IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 24 June 2023, accepted 11 July 2023, date of publication 28 July 2023, date of current version 23 August 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3296580

RESEARCH ARTICLE

A Comparative Assessment of Human Factors in Cybersecurity: Implications for Cyber Governance

MUHAMMAD UMAIR SHAH[1], FARKHUND IQBAL[2], (Member, IEEE), UMAIR REHMAN[3], AND PATRICK C. K. HUNG[4], (Member, IEEE)

[1]Department of Management Sciences, Faculty of Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada
[2]College of Technological Innovation, Zayed University, Dubai, United Arab Emirates
[3]Department of Computer Science, University of Western Ontario, London, ON N6A 3K7, Canada
[4]Faculty of Business and Information Technology, Ontario Tech University, Oshawa, ON L1G 0C5, Canada

Corresponding author: Muhammad Umair Shah (mushah@uwaterloo.ca)

This work was supported by Zayed University, United Arab Emirates, under Grant R19044 and Grant R18055.

This work involved human subjects. Approval of all ethical and experimental procedures and protocols was granted by the Research Ethics Committee at Zayed University (under Ethics Application No. ZU20_099_F), and performed in line with the Belmont Report.

ABSTRACT This paper provides an extensive overview of cybersecurity awareness in the young, educated, and technology-savvy population of the United Arab Emirates (UAE), compared to the United States of America (USA) for advancing the scholarship and practice of global cyber governance. We conducted comparative empirical studies to identify differences in specific human factors that affect cybersecurity behaviour in the UAE and the USA. In addition, we employed several control variables to observe reliable results. We used Hofstede's theoretical framework on culture to advance our investigation. The results show that the targeted population in the UAE exhibits contrasting interpretations of cybersecurity awareness of critical human factors as compared to their counterparts from the USA. We identify possible explanations for this relatively different behaviour in the UAE population. Our key contributions are to provide valuable information for cybersecurity policymakers in the UAE and Gulf Cooperation Council (GCC) region to further enhance cyber safety, governance, awareness, and trust among citizens.

INDEX TERMS Human factors in cybersecurity, cyber risk awareness, evidence-based cybersecurity policy, cyber governance, stakeholder engagement.

I. INTRODUCTION

Cybersecurity and cyber vulnerabilities are usually attributed to various physical, humanistic, or social factors. Many global institutional policymakers and governments prefer building more robust physical infrastructures to counter them. This phenomenon is also recognized as the outdated "Castle Model," according to which thick defense boundaries (or walls) are built around the system to protect against security breaches ([1], [2], [3]) The Castle Model helps protect; however, due to cultural diversity, complex socio-technical systems, and cybersecurity awareness levels among global populations, governments to struggle to eradicate these cyber risks. Therefore, an evidence-based investigation of human factors and cyber risk awareness levels is required to build a holistic cybersecurity framework.

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These attacks are usually aimed at accessing, changing, or destroying sensitive information, extorting money from users, or interrupting normal business processes, [4]. Information security awareness plays an essential role in preventing cybercrimes in [6] and [5]. Due to a lack of understanding cybersecurity risks, online user behaviour becomes vulnerable to cybercrimes. According to a general observation, global Internet users possess divergent online habits and behaviors. Given the vast Internet connectivity and diversity worldwide, it is challenging to educate people about the correct behaviours to

The associate editor coordinating the review of this manuscript and approving it for publication was Liang-Bi Chen.

preserve cybersecurity. To support this point, according to the Cybersecurity Exposure Index,[1] the United States of America (USA) has one of the lowest exposure rates of 0.145, while the United Arab Emirates (UAE) has a comparatively higher exposure index of 0.359.

Consequently, the Gulf Cooperation Council (GCC) region seems more exposed to cyberattacks than the United States of America (USA). Recent research suggests a significant lack of security awareness among GCC countries' citizens compared to the USA, [7]. Among European countries, Finland tops the Cybersecurity Exposure Index list with a score of 0.11, whereby Afghanistan ranks the lowest with a 1.0 score. These facts illustrate significant differences in the cybersecurity risk awareness of various countries. We suspect that global cybersecurity exposure scores result from behavioural aspects of human factors that influence cybersecurity awareness. For instance, the diversity between cultures, socioeconomic characteristics, digital divide, education, and beliefs of people living in the GCC countries versus the USA directly influences these rankings.

Furthermore, there is a gap in the literature that examines the linkages between various human factors of Internet users living in different regions or countries. Some users' positive attitudes toward cybersecurity a specific region could pose a striking contrast with the negative or indifferent attitudes in another. Prior literature investigated human-centric factors that interplay with autonomous systems [50] and cybersecurity awareness. However, most of these studies focus on business environments (for instance investigating employees' behaviour and their implications for organizations) or lack empirical evidence, [9], [10], [11].

Recently, two separate cyberattacks in Canada compromised thousands of citizens' identities using the Canada Revenue Agency (CRA) portal, disseminating employment insurance, child care, and other critical social benefits to its citizens [12]. It has further implications, as it occurred during the ever-testing times of the COVID-19 pandemic. As a result, the Canadian government temporarily shut down its CRA portal, which is critical for supporting many citizens to avoid further damage. According to some experts, a major factor contributing to this breach is ''credential stuffing,'' which refers to individuals re-using their username and password on multiple websites and applications. Similarly, in other countries, such as Saudi Arabia and UAE, a well-reputed Information Technology (IT) firm, IBM, recently estimated that there would be a yearly increase of 9.4% in the cost of data breaches in 2020 [13]. Given the alarming rates at which cybercrime has grown globally, it is an urgent issue that researchers must explore further. Previously, it was reported that black-hat hackers have caused a 20% loss in companies' clientele, which translates to a decline in revenues [14]. This makes cybersecurity a topic of deep interest for scholars and practitioners.

Hackers typically exploit Internet users based on their online behaviours and habits. Due to cultural differences between humans, these factors vary globally. Overwhelming evidence demonstrates that cybersecurity awareness among individuals can significantly counter these threats. However, this area lacks proper empirical inquiry [15]. We believe investigating cybercrime awareness among different world regions could significantly contribute to understanding the cybersecurity phenomenon. To fill this gap in the literature, we decided to focus on two culturally different regions, such as the UAE, and compare the outcomes of cybersecurity awareness to a similar population in the USA. In this exploratory study, we addressed these two questions:

1. Which specific human factors affect cybersecurity behaviour in diverse cultures, such as the UAE and USA? Why is it important to draw this comparison?
2. How can these findings benefit governments at a global level to enhance cybersecurity policymaking?

We acknowledge that including other regions will broaden our understanding of global cybersecurity awareness issues. However, to manage this study's scope, we restricted our inquiry to draw a comparison between the UAE and USA populations as a first step. In the future, our goal will be to compare the state of cybersecurity awareness among other regions of the world and provide guidance to policymakers at a global level.

To investigate the first question, we decided to employ an existing cybersecurity awareness survey instrument, called the Human Aspects of Information Security Questionnaire (HAIS-Q), a validated and reliable instrument [16]. However, when we conducted a pre-test of this instrument on our targeted UAE population, we experienced non-responsiveness due to our participants' inability to understand some factors properly. This experience proved to be consistent with the findings of a study conducted by the Pew Research Center[2] on the ineffectiveness of using existing cybersecurity questionnaires on the American population. We attempted to simplify further and adapt these questions. However, that also proved to be futile. We realized that instruments such as HAIS-Q would not capture the correct picture of cybersecurity awareness, especially among our targeted population in the UAE. Therefore, we decided to conduct an exploratory study to enlist factors that define cybersecurity awareness construct more accurately for the UAE population. Following this exploratory study, it involved a systematic literature review and interviews with five global cybersecurity experts from the UAE and North America. A convenience sampling technique was employed to select these experts. Two expert respondents were recruited from the UAE and the interviews were conducted online. Whereby, three experts representing the USA were recruited, and the interviews were conducted in-person. On average, each interview took about fifty minutes

[1]The lower the score, the lower the exposure. The Cybersecurity Exposure Index (CEI) reports the score between 0 and 1. URL: https://passwordmanagers.co/cybersecurity-exposure-index/

[2]This study is conducted by Aaron Smith at Pew Research Center in Washington D.C. (USA). It is a nonpartisan fact tank to inform public about issues, attitudes and trends shaping the world. Retrievable on August 18, 2020 from: https://www.pewresearch.org/internet/2017/03/22/what-the-public-knows-about-cybersecurity/

to complete. We then designed a survey instrument to collect responses from our targeted populations in the UAE and the USA.

In the following sections, we outline the theoretical framework for our research and highlight factors that prior literature and cybersecurity expert panelists recommend contributing to cybercrime incidents globally, especially in the GCC countries. Subsequently, we describe the process of survey instrument development and research method. We then share the study results and offer an extensive discussion on GCC countries' state-of-the-art information security awareness. Our discussion mainly features these six factors contributing to cybercrimes in the GCC region: the growth of the user base, lack of security awareness programs, inadequate laws and regulations, limited education, culture, and the Internet gender gap. We propose various interventions relevant stakeholders, such as governments or other lawmaking authorities, can implement to improve cybersecurity awareness in different regions. Several interventions can be implemented to prevent cybercrimes, such as capacity-building initiatives, security awareness/training programs, and legislation. In particular, prior research has demonstrated that an increased emphasis on security training programs leads to fewer cybersecurity incidents occurrences [17]. Finally, we conclude with a summary to offer practical recommendations for policymakers. We believe that our findings will contribute to a greater theoretical and practical understanding of cybersecurity in different regions and assist multiple stakeholders, such as governments, business communities, and the public, in creating awareness around information security at a global level.

II. THEORETICAL FRAMEWORK

In order to address our above-mentioned research questions, we use Hofstede's theoretical framework on culture. Hofstede's model provides valuable insights into cross-cultural relationships' dynamics, which can be applied directly to our research theme. In his framework, Hofstede discovered that four dimensions characterize differences across various cultures: Power Distance (PD), Individualism-Collectivism (IC), Masculinity Femininity (MF), and Uncertainty Avoidance (UA), [18]. These four dimensions can draw comparisons between factors that impact cybersecurity behavior in the UAE and USA.

Hofstede's cultural dimensions theory provides valuable insights into the impact of cultural differences on cybersecurity strategies in the USA and UAE. In the USA, a culture characterized by low power distance, individualism, and low uncertainty avoidance shapes the approach to cybersecurity [19], [26]. This translates into an emphasis on personal privacy and individual responsibility in protecting online information. The competitive nature of the society fosters a focus on technological dominance and proactive measures to secure cyber assets. Additionally, the culture's low uncertainty avoidance encourages a willingness to adopt new technologies and adapt to emerging threats promptly. Conversely, the UAE's cultural landscape, marked by high power distance, collectivism, and high uncertainty avoidance, has implications for cybersecurity. The emphasis on hierarchical structures and respect for authority promotes a centralized approach to cybersecurity, with a reliance on designated authorities to protect shared resources. Furthermore, the high uncertainty avoidance drives a conservative approach, favoring established security practices and validated technologies over unproven solutions.

To start with, power distance is a relevant dimension that affects cybersecurity behavior in the UAE culture. Power Distance (PD) refers to the extent to which unequal distributions of power and wealth are tolerated within certain countries [20]. Individuals who uphold hierarchy positions demonstrate considerable power in high power distance cultures. In contrast, in low power distance cultures, individuals are less likely to accept hierarchical inequality and participate in decision-making [21]. For example, Hofstede Insights indicates that Saudi Arabia scores high on this dimension with a score of 95. This research demonstrates that citizens in the country follow a hierarchal order in which everyone has a status and requires no justification [22]. This cultural dimension tends to represent an obstacle and has a negative effect on the country's information security practices [21]. Thus, power distance is a factor that affects cybersecurity practices in UAE culture. Whereas power distance tends to be higher in the UAE, the United States has a comparatively lower score on this dimension [22]. Since Americans are less likely to accept rigid power structures, this dimension does not significantly impact their information security practices. In this regard, Hofstede's framework can draw comparisons between cybersecurity behaviors in the UAE and the USA.

Another cultural dimension of Hofstede's framework that impacts cybersecurity behavior in the UAE is individualism-collectivism. According to [20], this scale is a measure of whether people prefer to work within groups or alone. Individualist cultures value personal accomplishments over group achievements, whereas collectivist cultures emphasize the group's well-being rather than individual desires [23]. To illustrate this point, Saudi Arabia is a country that measures high on collectivism and low on individualism [24]. This may suggest that Saudi society is less likely to implement and adopt cybersecurity practices in their culture. In contrast, the United States is an individualistic country with independent values [22]. Given its high individualism, the USA is more likely to integrate cybersecurity practices into its culture. For instance, a recent study found that countries from national cultures that express individualism tend to perform better in cybersecurity development [25]. Given its highly individualistic culture, the United States has a high level of cybersecurity development. Therefore, individualism-collectivism may explain differences in cybersecurity behavior between the UAE and the USA.

The Masculinity and Femininity (MF) aspect of Hofstede's cultural model represents societal values, ranging from the pursuit of achievement, heroism, assertiveness, and material success (masculinity), to favoring cooperation, modesty, care

for the vulnerable, and a focus on life quality (femininity) [26]. These cultural preferences could shape individual attitudes towards cybersecurity procedures, the understanding of cyber threats, and the emphasis placed on cybersecurity strategies. We believe that there is a potential difference in the MF dimension between the United Arab Emirates (UAE) and the United States (USA) populations, which may influence cybersecurity behaviors. The USA, scoring highly on the masculinity scale tends to prioritize achievement and success, possibly leading to a competitive approach to cybersecurity awareness. Conversely, the UAE, with a tendency towards the femininity side of the scale, appears to adopt a cooperative stance, emphasizing collective responsibility for cyber safety [26]. These cultural distinctions are expected to provide valuable insights into the divergent cybersecurity behaviors we plan to further examine in our study. Hofstede's initial survey had estimation errors, particularly in the masculine-femininity dimension, challenging the notion that the US society is more feminist than the UAE [27].

The final aspect of Hofstede's framework that affects cybersecurity behavior in the Middle East is uncertainty avoidance. Alamri et al., [28] define uncertainty avoidance as the degree to which members of a culture feel a sense of threat in ambiguous or uncertain situations. Research suggests that Arab countries such as Saudi Arabia measure high on this dimension. Given their high levels of uncertainty avoidance, countries in the Middle East are less likely to integrate new technologies and cybersecurity practices into their culture [29]. On the other hand, the opposite is true when it comes to the United States. Unlike the UAE's fear of uncertainty, the USA has been found to score only a moderate degree on this dimension. This indicates that the country shows a fair degree of acceptance and is willing to be exposed to new experiences [30]. The USA places great value on technology, innovation, and individual initiatives and embraces new scientific advancements. Consequently, Patton [30] proposes that the USA is more likely to adopt cybersecurity practices than other countries. Therefore, uncertainty avoidance is a cultural factor highlighting significant discrepancies between cybersecurity behavior in the UAE and the USA.

In summary, Hofstede's framework can be used to inform researchers about cybersecurity policy development. Exploring the specific themes or human factors that cause a difference in cybersecurity practices and their implications remains under investigation. Therefore, the central focus of this paper is to expand onthe cultural differences, as indicated by Hofstede's framework between the tech-savvy and educated populations in the UAE and USA, and then identify human factors that affect cybersecurity behaviour in these diverse cultures. Theoretically, it is evident from the above discussion on Hofstede's framework that the citizens in the UAE and USA regions belong to opposite poles on the power distance, individualism-collectivism, masculinity-femininity, and uncertainty avoidance continuums. Prior research points to cultural and behavioral differences between the tech-savvy, educated populations in the USA and UAE, especially regarding cybersecurity awareness [26], [14]. However, very little is known about certain human factors, such as cognitive biases and social influences to better understand the human dimension of cybersecurity. Our hypothesis suggests these factors will reveal cultural and behavioral differences in newly identified cybersecurity awareness constructs among these populations. Thus, we hypothesize that:

H1: the tech-savvy and educated populations in the UAE and USA regions will predominately demonstrate cultural and behavioural differences with respect to the newly elicited cybersecurity awareness constructs and overlooked human factors.

We believe that this comparative investigation will allow the governments and relevant law enforcement agencies in the UAE region to further enhance cybersecurity policymaking and reduce cybersecurity risks for their citizens.

III. RESEARCH METHOD

A. SURVEY INSTRUMENT

We used a causal-comparative research design to determine the difference in cybersecurity awareness between two distinct groups (respondents from the UAE versus respondents from the USA). We ensured that education, gender, age group, and qualification were controlled (see Table 1 for details). We have discussed the effects of these variables on the cybersecurity practices in detail in the descriptive statistical section below. A minimum sample size of 122 respondents from our targeted populations was estimated using the G∗power 3.0 program by [32].

In addition to systematically reviewing prior literature, the survey was developed in consultation with five global cybersecurity experts specializing in cybersecurity awareness and cybercrime prevention. The sampling strategy was designed to target individuals with expertise and experience in the specific topic of cybersecurity. We employed rigorous selection criteria, including pre-screening measures and targeted recruitment from professional networks, to ensure the inclusion of knowledgeable participants. Semi-structured interviews were initially carried out with these experts to develop questions for the survey. The interviews lasted thirty to forty-five minutes each. The experts were asked to enlist the most common cybercriminal activities in the global and GCC regional contexts. The results of the interview process were structured and coded using NVivo 12 Pro. We later applied thematic analysis to identify themes (also referred to as constructs) that helped us craft the survey questions. As a result, only one construct emerged, termed cybersecurity awareness, consisting of fourteen items (questions) about preventative practices, experiences with cybercrimes, and perceptual reflections about feeling safe and secure online.

1) DESCRIPTIVE SECTION

In total, our survey consisted of thirty questions. The first question was set up to gather consent from the study participants. We asked four demographic questions about age,

gender, professional, and educational background, categorized as control variables in the study. In addition to the fourteen Likert scale questions (to measure the cybersecurity awareness construct), we also carefully crafted another eleven descriptive questions, that sheds light on other important factors, such as experiences and reporting of cybercrimes, password compositions, the prevalence of protective software, the ranking of common cybercrimes, and monetary loss.

2) CYBERSECURITY AWARENESS

Our resultant theme of cybercrime awareness outlines several sub-categories. These factors have been deduced from extensive literature review and elicited constructs from our five cybersecurity experts. Within this category, while developing the survey instrument, we inquired about whether individuals opened their emails received from unknown sources or not. We also probed about users storing important documents or credentials, such as credit card information, in the web browser. Other important issues were also highlighted: how often users secure their data or files using a password or encryption techniques. How often do they check the security features of a website before sharing sensitive information online? We further explored how often online users update their social media apps or devices and how often they change their account passwords or privacy settings. Lastly, we wanted to know how comfortable users feel about the multi-factor authentication techniques that many social media accounts require to function.

Furthermore, we inquired about the frequency of phishing requests. For instance, how often do users receive fake urgent requests in an email to reset their password? We also investigated whether participants' close family or friends also fell victim to phishing attacks or received messages from fake accounts/strangers. We then asked about how common cyberbullying is, and whether participants of the study have experienced it themselves or witnessed it being done to others. Among related issues was how secure users felt about sharing information on social media and performing online banking. Lastly, we wanted to inquire whether respondents have awareness or experience Artificial Intelligence (AI) agents, such as ''bots'' operating in the social media space.

A 7-point Likert scale was used in the survey to explore potential differences between respondents from the UAE and respondents from the USA. On this scale, 1 depicted ''Not at all,'' whereby 7 described, ''A great deal/Regularly.'' Both these survey studies were administered online using the SurveyMonkey®tool.

This study is notable for its comprehensive analysis of human factors and their influence on cybersecurity practices. It adopts a unique comparative approach, examining cultural and organizational contexts in the USA and UAE regions, to provide valuable insights for stakeholders. By highlighting the significance of addressing human vulnerabilities and decision-making in cybersecurity, the research contributes to the improvement of practices and policies in this field. To design more effective cybersecurity technologies, it is essential to incorporate human factors into the systems' design, considering cultural considerations. Traditional technologies have often focused excessively on infrastructure, following a one-size-fits-all approach, such as the castle model. However, for policymaking, it is crucial to tailor strategies to address the specific cultural needs of the local context. The approach should be flexible, acknowledging the heterogeneity of factors in the local landscape.

B. PARTICIPANTS

Study participants were initially screened to determine whether they met the inclusion and matching criteria. We set the criteria to include participants who have completed secondary education and are pursuing or have already pursued professional education. After receiving ethics approval from our institution's Office of Research Ethics to conduct the study with human participants, we circulated the survey to a well-reputed post-secondary institution in the UAE. Our survey instrument remained open for three weeks to collect responses. To recruit our participants from the USA, we used Amazon Mechanical Turk and restricted the settings to only recruit participants from that region. On average, the questionnaire took 10 minutes to complete. A total of 157 individuals participated in the survey from the USA and 176 from the UAE. There were no incomplete responses from our USA sample. However, only eleven respondents from the UAE submitted incomplete survey responses, which failed to meet the inclusion criteria and were excluded from our analysis. As a result, 157 and 165 survey responses from the USA and UAE regions were used for further statistical analyses. The survey was conducted independently, without the sponsorship from an organization. This was done to ensure unbiased data collection and research integrity. Additionally, we collected demographic information to identify any biases and employ statistically control while conducting data analysis. The respondent's demographic detail is presented in Table 1.

The overwhelming majority of respondents from the USA and UAE have a background in Science, Technology, Engineering, and Mathematics (STEM) related education/professions. According to our survey, the following branches refer to STEM disciplines: IT, enterprise systems, cybersecurity, computer sciences, engineering, mathematics, life sciences, and physical sciences. Respondents could select as many options in this question as they desired. We received 163 (103.2%) responses from the USA sample in the STEM category, whereby 217 (131.73%) respondents picked this discipline from the UAE sample. This similarity in age groups, education, gender, and professional backgrounds in these two populations helps us draw meaningful conclusions.

IV. RESULTS

This section provides a detailed descriptive analysis of categories, such as experiences and reporting of cybercrimes, password compositions, the prevalence of protective software, the ranking of common cybercrimes, and monetary

TABLE 1. Demographic details of the study participants.

		Study Sample 1: USA N=157	Study Sample 2: UAE N=165
Education			
	Less than high school	0	0
	Post-secondary/undergraduate degree	114	143
	MBA/Master's or equivalent graduate degree	42	8
	Doctorate or equivalent graduate degree	1	10
	Prefer not to answer	0	2
	Other (please specify)	0	2
Age			
	I am under 20 years of age	4	20
	I am between 20 and 45 years of age	136	142
	I am over 46 years of age	17	3
	I prefer not to answer	0	0
Gender			
	Male	40	43
	Female	117	120
	I prefer not to answer	0	2
	Other (please specify)	0	0
Profession			
	Information Technology	60	136
	Enterprise systems	60	6
	Cybersecurity	16	54
	Computer sciences	0.	0
	Engineering	53	12
	Business	34	16
	Arts / Humanities	11	2
	Mathematics	10	6
	Social sciences	18	1
	Life sciences	8	2
	Physical sciences	8	1
	Prefer not to answer	3	2
	Other (please specify)	3	12

losses. Also, we conducted a statistical analysis of the cybersecurity awareness questionnaire (fourteen 7-point Likert questions) by drawing comparisons among the means of two groups (i.e., the UAE and the USA).

A. DESCRIPTIVE ANALYSIS

1) CYBERCRIME EXPERIENCES

In our survey, we asked respondents whether they personally experienced or suspected cybercrime. An overwhelming majority, 68.79% from the USA sample (n = 157), reported "Yes," while 17.83% reported "No." Only 10.83% reported "Probably Yes," and 2.55% reported, "Probably Not." However, none of the respondents selected the "Don't Know" option. In contrast, respondents from the UAE sample (n = 165) reported very different answers. The majority of them (34.73%) answered "No" to this question. However, 32.34% selected "Yes." Only 17.96% and 10.18% answered "Probably Yes" and "Probably Not," respectively. Furthermore, 4.79% said that they "Don't Know" about experiencing a cybercrime situation.

Similarly, in another question, we asked whether people in their close circle (e.g., family, friends, and relatives experienced or suspected a cybercrime situation). The majority, 65.61%, of respondents from the USA, picked "Yes," versus 39.39% from the UAE sample. At a similar level, 14.01% from the USA and 18.10% from the UAE picked "No" as their choice. Fewer, 10.83% of respondents from the USA picked "Probably Yes," versus 24.85% of respondents from the UAE suspected "Probably Yes." Very few, 2.55% from the USA sample answered, "Probably Not," whereby 10.91% from the UAE picked this answer. An almost similar number of respondents (7.01% from the USA and 6.67 from the UAE) picked "Don't Know" as their response.

Amongst devices, the majority (75.16%) of the USA respondents reported that they experienced or suspected cybercrime while using a laptop. These figures dropped significantly for operating a gaming console (7.01%), Apple iPhone (8.92%), and smartwatch (18.47%). On the other hand, Android phones (28.03%) and desktop computers (47.77%) ranked somewhere in the middle. The same respondents also revealed that they mainly experienced such cybercrime incidents at their workplace/university (61.15%) and home (59.87%), followed by public places (20.38%), such as shopping malls and airports. In comparison, the majority (66.05%) of our respondents believe that they have experienced cybercrime incidents on their Apple iPhones. This finding seems counterintuitive and warrants further research. Generally, Apple products are considered to be much safer than other devices. Our respondents from the UAE also reported laptops at the second position (56.79%), followed by Android phone (46.30%). Their responses about gaming consoles (12.35%) and smartwatches (4.94%) appeared very similar to their counterparts in the USA. The majority (82.72%) of the UAE respondents mentioned that they experienced cybercrime incidents at home. Approximately 31% and 25% experienced it in public places and workplaces/universities. In this particular question, respondents could select multiple options.

2) REPORTING OF CYBERCRIMES

When asked whether they report digital or online crimes to a security agency, about 67% said "Yes" from the USA, compared to only 31.52% from the UAE. About 39% of the UAE indicated that they do not possess much knowledge about reporting cybercrimes to relevant authorities, compared to only 2.55% from the USA. This finding provides an opportunity for relevant stakeholders, such as the government, educational institutions, organizations, and law enforcement agencies in the UAE, to better educate citizens about reporting cybercrimes.

3) PASSWORD COMPOSITION

We also inquired about how many different passwords respondents use to operate online (i.e., using banks, social media accounts, online shopping portals, etc.) The majority, 49.7% of respondents from the UAE region, picked 3 to 4 passwords to respond to this question. This outcome

is similar to the USA sample, where 54.14% picked the same 3 to 4 passwords option. However, we asked them about what constitutes their passwords. This question allowed respondents to choose as many options as they deemed fit. We noticed that our UAE respondents showed all the best practices of picking almost all of the categories: at least 6 to 8 characters (86.06% versus 63.33% in the USA); at least an uppercase letter (84.24% versus 43.31% in the USA); at least a lowercase letter (76.97% versus 46.5% in the USA); at least a number (80% versus 37.58% in the USA); and at least a special character (69.7% versus 28.03% in the USA).

4) PREVALENCE OF PROTECTED SOFTWARE

In response to our question about installing security software, such as antivirus, anti-spyware, and firewalls on their systems, 80.89% of respondents in the USA said ''Yes,'' versus 68.48% in UAE. Almost 15% of the UAE respondents mentioned that they do not know about it, compared to only 3.18% from the USA.

5) RANKING COMMON CYBERCRIMES

In particular, we asked whether respondents believe that their social media accounts have been hacked. In summary, 68.15% from the USA said ''Yes,'' compared to 52.12% from the UAE. A larger number of respondents, 24.24% from the UAE, answered that they did not know, compared to only 6.37% from the USA.

The majority (50.96%) of the USA respondents mentioned social media fraud when asked what types of cybercrimes they experienced or suspected. This is followed by email fraud (38.85%), bank account fraud (32.48%), phone call fraud (31.21%), credit card fraud (29.94%), cyberbullying (22.93%), e-commerce fraud (21.66%), and personal data leaks (9.55%). However, in contrast, the majority of the UAE respondents (61.59%) reported phone call fraud. This is then followed by email fraud (54.27%), social media fraud (45.73%), credit card fraud (40.24%), e-commerce fraud (28.66%), bank account fraud (26.22%), cyberbullying (21.34%), and personal data leaks (17.68%). In this particular question, respondents had the option to make multiple selections.

6) MONETARY LOSSES

The majority of study participants (52.87%) from the USA mentioned that they or people in their close circle had incurred a monetary loss between US$ 1 and US$ 1,499. Whereby 22.93% reported losses between US$ 1,500 and US$ 2,999. Similarly, only 12.74% reported losses between US$ 3,000 to US$ 9,999, while 11.04% reported no losses. Compared to this, the majority (58.18%) in the UAE reported that they or people in their close circle had not incurred any monetary losses. Almost 26% of them reported losses between AED 1 and AED 4,999 (approximately US$ 1 and US$ 1,500). Only 9.09% suffered losses between AED 5,000 and AED 9,999 (approximately US$ 1,500 and US$ 2,999). In contrast, 6.67% reported a loss between AED 10,000 and AED 50,000 (approximately US$ 3,000 and US$ 15,000).

B. STATISTICAL ANALYSIS OF CYBERSECURITY QUESTIONNAIRE

An independent sample t-test was used in this study. There were no outliers in the data, as assessed by inspection of a boxplot. The results were normally distributed, as assessed by Shapiro-Wilk's test ($p > .05$), and variances were homogeneous, as assessed by Levene's test for equality of variances ($p = .164$). All descriptive statistics, such as the mean and standard deviations, are shown in Table 2. The outcomes of this research study indicate that there are several areas in which cybersecurity awareness among respondents from the UAE is statistically significantly different from their counterparts in the USA. We first ran the study in the UAE. Based on the demographics, we set similar controls on Mechanical Turk to ensure the experiment's demographic makeup was similar to the USA data set. Additionally, we observed similar outcomes by comparing the males in the UAE population ($n = 42$) to the USA population ($n = 40$). These steps enabled us to control gender biasness in our study.

This questionnaire consisted of fourteen Likert-scale (7-point) questions. The scale had a high internal consistency level, as determined by a Cronbach's alpha of 0.794. We believe that translating the questionnaire in the local languages (instead of relying on local interpreters to conduct questionnaires), brining clarity in item wording, limiting redundancy, and adding more items when aligned with the measured construct might further enhance the internal consistency scores. These steps could increase the internal consistency and reliability of future questionnaires. The results of the t-test (in Table 3) indicate that items 1, 3, and 4 were statistically insignificant, whereby the remaining items 2, 5, to 14 were statistically significant.

V. DISCUSSION

This section explains the results and discusses the implications of our findings to allow relevant cybersecurity stakeholders to develop an effective strategy against the cybercrime pandemic globally. Our paper significantly contributes to the field by examining the role of human factors in cybersecurity and their implications for cyber governance. The findings expand the understanding of the socio-technical aspects of cybersecurity, highlighting the need to address human vulnerabilities alongside technical measures. This has practical implications for policymakers, organizations, and cybersecurity professionals, empowering them to enhance strategies, policies, and practices to mitigate risks effectively and improve overall security resilience.

Our study investigated specific human factors that affect cybersecurity behaviour in diverse cultures. Prior studies have not addressed this gap adequately. We further probed the issue of whether people in different geographies behave differently online. We conducted two empirical survey studies on the UAE and USA populations while controlling various factors, such as age group, gender, and educational and professional qualifications.

TABLE 2. Descriptive statistics of "cybersecurity awareness" construct.

Questions	Groups	N	M	SD	SE
1. How careful are you about opening an email/attachment received from an unknown person or account?	UAE	166	5.66	1.77	0.14
	USA	155	5.65	1.77	0.09
2. How often do you secure your data or files by using a password or encryption technique?	UAE	160	4.28	2.00	0.16
	USA	157	5.69	1.21	0.10
3. How often do you check the security features (e.g., https://) of a website before sharing sensitive (e.g., banking) information on it?	UAE	162	5.45	1.93	0.15
	USA	155	5.62	1.14	0.09
4. How often do you update your apps (social media) or devices when available?	UAE	164	5.63	1.62	0.13
	USA	156	5.69	1.17	0.09
5. How comfortable do you feel when your social media account requires you to enter your phone number to authenticate your account during sign-up?	UAE	162	4.37	2.00	0.16
	USA	156	5.33	1.35	0.11
6. After signing up for a social media account (e.g., Facebook, Instagram, etc.), How often do you change your account password or privacy settings?	UAE	161	3.75	1.89	0.15
	USA	156	5.38	1.30	0.10
7. How often do you store important documents/credentials (e.g., credit card information) in the system browser?	UAE	162	3.05	1.97	0.15
	USA	155	5.05	1.66	0.13
8. How secure do you feel about your information available on social media?	UAE	163	3.85	1.64	0.13
	USA	156	5.45	1.45	0.12
9. While doing online banking and shopping, how safe do you feel on the Internet?	UAE	161	4.13	1.79	0.14
	USA	156	5.37	1.22	0.10
10. How often do you receive a fake "urgent" request in an email to reset a password?	UAE	162	3.62	2.04	0.16
	USA	155	5.10	1.53	0.12
11. How aware are you of the "bots" operating in the social media space?	UAE	147	4.47	1.82	0.15
	USA	156	5.41	1.25	0.10
12. How often do you experience or witnessed someone else being humiliated/harassed on social media?	UAE	156	4.53	1.95	0.16
	USA	156	5.37	1.39	0.11
13. How often do you or people in your close circle (e.g., family, friends, and relatives) experience phishing attacks (such as emails or call inquiries for personal or financial information)?	UAE	154	4.44	1.72	0.14
	USA	156	5.26	1.27	0.10
14. How often do you or people in your close circle (e.g., family, friends, and relatives) receive a message from an unknown or fake account on social media?	UAE	150	4.53	1.76	0.14
	USA	155	5.15	1.24	0.10

We attempted to address these questions in our detailed study: What specific human factors affect cybersecurity behaviour in diverse cultures, such as the UAE and the USA)? And why is it important to draw this comparison? How can these findings inform governments at a global level to enhance cybersecurity policymaking?

A detailed analysis of descriptive and Likert scale questions revealed that the UAE population lacks cybersecurity awareness at various levels. A combined view of the twenty-five (eleven descriptive and fourteen Likert scales) factors provides in-depth knowledge about the targeted, technology-savvy population in the UAE to be diverging from their USA counterparts. These results collectively confirm that superior measures are required for effective cybersecurity policymaking in different parts of the world, especially in regions like the UAE.

A. EXPLANATION OF RESULTS

This study examines cybercrime and cybersecurity awareness in the USA and UAE, revealing some key differences. A larger portion of respondents from the USA (68.79%) reported personal experiences or suspicions of cybercrime compared to UAE participants (32.34%). Moreover, a higher percentage of participants from the USA reported cybercrimes (67%) compared to the UAE (31.52%). Participants in both countries predominantly experienced cybercrimes through laptops, though in the UAE, Apple iPhones were also a common source.

UAE participants demonstrated safer password practices, though protective software use was higher in the USA (80.89%) than in the UAE (68.48%). The most common types of cybercrimes differed between the two regions, with social media fraud most frequently reported in the USA and phone call fraud in the UAE.

Statistical analysis of cybersecurity awareness showed significant differences between the USA and UAE, with the USA scoring higher in areas like data security practices, comfort with sharing phone numbers for social media authentication, changing social media passwords or privacy settings, storing important documents/credentials in the browser, and awareness of social media ''bots''.

While there are common behaviors and experiences between the groups, the study suggests that the USA participants demonstrate greater cybersecurity awareness and preventative behaviors, despite having higher exposure to cybercrime. UAE respondents report less cybercrime but also show less awareness and reporting of such incidents. This research underscores the need for enhanced cybersecurity education and policies in regions like the UAE and highlights the importance of future research to better understand and address the differences between the two regions.

The outcomes of this research study also indicate that there are several areas in which cybersecurity awareness

TABLE 3. Independent samples T-Test of "cybersecurity awareness" construct.

	df	Sig. (2 tailed)
1. How careful are you about opening an email/attachment received from an unknown person or account?	319	0.950
2. How often do you secure your data or files by using a password or encryption technique?	315	0.00**
3. How often do you check the security features (e.g., https://) of a website before sharing sensitive (e.g., banking) information on it?	315	0.350
4. How often do you update your apps (social media) or devices when available?	318	0.69
5. How comfortable do you feel when your social media account requires you to enter your phone number to authenticate your account during sign-up?	316	0.00**
6. After signing up for a social media account (e.g., Facebook, Instagram, etc.), How often do you change your account password or privacy settings?	315	0.00**
7. How often do you store important documents/credentials (e.g., credit card information) in the system browser?	315	0.00**
8. How secure do you feel about your information available on social media?	317	0.00**
9. While doing online banking and shopping, how safe do you feel on the Internet?	315	0.00**
10. How often do you receive a fake "urgent" request in an email to reset a password?	315	0.00**
11. How aware are you of the "bots" operating in the social media space?	301	0.00**
12. How often do you experience or witnessed someone else being humiliated/harassed on social media?	310	0.00**
13. How often do you or people in your close circle (e.g., family, friends, and relatives) experience phishing attacks (such as emails or call inquiries for personal or financial information)?	308	0.00**
14. How often do you or people in your close circle (e.g., family, friends, and relatives) receive a message from an unknown or fake account on social media?	303	0.00**

** p <0.01

among respondents from the UAE is statistically significantly different from their counterparts in the USA. Out of fourteen Likert scale items, only three factors resulted in similar higher awareness levels among respondents from the UAE and USA. These three factors are: a) opening an unsolicited email from an unknown person, b) checking security features (e.g., https://) of a website before sharing sensitive (banking) information, and c) updating apps or devices regularly. The remaining eleven items (factors) showed statistically significantly different results for the UAE and USA populations.

Among the ones that are statistically significantly different, it is interesting to note that respondents from the UAE scored less than their USA counterparts in terms of using passwords or encryption techniques to transfer files, comfortable in using phone number authentication for creating social media accounts, changing account password and privacy settings after signing up on social media services, storing important credentials (e.g., credit card information) in system browser, making personal information available on social media, doing banking and shopping online, experiencing urgent unsolicited email requests to change password, awareness about "bots" operating in social media space, cyberbullying, and awareness of phishing attacks and receiving of messages on social media from fake accounts.

Overall, these results predominantly support our hypothesis (H1) that the tech-savvy and educated populations in the UAE and USA regions will demonstrate cultural and behavioural differences with respect to the newly elicited cybersecurity awareness constructs and overlooked human factors. These findings also indicate that our targeted population in the UAE is very conservative about fully exploring the extent of online services (e.g., banking, shopping, and social media) compared to the USA population. There are two possible explanations for this behaviour among the UAE respondents: a) lack of awareness about these factors or b) lack of trust in operating safely online. Either way, this depicts an important area for further exploration. We believe that our empirical findings provide guidance for cybersecurity policymakers in the UAE and the extended GCC region to focus on these significant factors for enhancing cyber safety, awareness, and trust. We also propose various interventions that relevant stakeholders, such as governments and law enforcement agencies, can implement to reduce cyber risks in the region.

B. REASONS FOR RELATIVELY LOW AWARENESS IN THE UAE

Since our findings indicate that the UAE respondents differed in demonstrating adequate cybersecurity awareness compared to the USA population, it is useful to uncover the underlying reasons for the rise of cybercrime and low cybersecurity awareness in the UAE and other GCC countries. We also acknowledge that although the UAE is ranked very high on the Global Talent Competitiveness Index in terms of attracting top talent by offering internal and external openness [33], there is room for improvement in terms of innovation and technology outputs [34].

Cybercrime has long been a contentious issue in the region. The last decade has seen a drastic increase in the number of cybercrime incidents [35]. Research indicates that several factors contribute to the rise of cybercrime, such as the growth of the user base, lack of training for law enforcement, and lack of regulations [7]. Also, information security awareness has proven to be one of the strongest lines of defense against cybercrimes. There is a serious lack of security awareness among the population of other GCC countries which has its bearing on the UAE. Users are not educated enough on cybercrime and lack basic knowledge of information security concepts. Consequently, limited security awareness among users has made the region an attractive target for cybercriminals [36].

We also take this to mean that since the UAE government provides adequate safety to its citizens, the general population does not feel the immediate need to protect themselves

against cybercrimes. This may also have to do with the UAE culture, which focuses on collectivism, compared to the USA, which is more geared towards individualism. In case of a cyber breach, an extended circle of family, friends or the government would likely provide relief to the individual in the UAE. A similar outcome may be different in the USA. The stakes are also considered low in the UAE, as compared to the counterparts of the USA. For instance, someone with a cyber breach or identity theft in the USA may run into a variety of serious financial and social issues. However, UAE protections might result in less serious outcomes.

1) GROWTH OF THE USERBASE

Perhaps, the most important factor contributing to rising cybercrime in the region is the growth of the user base. With the increasing availability of broadband connections, the number of online users in the GCC countries has surpassed the rest of the world [7]. For instance, a longitudinal study found that in the past 10 years, the GCC region had registered an internet usage growth of 1825% compared with 445% in the rest of the world [37]. This growing number of users has made the Internet a popular means of communication and opened up new online businesses in the GCC countries. However, at the same time, it has also led to an increase in the number of cybercrime incidents. To provide a specific example, one of the fastest developing countries in the region that has been particularly affected by cyber-attacks is Saudi Arabia. According to Alotaibi [38], Saudi Arabia is the second largest e-commerce market in the region, with figures accounting for $520 million. Due to its overreliance on the Internet, the country has become a popular hotspot for cybercrime, with 60 million cyber-attacks witnessed in 2015 alone [38]. In this respect, the Internet's reliance on various activities has made the whole region more vulnerable to cyberattacks.

2) LACK OF SECURITY AWARENESS PROGRAMS

Another factor contributing to cybercrimes is a lack of security awareness. El Guindy [7] argues that there is a lack of security awareness initiatives for the public, organizations, and enterprises. Although security awareness programs do exist, they are generally considered to be ineffective. Moreover, most IT security awareness programs are available only in English, making them difficult to implement in the region [7]. Furthermore, [35] concur that there is a need for effective information security awareness programs in the GCC countries. For instance, these researchers found a clear lack of knowledge concerning information security concepts and low awareness levels within the GCC region's educational environments. An extensive study conducted in the academic sector indicated that participants did not possess the requisite knowledge of information security principles and their application in day-to-day work [35]. Implementing security awareness programs can alleviate these issues among the masses as it would help them develop a deeper understanding of cybersecurity principles.

3) SLOW-PACED LEGISLATION

Another factor that contributes to cyberattacks in the GCC countries is poor laws and regulations. According to El Guindy and Hegazy [39], cybercrime legislation in the region is largely absent. While a few countries, such as Oman, Saudi Arabia, and the UAE, have attempted to form new legislation for cybercrime, there is a need for more specific cybercrime activities. Governments often use traditional laws, penal codes, or emergency regulations, making it hard to investigate real cases of cybercrime [39]. This inconsistency in law makes it almost impossible to efficiently address the issue of cybercrime in the region.

Similarly, Al Amro [40] concurs that there is a need for more specific laws to address cybercrime in the region. Their study highlights that many countries merely use emergency laws rather than laws that address online crimes against citizens [40]. Other countries have attempted to prevent misconduct by blocking access to illegal websites. However, these procedures have proven ineffective because emergency regulations are not explicitly designed to combat cybercrime

4) EDUCATION

Arguably the most important factor that affects information security awareness is the education of users in the GCC countries. According to Aloul [36], user education and training are crucial to combating IT security threats. Uneducated users can easily target hackers and increase their vulnerability to cyberattacks [36]. However, research suggests that little effort is being made to educate users about cybercrimes. For instance, a survey conducted in three cities, including Abu Dhabi, Dubai, and Sharjah found that 35% of organizations employed Wi-Fi Protected Access (WPA) encryption, 33% employed WEP encryption, and 32% had no encryption [36]. These findings suggest limited security awareness among users and a pressing need for further education in the region. Furthermore, Alqurashi et al., [41] believe that education is one of the most effective tools that can be used to combat cybercrime.

Unfortunately, there is currently no operative approach or proposal to advance cybercrime education in the region [41]. To confront cybercrime, Alqurashi et al., [41] propose that administrations must advance their workforce and inhabitants' education. Despite this lack of progress, Aboul-Enein [42] argues that a few awareness campaigns are currently in place in Oman, Saudi Arabia, Qatar, and the UAE to increase cyber education. For instance, one proposal involves the United Nations Women and its programs for Syrian refugee women. In this manner, the research suggests minimal efforts are being made to educate GCC citizens on the dangers of cybercrimes

5) THE INTERNET GENDER GAP

In relation to education, another factor that poses challenges to cyber stability is the Internet gender gap. According to an extensive report by the Government Commission on Internet Governance [43], many individuals in the region are denied

Internet access due to high costs and limited availability of the necessary technology. Most women have lower earnings and less control over spending than men and are disproportionately affected by a lack of access to the Internet [43]. Consequently, limited access to the Internet reduces information security awareness and knowledge among women in the GCC countries. To illustrate this point, another report by Intel (2012) found that nearly 25 percent fewer women than men have access to the Internet in the developing world.

Moreover, it is estimated that almost 35 percent fewer women than men have Internet access in the GCC countries alone (Intel, 2012). This lack of access to the Internet puts women at a severe disadvantage compared to men. Not only does it reduce their sense of gender equity, but it puts them at greater risk of becoming victims of cybercrimes. Gender-wise differences have also been observed in terms of behaviour and self-efficacy in cybersecurity [45]. In this regard, bridging the Internet gap can transform women's lives by contributing to greater awareness of information security. To become conscious of cyber-attacks, women need to be given ample access to the Internet and equal opportunities to build knowledge. Bridging the Internet gender gap would provide women with the tools necessary to make information security awareness better equipped to combat cybercrimes. Therefore, addressing the Internet gender gap will pave the way for vast improvements in women's information security awareness in the GCC region

6) CULTURE

The final component that influences information security awareness in the GCC is cultural practices. According to Alzahrani and Alomar, cultural values play an essential role in individuals' information security awareness. We did not come across significant literature discussing the impact of culture influencing cybersecurity awareness in the UAE. However, we found some unique studies that explain the impact of culture on Saudi Arabia. While the UAE's situation might be more relaxed than Saudi Arabia's. It certainly has a traditionally orthodox culture and similar to Saudi Arabia in many aspects. It is important to note that Saudi Arabia's national culture substantially affects its information security awareness. In a study involving undergraduate students in Saudi Arabia, these researchers found low information security awareness. To account for these results, the researchers explain that information security awareness is low mainly due to the highly censored, patriarchal, and tribal nature of Saudi culture. Furthermore, Al Arifi et al., [47] found that its culture influences Saudi Arabia's poor information security rating. In an extensive survey, these researchers found several information security risks linked to the country's culture. For instance, most participants in the study were comfortable sharing their passwords with family members. Moreover, the majority of participants believed that the government or other information providers were responsible for information security. Finally, Alnatheer and Nelson [24] contended that cultural factors impact the information security awareness of individuals in Saudi Arabia. Studies have found that the country has specific cultural characteristics that lower its chances of implementing information security. For instance, cultural research based on Hofstede's framework found that the country measured high on the following scales: power distance, uncertainty avoidance, collectivism, and femininity [21]. These factors tend to be obstacles and prevent the adoption of information security practices in Saudi Arabia.

According to Sofio and Carter [48], cybersecurity culture is perceived from the "end-users" viewpoint. It enables them to become conscious of various threats of online malpractices and avoid bad practices to enhance cybersecurity. In the USA, among other important laws and regulations, the "Cybersecurity Culture and Compliance Initiative (DC31)" and "Promoting Good Cyber Hygiene Act" have enabled the US government to protect businesses, ordinary citizens, and military establishments against vulnerabilities. It is generally believed that providing education about cybersecurity or creating awareness about effective practices will significantly reduce cybercrimes. This notion is quite intuitive; however, we contend that the dynamics of different regions or countries are so diverse that it will not be enough to implement the laws and rules of one particular region into another.

We believe these implications from our study will guide relevant authorities in the UAE to take measures that can increase cybersecurity awareness among citizens. In the following section, we elaborate on some of the points discussed earlier as practical recommendations for the future.

C. PRACTICAL IMPLICATIONS: WHAT CAN BE DONE TO IMPROVE CYBERSECURITY AWARENESS IN THE UAE

1) TRAINING PROGRAMS AND INTERVENTION

In light of the above discussion, there is a pressing need for stakeholders, such as organizations, governments, and law-enforcement authorities, to implement interventions to improve information security awareness among the general population, business organizations, and employees. Research indicates that targeting individuals' attitudes and implementing cybersecurity awareness programs are considered proactive steps to prevent cybercrime. It is also important that training programs serve the needs of distinct stakeholder groups at the start-up, growth, and mature organizational life cycle stages of technology firms. At each organizational developmental stage of the information and communications technology sector, stakeholders either evolve or change, presenting organizations with unique challenges to overcome and providing an opportunity to create sustainable technological advancement [49], [50].

a: TARGETING EMPLOYEES' ATITUDES

One of the most effective ways organizations can improve information security awareness is by targeting employees' attitudes. According to [51], employees' perceptions, attitudes, and behavior play a significant role in their information security awareness. In a study investigating employees' attitudes, these researchers found constructivist methods to

enhance awareness of information security ideas and concepts [51]. The constructivist method involves the active engagement of individuals interacting in enjoyable activities to improve information security awareness. These findings suggest that constructivist methods are an effective way of boosting information security awareness.

Moreover, [52] contended that targeting employees' attitudes improves their information security awareness. In their investigative study, these researchers found that employees' information security awareness significantly affected attitudes toward security compliance [52]. In this respect, the researchers suggested that it is important to create a security-aware culture within an organization, posing a significant threat to both business and non-business entities. Prior research has also indicated differences in terms of smartphone cybersecurity-related behavioural preferences of employees in regions such as the UK, USA, and UAE [26]. To ward off the dangers posed by cybercrimes, it is essential to create a positive culture that promotes security awareness. By targeting employee attitudes, organizations can go a long way in improving information security awareness.

b: SECURITY AWARENESS AND TRAINING PROGRAMS

Another approach that can be employed to prevent cybercrimes is implementing Security Awareness and Training programs (SAT). According to Eyadat [53], using an SAT program is one of the most important steps organizations or other relevant agencies can take to prevent cybercrimes. Security awareness programs are designed to modify any person's behavior that threatens the organization's security [53]. These programs are extremely effective in that they minimize the risks of cybercrimes. However, in his study, Eyadat [53] found an alarmingly low SAT program employed by educational institutions in the GCC region. The results indicated that the majority of institutes offered no SAT program, and only 30% offered a complete or partial program [53]. Therefore, universities must integrate security awareness and training programs into their curriculum.

Furthermore, Al Shamsi [54] supported the effectiveness of cybersecurity awareness programs in educating young children. Children may face different kinds of danger while using the Internet and are thus especially vulnerable to cyberattacks. In this regard, cybersecurity awareness programs help educate children about online safety [54]. A study investigating cybersecurity programs offered to children in the UAE found these programs extremely effective. All children that participated in the program vouched for its effectiveness and agreed that it influenced their online behavior. Therefore, these research findings suggest that security awareness programs are efficacious interventions that can reduce cybercrimes in the GCC countries.

2) TOWARDS A UBIQUITOUS CYBERSECURITY POLICY

Given the effectiveness of these interventions, there are several procedures that policymakers can take to address cybercrime in the region. For instance, governments can significantly reduce cyber risks by focusing on various ethical issues in cybersecurity and using a stakeholder theory approach. According to stakeholder theory, an organization's fiduciary duty is to create value for all its stakeholders, typically classified as suppliers, financiers, communities, customers, and employees [55]. In the case of cybersecurity, the list of stakeholders also includes governments, Internet users, and law enforcement agencies. In other words, these stakeholders must work together and harmonize their interests by removing or reducing any competing trade-offs. The current literature offers strong recommendations on policymakers' steps to address cybercrime in the GCC countries. A literature review suggests several guidelines that governments can enact to reduce cybercrimes and address these multi-stakeholder issues, from capacity-building to promoting a cybersecurity culture. Therefore, this section will discuss the most effective initiatives that policymakers can implement to minimize the likelihood of cybercrimes in the region.

a: CAPACITY-BUILDING

To start with, one of the most successful initiatives that can be implemented to address cyber threats is capacity-building. According to Aboul-Enein [42], capacity-building regularly tests national cybersecurity capabilities to pinpoint weaknesses and develop mitigation plans. It consists of promoting cybersecurity as a vital component of the state, private sector, and citizens' decision-making. Aboul-Enein [42] suggested that capacity-building is an important initiative that can be used to alleviate the risks posed by cybercrimes. On a similar note, Tohme et al. concurred that capacity-building should be a part of the GCC countries' strategic plan to combat cybercrimes. The government should take the lead in developing preventive and reactive national cyber-security capabilities to prevent cybercrimes in the region. For instance, this may include developing national cyber-security standards and policies such as the national information assurance standard (Tohme et al.). Building capacity through protective behaviour training can also reduce cybersecurity risks significantly [57]. Finally, Al-Alawi et al. [58] contended that cyber defense capacity building should be a top priority for GCC region governments. In a literature review, these researchers suggest that developing the ability to adapt cyber defense resources is essential to responding to cybercrimes [58]. To mitigate the dangers posed by cybercrimes, regional states must remain committed to making capacity-building a national priority. In this regard, these research findings suggest that capacity-building is a practical initiative that policymakers can employ to address cybercrime in the GCC region.

b: PROMOTING CYBERSECURITY CULTURE

Another cost-effective approach that policymakers can take to combat cybercrime in the region is promoting a culture of cybersecurity. Given the rapid rate at which cyber warfare has grown in the GCC countries, fostering a global culture

of cybersecurity is an essential step for policymakers. This procedure would entail three steps: creating awareness of the dangers posed by cybercrimes, tightening information management systems to safeguard information security, and integrating cybersecurity needs into education programs [42]. To create a culture of cybersecurity, it is crucial to raise awareness of cybercrimes. In the wake of imminent cybersecurity risks, researchers have investigated precautionary cybersecurity measures, such as a preventive cybersecurity protocol and an identifiable anonymity protocol [59]. These tools enhance defensive cybersecurity infrastructure.

Moreover, Al Neaimi et al. [60] stressed the importance of creating culturally sensitive training and awareness programs. In a study investigating cyber defenses in the UAE, these researchers found a lack of awareness of cybersecurity issues to be the greatest danger facing organizations [60]. In light of these findings, the researchers proposed a framework for cyber defenses that incorporates user training and awareness programs. By implementing these programs, policymakers could ensure a strong cybersecurity defense in the UAE. Finally, Alnuaimi further supported culturally sensitive training and awareness programs. In a study that evaluated cybersecurity effectiveness in Abu Dhabi, Alnuaimi found training/awareness programs integral to combating cybercrime. The multicultural nature of the GCC countries necessitates culturally appropriate training and awareness programs to combat cybercrime (Alnuaimi). Therefore, Alunaimi advised that governments need to play an active role in instituting a cybersecurity culture among citizens through training and awareness, culturally sensitive policies, and education. By cultivating a cybersecurity culture, policymakers would go a long way in preventing cybercrime in the GCC region.

c: CYBERSECURITY LEGISLATION

The final aspect of cybersecurity policy that merits research attention is legislation. As discussed in section 4.2.3, one of the major factors contributing to cybercrimes in the region is poor laws and regulations. Thus, Hakmeh [62] argued that there is a critical need for GCC countries' governments to update their anti-cybercrime laws. Governments can accomplish this endeavor by training the judiciary and law enforcement agencies, pioneering public-private partnerships, and revisiting cybercrime legal frameworks [62]. In this regard, legislative frameworks can assist policymakers in combating cybercrimes.

Furthermore, Finckenstein [63] concurred that there is a need for cybercrime laws in the region. While a few GCC countries have updated their cybercrime laws from 2011 onwards, these laws lack the mechanisms to tackle actual cybercrime [63]. Finckenstein [63] proposed that countries in the region could orient themselves toward several existing conventions to solve this issue. For instance, the Budapest Convention on Cybercrime could assist GCC countries tremendously by putting them on the appropriate path of legislation and harmonizing cybercrime laws. Finally, Alshammari and Singh [64] contended that countries in the region need to strengthen their anti-cybercrime laws. In a study investigating Saudi Arabia's preparedness to defend against cyber-crimes, these researchers found that the country was only semi-prepared [64]. Although Saudi Arabia formed the anti-cybercrimes law in 2007, it was deficient in protecting against identity theft, invasion of privacy, and cyber-bullying. To become one of the leading nations in cybersecurity, Alshammari and Singh [64] proposed that Saudi Arabia needs to strengthen its anti-cybercrime law and regulations. Ultimately, these recommendations on legislation can tremendously assist policymakers in their crusade to eradicate cybercrimes in the UAE and other GCC regions.

VI. CONCLUDING REMARKS

In this paper, we argue that due to diversity in cultures, socio-technical systems, human factors, and risk awareness levels, governments worldwide struggle to fully mitigate cyber risks. We investigated various human factors and cybersecurity behaviour in two distinct regions, such as the UAE and the USA, and compared them. We provided an extensive overview of cybersecurity awareness in particularly young, educated, and technology-savvy populations of the UAE compared to the USA. Based on the findings presented, it is reasonable to conclude that the UAE population differs in awareness of cybersecurity risks compared to their counterparts in the USA. Whether it is due to education, the internet gender gap, or cultural factors, the UAE citizens lack a comprehensive understanding of cybersecurity. Drawing a comprehensive comparison between the UAE and USA targeted populations enabled us to identify major cybersecurity concerns in the GCC region. Our paper's key contributions are providing evidence-based information for cybersecurity policymakers in the UAE and other GCC countries to further enhance cyber safety, awareness, and trust among citizens. In light of these findings, several training and intervention programs can raise cybersecurity awareness in the region. In regard to developing an effective strategy, policymakers can combat cybercrimes through capacity-building, promoting a culture of cybersecurity, and reforming legislation. Hopefully, these pertinent research findings will incentivize states in the region to take immediate action and raise awareness of cybersecurity.

VII. LIMITATIONS AND FUTUTRE WORK

This paper attempted to develop a survey instrument that captures the main differences between the UAE and the USA. Although the sample from both groups (the UAE and the USA) was large enough to run adequate statistical analyses, it was mostly limited to university students, young, educated, and technology savvy, limiting generalization to a more general population. In the future, we will continue this study to include more regions and countries and gather responses from a more generalized population. Furthermore, we will continue to develop a robust measurement scale that accurately captures the cybersecurity awareness level of people

from different cultures and origins. We plan to exhibit the best approaches to guide a comprehensive policy on ethics and privacy issues in cybersecurity globally through evidence.

REFERENCES

[1] C. Leuprecht, D. B. Skillicorn, and V. E. Tait, "Beyond the castle model of cyber-risk and cyber-security," *Government Inf. Quart.*, vol. 33, no. 2, pp. 250–257, Apr. 2016.

[2] G. Markowsky and L. Markowsky, "Using the castle metaphor to communicate basic concepts in cybersecurity education," in *Proc. Int. Conf. Secur. Manag. (SAM)*, 2011, p. 1.

[3] J. H. Schannep, J. C. Doukas, S. C. Song, E. Y. Wong, and J. M. Comstock Jr., "Advancing cybersecurity from medieval castles to strategic deterrence: A systems approach to cybersecurity," in *Proc. Int. Annu. Conf. Amer. Soc. Eng. Manag.*, 2018, pp. 1–10.

[4] B. von Solms and R. von Solms, "Cybersecurity and information security—What goes where?" *Inf. Comput. Secur.*, vol. 26, no. 1, pp. 2–9, Mar. 2018.

[5] H.-W. Wang, S.-Y. Kuo, and L.-B. Chen, "Exploring the relationship between internal information security, response cost, and security intention in container shipping," *Appl. Sci.*, vol. 11, no. 6, p. 2609, Mar. 2021.

[6] H. Berkman, J. Jona, G. Lee, and N. Soderstrom, "Cybersecurity awareness and market valuations," *J. Accounting Public Policy*, vol. 37, no. 6, pp. 508–526, Nov. 2018.

[7] M. N. El-Guindy, "Cybercrime in the Middle East," *ISSA J.*, vol. 6, no. 6, pp. 16–19, 2008.

[8] M. U. Shah, U. Rehman, F. Iqbal, and H. Ilahi, "Exploring the human factors in moral dilemmas of autonomous vehicles," *Pers. Ubiquitous Comput.*, vol. 26, no. 5, pp. 1321–1331, Oct. 2022, doi: 10.1007/s00779-022-01685-x.

[9] H. de Bruijn and M. Janssen, "Building cybersecurity awareness: The need for evidence-based framing strategies," *Government Inf. Quart.*, vol. 34, no. 1, pp. 1–7, Jan. 2017.

[10] L. Hadlington, "Human factors in cybersecurity; examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours," *Heliyon*, vol. 3, no. 7, Jul. 2017, Art. no. e00346.

[11] P. Ifinedo, "End user nonmalicious, counterproductive computer security behaviors: Concept, development, and validation of an instrument," *Secur. Privacy*, vol. 2, no. 3, p. e66, May 2019.

[12] T. Haig. (Aug. 17, 2020). Canada Revenue Agency suspends online services following cyber attacks. Radio Canada International. Accessed: Aug. 17, 2020. [Online]. Available: https://www.rcinet.ca/en/2020/08/17/canada-revenue-agency-suspends-online-services-after-cyber-attacks/

[13] C. Kelly. (Aug. 5, 2020). IBM cyber breaches cost enterprises in the UAE and KSA over 65M per attack in 2020. ITP. Accessed: Aug. 17, 2020. [Online]. Available: https://www.itp.net/news/93473-ibm-cyber-breaches-cost-enterprises-in-the-uae-and-ksa-over-65m-per-attack-in-2020

[14] M. Silic and P. B. Lowry, "Breaking bad in cyberspace: Understanding why and how black hat hackers manage their nerves to commit their virtual crimes," *Inf. Systems Frontiers*, vol. 23, pp. 329–341, 2021, doi: 10.1007/s10796-019-09949-3.

[15] N. H. A. Rahim, S. Hamid, M. L. M. Kiah, S. Shamshirband, and S. Furnell, "A systematic review of approaches to assessing cybersecurity awareness," *Kybernetes*, vol. 44, no. 4, pp. 606–622, Apr. 2015.

[16] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, "The human aspects of information security questionnaire (HAIS-Q): Two further validation studies," *Comput. Secur.*, vol. 66, pp. 40–51, May 2017.

[17] E. Kweon, H. Lee, S. Chai, and K. Yoo, "The utility of information security training and education on cybersecurity incidents: An empirical evidence," *Inf. Syst. Frontiers*, vol. 23, pp. 361–373, Dec. 2019.

[18] F. A. Al-Khalifa, F. G. Kohun, and R. J. Skovira, "A discussion about culture and information security policy compliance: A sub-culturally bound determinant—Redefining the Hofstede hypothesis," *Issues Inf. Syst.*, vol. 16, no. 4, pp. 202–208, 2015.

[19] N. Ameen, A. Tarhini, M. H. Shah, and N. O. Madichie, "Employees' behavioural intention to smartphone security: A gender-based, cross-national study," *Comput. Hum. Behav.*, vol. 104, Mar. 2020, Art. no. 106184.

[20] M. L. Jones and I. Alony, "The cultural impact of information systems—Through the eyes of Hofstede—a critical journey," 2007.

[21] M. A. Chadhar and N. Rahmati, "Impact of national culture on ERP systems success," in *Proc. 2nd Austral. Undergraduate Students' Comput. Conf.* Melbourne, VIC, Australia: RMIT Univ., 2004, p. 23.

[22] (2021). *Hofstede Insights*. Accessed: Mar. 31, 2021. [Online]. Available: https://www.hofstede-insights.com/country-comparison/saudi-arabia/

[23] D. P. Ford, C. E. Connelly, and D. B. Meister, "Information systems research and Hofstede's culture's consequences: An uneasy and incomplete partnership," *IEEE Trans. Eng. Manag.*, vol. 50, no. 1, pp. 8–25, Feb. 2003.

[24] M. Alnatheer and K. Nelson, "Proposed framework for understanding information security culture and practices in the Saudi context," in *Proc. 7th Austral. Inf. Secur. Manag. Conf.*, 2009, pp. 6–17.

[25] A. Onumo, A. Cullen, and I. Ullah-Awan, "An empirical study of cultural dimensions and cybersecurity development," in *Proc. IEEE 5th Int. Conf. Future Internet Things Cloud (FiCloud)*, Prague, Czech Republic, Aug. 2017, pp. 70–76.

[26] N. Ameen, A. Tarhini, M. H. Shah, N. Madichie, J. Paul, and J. Choudrie, "Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the gen-mobile workforce," *Comput. Hum. Behav.*, vol. 114, Jan. 2021, Art. no. 106531.

[27] D. Shin, V. Chotiyaputta, and B. Zaid, "The effects of cultural dimensions on algorithmic news: How do cultural value orientations affect how people perceive algorithms?" *Comput. Hum. Behav.*, vol. 126, Jan. 2022, Art. no. 107007.

[28] A. Alamri, A. Cristea, and M. Al-Zaidi, "Saudi Arabian cultural factors and personalized e-learning," in *Proc. 6th Int. Conf. Educ. New Learn. Technol. (EDULEARN)*. Barcelona, Spain, 2014, pp. 1–9.

[29] H. Alqahtani and M. Kavakli-Thorne, "Factors affecting acceptance of a mobile augmented reality application for cybersecurity awareness," in *Proc. 4th Int. Conf. Virtual Augmented Reality Simulations*, Sydney, NSW, Australia, Feb. 2020, pp. 18–26.

[30] D. E. Patton, "Evaluating U.S. and Chinese cyber security strategies within a cultural framework," Doctoral dissertation, Air Command Staff College, Air Univ., Montgomery, AL, USA, 2016.

[31] F. Zhao and M. S. Khan, "An empirical study of e-government service adoption: Culture and behavioral intention," *Int. J. Public Admin.*, vol. 36, no. 10, pp. 710–722, Aug. 2013.

[32] F. Faul, E. Erdfelder, A. G. Lang, and A. Buchner, "G* power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences," *Behav. Res. Methods*, vol. 39, no. 2, pp. 175–191, 2007.

[33] (2020). *GTCI—Global Talent Competitiveness Index*. Accessed: Apr. 21, 2021. [Online]. Available: https://gtcistudy.com

[34] (2020). *Global Innovation Index*. Accessed: Apr. 21, 2021. [Online]. Available: https://www.globalinnovationindex.org/Home

[35] S. Al-Janabi and I. Al-Shourbaji, "A study of cyber security awareness in educational environment in the Middle East," *J. Inf. Knowl. Manag.*, vol. 15, no. 1, pp. 1–30, 2016.

[36] F. Aloul, "The need for effective information security awareness," *Int. J. Intell. Comput. Res.*, vol. 2, no. 1, pp. 116–123, Mar. 2011.

[37] F. A. Aloul, "Information security awareness in UAE: A survey paper," in *Proc. Int. Conf. Internet Technol. Secured Trans.*, London, U.K., Nov. 2010, pp. 1–6.

[38] F. F. Alotaibi, "Evaluation and enhancement of public cyber security awareness," Ph.D. dissertation, Dept. Sci. Eng., Univ. Plymouth, Plymouth, U.K., 2019.

[39] M. N. El-Guindy and F. Hegazy, "Cybercrime legislation in the Middle East: The road not travelled," *ISSA J.*, vol. 27, pp. 1–32, Feb. 2012.

[40] S. Al Amro, "Cybercrime and its impact on e-government services and the private sector in the Middle East," *Int. J. Comput. Sci. Inf. Secur.*, vol. 14, no. 3, pp. 69–73, 2016.

[41] R. K. Alqurashi, M. A. AlZain, B. Soh, M. Masud, and J. Al-Amri., "Cyber attacks and impacts: A case study in Saudi Arabia," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 9, no. 1, pp. 217–224, Feb. 2020.

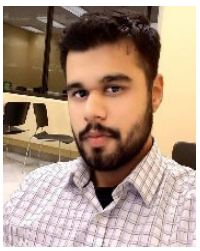
[42] S. Aboul-Enein, "Cybersecurity challenges in the Middle East," Geneva Centre Secur. Policy, Geneva, Switzerland, Tech. Rep. 22, 2017, pp. 1–52.

[43] (2016). *GCIG—Global Commission on Internet Governance*. Accessed: May 2, 2022. [Online]. Available: https://www.cigionline.org/sites/default/files/documents/GCIG%20no.45.pdf

[44] Intel Corporation. (2014). *Women and the Web: Bridging the Internet Gap and Creating New Global Opportunities in Low and Middle-Income Countries*. [Online]. Available: https://www.smefinanceforum.org/post/women-and-the-web-bridging-the-internet-gap-and-creating-new-global-opportunities-in-low-and
[45] M. Anwar, W. He, I. Ash, X. Yuan, L. Li, and L. Xu, "Gender difference and employees' cybersecurity behaviors," *Comput. Hum. Behav.*, vol. 69, pp. 437–443, Apr. 2017.
[46] A. Alzahrani and K. Alomar, "Information security issues and threats in Saudi Arabia: A research survey," *Int. J. Comput. Sci. Issues*, vol. 13, no. 6, pp. 129–135, 2016.
[47] A. ALArifi, H. Tootell, and P. Hyland, "Information security awareness in Saudi Arabia," in *Proc. CONF-IRM*, vol. 57. Vienna, Austria: Association for Information Systems, 2012, pp. 1–11.
[48] D. G. Sofio and W. A. Carter, "Putting U.S. cybersecurity culture in perspective," in *Homeland Security Cultures: Enhancing Values While Fostering Resilience*, A. Siedschlag and A. Jerkovic, Eds., 2018, pp. 103–126.
[49] M. U. Shah and P. D. Guild, "Toward an understanding of firms creating value for stakeholders: Using the repertory grid technique for exploring differences among ICT-sector firms at various organizational life cycle stages," in *Personal Construct Psychology at 60: Past, Present and Future*. Newcastle, U.K.: Cambridge Scholars Publishing, 2017, pp. 359–389.
[50] M. U. Shah and P. D. Guild, "Stakeholder engagement strategy of technology firms: A review and applied view of stakeholder theory," *Technovation*, vol. 114, Jun. 2022, Art. no. 102460.
[51] M. Boujettif and Y. Wang, "Constructivist approach to information security awareness in the Middle East," in *Proc. Int. Conf. Broadband, Wireless Comput., Commun. Appl.* IEEE, Nov. 2010, pp. 192–199.
[52] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness," *MIS Quart.*, vol. 34, no. 3, pp. 523–548, 2010, doi: 10.2307/25750690.
[53] M. Eyadat, "Information security: Awareness and training program in the Middle East universities," *Asian J. Comput. Inf. Syst.*, vol. 6, no. 5, pp. 38–44, Oct. 2018.
[54] A. A. Al Shamsi, "Effectiveness of cyber security awareness program for young children: A case study in UAE," *Int. J. Inf. Technol. Lang. Stud.*, vol. 3, no. 2, pp. 8–29, 2019.
[55] R. E. Freeman, *Strategic Management: A Stakeholder Approach*. Cambridge, U.K.: Cambridge Univ. Press, 2010.
[56] E. Tohme, J. Lindeyer, I. Harb, and S. Papazian. (2017). Cybersecurity in the Middle East: A strategic approach to protecting national digital assets and infrastructure. Strategy&. [Online]. Available: https://www.strategyand.pwc.com/m1/en/reports/cyber-security-middle-east.html
[57] A. R. Gillam and W. T. Foster, "Factors affecting risky cybersecurity behaviors by U.S. workers: An exploratory study," *Comput. Hum. Behav.*, vol. 108, Jul. 2020, Art. no. 106319.
[58] A. I. Al-Alawi, S. Al-Bassam, and A. A. Mehrotra, "Critical cybersecurity threats: Frontline issues faced by bahraini organizations," in *Implementing Computational Intelligence Techniques for Security Systems Design*, Y. A. Albastaki and W. Awad, Eds. Hershey, PA, USA: IGI Global, 2020, pp. 210–229.
[59] J. K. Lee, Y. Chang, H. Y. Kwon, and B. Kim, "Reconciliation of privacy with preventive cybersecurity: The bright internet approach," *Inf. Syst. Frontiers*, vol. 22, no. 1, pp. 45–57, Feb. 2020.
[60] A. Al Neaimi, "A framework for effectiveness of cyber security defenses, a case of the United Arab Emirates (UAE)," *Int. J. Cyber-Secur. Digit. Forensics*, vol. 4, no. 1, pp. 290–301, 2015.
[61] A. R. Alunaimi, "A framework for the evaluation of cybersecurity effectiveness of Abu Dhabi government ethics," Ph.D. dissertation, Bus. Admin., United Arab Emirates Univ., Al Ain, United Arab Emirates, 2017.
[62] J. Hakmeh, "Cybercrime legislation in the GCC countries: Fit for purpose?" Chatham House, London, U.K., 2018.
[63] V. V. Finckenstein. (2019). Cybersecurity in the Middle East and North Africa. Konrad Adenauer Stiftung. Accessed: Dec. 23, 2020. [Online]. Available: https://www.kas.de/documents/284382/284431/Policy+Paper+on+Cybersecurity+in+the+Middle+East+and+North+Africa.pdf/50199440-b10e-3dea-52ca-c0e3714ebc75?version=1.0&t=1564581818218
[64] T. S. Alshammari and H. P. Singh, "Preparedness of Saudi Arabia to defend against cyber crimes: An assessment with reference to anti-cyber crime law and GCI index," *Arch. Bus. Res.*, vol. 6, no. 12, pp. 131–146, Dec. 2018.

MUHAMMAD UMAIR SHAH received the M.A.Sc. and Ph.D. degrees in management of technology from the University of Waterloo, ON, Canada. He is currently a Lecturer with the Department of Management Sciences, Faculty of Engineering, University of Waterloo. Among other avenues, he has published research in *Journal of Business Ethics*, *Technovation*, *Journal of Cleaner Production*, *Personal and Ubiquitous Computing*, and IEEE Access. He actively pursues research, teaching, and industry consultation in these areas, such as stakeholder theory, management of technological innovation, human–computer interaction, design research, detection of cybercrimes, and technology ethics.

FARKHUND IQBAL (Member, IEEE) received the master's and Ph.D. degrees from Concordia University, Canada, in 2005 and 2011, respectively. He is an Associate Professor with the College of Technological Innovation, Zayed University, United Arab Emirates, where he is also the Team Lead of the Cybersecurity and Digital Forensics (CAD) Research Group, Center for Smart Cities and Intelligent Systems. He is also an Adjunct Professor with the School of Information Studies, McGill University, Canada, and an Associate Graduate Faculty Member with the Faculty of Business and IT, Ontario Tech University, Canada. He has more than 15 years of teaching and research experience. He is using artificial intelligence, machine learning, service robotics, and data analytics techniques, for problem-solving in digital security, digital forensics, healthcare, cybercrime investigation, and smart city domains.



UMAIR REHMAN received the M.A.Sc. and Ph.D. degrees in systems design engineering from the University of Waterloo. He is currently as Assistant Professor with the Department of Computer Science, Western University. He works in the areas of information systems, human–computer interaction, and cognitive engineering. The crux of his work revolves around understanding, modeling, and predicting human performance and behavior in complex sociotechnical systems. He has published research in a diverse range of domains, including transportation and navigation, process control, digital games, and social media.

PATRICK C. K. HUNG (Member, IEEE) received the bachelor's degree in computer science from The University of New South Wales, Australia, the first master's degree in management sciences from the University of Waterloo, Canada, and the second master's and Ph.D. degrees in computer science from the Hong Kong University of Science and Technology. He is a Professor, the Graduate Program Director of computer science, and the Director of international programs with the Faculty of Business and Information Technology, Ontario Tech University, Canada. He is an Honorable Guest Professor with Shizuoka University, Hamamatsu, Japan. He was a Distinguished Visiting Fellow with Abertay University, Scotland, and a Visiting Researcher with the University of São Paulo, Brazil. He was with Boeing Research and Technology, Seattle, on aviation services-related research with two U.S. patents on the mobile network dynamic workflow systems. Before that, he was a Research Scientist with the Australia's Commonwealth Scientific and Industrial Research Organization. He is a Founding Member of the IEEE Technical Committee on Services Computing and IEEE Transactions on Services Computing. In addition, he is an Editorial Board Member of the IEEE Transactions on Engineering Management and a Coordinating Editor of the *Information Systems Frontiers*.