *19*, 469–479. [CrossRef]
120. Hanus, B.; Wu, Y. "Andy" Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. *Inf. Syst. Manag.* **2016**, *33*, 2–16. [CrossRef]
121. Hair, J.F.; Hult, G.T.M.; Ringle, C.M.; Sarstedt, M. A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM). *Eur. J. Tour. Res.* **2014**, *6*, 211–213.
122. Martens, M.; De Wolf, R.; De Marez, L. Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. *Comput. Human Behav.* **2019**, *92*, 139–150. [CrossRef]
123. Jansen, J.; van Schaik, P. Persuading end users to act cautiously online: A fear appeals study on phishing. *Inf. Comput. Secur.* **2018**, *26*, 264–276. [CrossRef]
124. Mohamud, A.J. A Framework for Information Security Management Adoption in Higher Education Institutions in Somalia: Perspectives PMT and TOE. no. 5. 2019. Available online: https://mu.edu.so/wp-content/uploads/2022/05/Dr.-Abdulkadir-Jeilani-Mohamud-English-2019.pdf (accessed on 26 February 2023).
125. Hweidi, R.F.A.; Eleyan, D. Social Engineering Attack Concepts, Frameworks, and Awareness: A Systematic Literature Review. *Int. J. Sci. Eng. Invent.* **2022**, *8*, 6–12. [CrossRef]
126. Knake, R.K. *A Cyberattack on the U.S. Power Grid*; Council on Foreign Relations: New York, NY, USA, 2017.
127. Willems, E. *Cyberdanger: Understanding and Guarding against Cybercrime*, 1st ed.; Springer: Cham, Switzerland, 2019; ISBN 3030045315/ 9783030045319.
128. Shillair, R.; Esteve-González, P.; Dutton, W.H.; Creese, S.; Nagyfejeo, E.; von Solms, B. Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. *Comput. Secur.* **2022**, *119*, 102756. [CrossRef]
129. Burns, A.J.; Johnson, M.E.; Caputo, D.D. Spear phishing in a barrel: Insights from a targeted phishing campaign. *J. Organ. Comput. Electron. Commer.* **2019**, *29*, 24–39. [CrossRef]
130. Kam, H.J.; Menard, P.; Ormond, D.; Crossler, R.E. Cultivating cybersecurity learning: An integration of self-determination and flow. *Comput. Secur.* **2020**, *96*, 101875. [CrossRef]
131. Elyas, M.; Maynard, S.B.; Ahmad, A.; Lonie, A. Towards a systemic framework for digital forensic readiness. *J. Comput. Inf. Syst.* **2014**, *54*, 97–105. [CrossRef]
132. Burrell, D.N.; Aridi, A.S.; Nobles, C. The critical need for formal leadership development programs for cybersecurity and information technology professionals. In Proceedings of the 13th International Conference on Cyber Warfare and Security, Washington, DC, USA, 8–9 March 2018; pp. 82–91.
133. Ioannou, M.; Stavrou, E.; Bada, M. Cybersecurity culture in computer security incident response teams: Investigating difficulties in communication and coordination. In Proceedings of the 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Oxford, UK, 3–4 June 2019; pp. 1–4. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.