Statistical Analysis of Cybersecurity Awareness Issues in Higher Education Institutes

Latifa Alzahrani
Department of Management Information Systems
College of Business Administration, Taif University, Saudi Arabia

***Abstract*—Now-a-days, computers and the Internet are becoming increasingly indispensable tools in several aspects of our lives, including academic study, professional work, entertainment, and communication. Despite the significant advantages of information technology, particularly in information accessibility and internet applications, cyber security has risen to become a national concern in Saudi Arabia, and cyber security threats now need to be taken more seriously. Therefore, computer and network security are a concern not only for traditional security awareness organisations, for example, military, bank, or financial institutions, but also for every individual and government official who use computers. Besides, nowadays, more and more organisations' valuable assets are stored in the computerised information system; security has become an essential and urgent issue. However, it is remarkable that most systems today are designed with little attention to security concerns. This study aims to examine and analyse cyber security issues, including cyber risk, cyber security, cyber security awareness, and cyber trust, among higher education students in Saudi Arabia. Based on an analysis of the collected data using SPSS, the findings of this study highlight a lack of awareness of basic information related to cyber security among Saudi students. In addition, the number of students attending training programs was very low. Considering other security issues, this study reveals that while Saudi students are aware of cyber risk, they are not aware of cyber security. In addition, Saudi students are not aware of and do not have cyber trust.**

Keywords*—*Cyber security; cyber security awareness; educational institutes; cyber risk; higher education; cyber trust

I. Introduction

The persistent threats from cyber attackers are a real danger, so much so that they rise to the level of a national security concern. Cybersecurity breaches are an all too common occurrence; seemingly every day, a new attack, data theft or other intrusion makes the news [1]. The U.S. Cyber Command protects Department of Defense networks and works to guard other federal agencies against malicious activity; the FBI, Secret Service, and Department of Homeland Security are among the agencies that investigate cybercrimes. But it is still up to the private industry to secure its networks. According to Internet World Stats 2017, the Internet users in Asia accounted for approximately half of Internet users worldwide. However, they are still immature with cybersecurity, exercises or cooperation to counter cyber incidents or cyber-attacks [2]. In fact, in 2016, hackers attacked some Asian countries by withdrawing US$81 million from the Bangladesh Central bank, accessing and leaking details of 3.2 million customer cards from several Indian banks, stealing US$65 million of bitcoins from Hong Kong-based digital currency exchange Bifinex, using malware to steal US$2.17 million from eight banks in Taiwan. In 2017, a remarkable attack in Korea was recorded, indicating that seven main banks were threatened by distributed denial of service attacks claiming ransom payment [3].

The security and privacy of cyber and cyber-physical systems are increasingly considered a major issue in many industries [4, 5]. Cyber security has become a national concern in Saudi Arabia because of worrying threats to be taken more seriously [6-9]. However, many users are still not knowledgeable about the online threats; therefore, they do not have an effective awareness of secure behaviour online. A recent study by McPhee and Weiss [10] highlights that lack of knowledge is an important factor that contributes to insecure online behaviour by Internet users. Awareness and education can provide Internet users with the ability to recognise and avoid any apparent risks [11-13]. Currently, there is a growing concern about cyber threats, the most dangerous ones worldwide. They can cause huge damage to finance, the economy, politics, and other aspects of life [10]. As a result, identifying types of cyber threats is a critical and urgent need not only for individuals and businesses but also for governments and organisations to increase awareness of cybersecurity and national security and find solutions to mitigate or reduce the damage from them [3]. Moreover, it was expected to figure out the differences in security cooperation among Asian nations to identify which model is suitable for small nations, including Saudi Arabia and its neighbours in the Asian region [2].

In the past, cyber-crime was considered with two major categories: computer as a target of the attack and computer as a means of attack. Firstly, the computer as a target of the attack - the attackers use some special tools to get unauthorised access and illegally manipulate the confidentiality, integrity, and availability of data—secondly, traditional offences with the assistance of computers, computer networks, and communication technology. For example, the blackmailers use the computer to spread a thousand blackmails or spam messages to the victim computers [7]. Moreover, cybercrime offences have also ranged from economic offences like fraud, theft, terrorism, extortion, etc. On the other hand, cybercrime includes some non-money offence activities such as programming viruses, spam, and spyware on the computer network or posting confidential business information on the Internet [10]. The current cybercrimes are no different from traditional criminals because they want to make money as fast

as possible. However, the current computer crimes are more sophisticated than the old ones with many forms on the Internet like child pornography, copyright or trademark infringement, money laundering, cyberbullying, online gambling, etc. As a result, cybercrime is currently separated into two main categories: machine-made attacks and man-made attacks [4, 9]. Machine-made attack defines some cyber-attacks by using computer network environment as a tool to exploit illegal sensitive data and sabotage them, especially in financial damage.

In contrast, a man-made attack is considered a cyber-terrorist attack by an individual or group of people with the purpose of politics and military [14]. In Europe, each country has different strategies to ensure its national security, especially cybersecurity. As each country has its contexts, strengths, technology development, and policies, it may be not easy to cooperate and operate the same strategy [8]. The results of this research are very important for Saudi Arabia because the study was conducted there on a certain sample of students in higher education. In Saudi Arabia, cyber-attacks are increasing due to the rise in digital devices (computers, tablets, and smartphones), lack of security awareness among Internet users, terrorism, politics, and an increase in cybercrime groups [15] . While Saudi organisations continue to protect computer systems and their information against cybercrimes, a recent report from Kaspersky Lab highlights that Saudi Arabia has one of the highest numbers of Web threat incidents [7, 16]. Consequently, this study first presents the level of awareness of cyber security in Saudi Arabia. It then proposes strategies to increase awareness and training on cyber security in line with Saudi Vision 2030 [17, 18]. Preliminary research has shown that studies on cyber security in Saudi Arabia are very few, and further research is needed in this area. These results will also be of great importance to all managers and decision-makers in the fields of information security and cyber security because it provides a clear and comprehensive picture of the concept of CSA from the field of higher education. This paper aims to investigate and analyse CSA levels among higher education students in a business college in Saudi Arabia. It also aims to examine students' knowledge and attitude towards the following major security issues related to cyber security: cyber risk, cyber security, cyber awareness and cyber trust.

Section II reviews the literature on cyber security, cyber threats, cybercrimes, cyber-attacks, and the like. Moreover, it clarified the differences between cybercrime and cyberwar to consider the new trends of cyber security and cyber threats. Furthermore, it primarily expressed an urgent need for Saudi Arabia cybersecurity strategies toward the new cybersecurity trends in the world. Section III explains the methodology of our study in which the dataset, tool, and workflow has been explained. Section IV presents the results through five analysis tools: the frequency distribution of variables, multiple response analysis, factor analysis for grouping different types of security, a reliability test, and descriptive analysis. Section V presents the discussion that provides a deeper understanding of students' awareness and their basic understanding of cyber security issues. Section VI provides some significant implications for research, and Section VII explains the summary of research findings, proposed method, and contributions to the research problem.

II. Related Work

Cyber security has been defined as “the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that could be used for protecting the cyber environment and organisation and user’s assets” [19]. Individuals and families and organisations, governments, educational institutions, and businesses are now concerned about cyber security. Kritzing and Von Solms [14] studied that cyber security is critical for families and parents to safeguard children and family members from online fraud. In terms of financial security, it's critical to safeguard financial information that might impact one's financial situation. As a result, understanding how to protect oneself against online fraud and identity theft is critical for Internet users. Kim [4] concluded that even though technology has done a lot to safeguard end-users information systems, security experts claim that technology alone cannot protect these systems adequately. Appropriate learning about online behaviour and system security decreases vulnerabilities and makes the Internet a safer place to be. Because of limited resources and a lack of sufficient cyber security expertise, small and medium-sized businesses face a variety of security difficulties [8, 14, 20]. Because the continual advancement of technology makes cyber security increasingly difficult, we do not offer lasting answers to this troubling situation. Nonetheless, we're attempting to provide a variety of frameworks or solutions to safeguard our networks and data. All of these measures, however, only give protection in the near run. Better security knowledge and methods may aid in the protection of intellectual property and trade secrets, as well as the reduction of financial and reputational harm [14, 21]. Large volumes of data and private documents are held digitally by the federal, state, and municipal governments, making them prime targets for a cyber-assault [8, 22]. Governments are frequently exposed to dangers due to low financing, inadequate infrastructure, and a lack of knowledge. Government agencies must offer dependable services to society, maintain good citizen-to-government contacts, and safeguard sensitive information [20, 21, 23].

With around 26 million inhabitants, Saudi Arabia is one of the largest countries in the Middle East. About 0.002% of Internet users are from Saudi Arabia [7, 24]. However, the number of cyberattacks experienced by Saudi Arabian users are far larger than the population of Internet users, i.e., 1.81% in 2009 and 1.77% in 2010 [25, 26]. Although Saudi Arabia is as highly censored as Iran, and the number of Internet users in Iran is also higher than in Saudi Arabia, the number of cyber-attacks is greater in Saudi Arabia than in Iran. Saudi Arabia is reported to be the ninth largest country in 2008 in terms of cyber-attacks and the incidence of information security attacks. It became the seventh-largest in 2009. The reasons behind such a larger number of attacks are a lack of CSA among the general public of Saudi Arabia. Alzahrani and Alomar [7] has revealed that information security awareness is very low, and there is a higher level of risk related to cyberspace in Saudi Arabia.

TABLE I. DIFFERENT CATEGORIES OF CYBER-CRIME [22]

Category	Definition
Hacking	The destruction and concealment of information from the victim's operating system by attacking the weaknesses and loopholes are known as hacking. It is usually done by installing some sort of backdoor programs by hackers on the computer of victims to obtain access to the information.
Cyber theft	When the victim's computer information is stolen through electronic attacks, this is known as cyber theft. The most common example of cyber theft is credit card fraud and illegal money transfers.
Viruses and worms	Viruses and worms are designed to damage the computers attached to other programs and documents in the computer. They appear to perform some other function, but the primary function of the virus is to corrupt the operating system of the computer.
Spamming	Spamming is done by sending massive numbers of emails to users that usually contain links designed to harm the programs of the victim's computer.
Financial fraud	This cybercrime is also known as a phishing scam, formed through social engineering and designed to obtain the victim's bank details.
Identity theft and credit card theft	In this cybercrime, emails are sent to users to induce them to provide their identity card and credit card information. The attacker represents him or herself as a representative of some well-known company, and hence unaware users provide their sensitive details by responding to these emails.
Cyber harassment	Cyber harassment is harassing and bullying individuals using electronic means; one such example is cyberstalking.
Cyber laundering	The transfer of illegally obtained money between two parties is known as cyber laundering.
Website cloning	Copying the websites of renowned companies and attacking the users who are unaware of this is a new category of cybercrime. Unaware consumers provide their details to the fraudster's personal database.

According to a report in 2016, the number of Internet users in Saudi Arabia has reached 22.4 million. These users belong to different sectors such as health, education, government, and other service sectors. However, with the growth of digital devices, the rate of cyber-attacks in Saudi Arabia also increases more quickly. To tackle this increasing problem, the CSA of the general public should be improved, and the government of Saudi Arabia is now taking practical steps to counter these problems. The report suggests that around 40% of companies in Saudi Arabia were the victim of cyber-attacks in 2015, leading to the leakage of the confidential data of Saudi employees. The primary step that the Saudi government could take to reduce the number of cyber-attacks is to increase CSA and educate children and young people about anti-cybercrime laws [14] [7] [27]. Very recent reports about the CSA level in Saudi Arabia have suggested that the government has yet taken no practical measures to respond to the issues of cyber-attacks. As a result, a large number of attacks have been experienced. Table I presents the different categories of cyber-crime.

III. METHODOLOGY

This study used a quantitative research technique to emphasise the relation between students' cyber security awareness and their cyber security practices. Quantitative research designs are either descriptive (in which subjects are generally measured just once) or experimental (subjects are measured many times). A relationship between variables is established in a descriptive investigation; causation is established in an experimental study. According to Quantitative Methods, objective measurements and statistical, mathematical, or numerical analysis of data collected through polls, questionnaires, and surveys, or by manipulating pre-existing statistical data using computational techniques, are the most important aspects of quantitative methods [28, 29]. Quantitative research collects statistical information and the generalisation or description of phenomena across groups of individuals. A pilot study was carried out for the questionnaire.

The pilot study aimed to test the understandability of the questionnaire before it was presented to the sampling frame of this study [30] [28] [31]. To analyse the collected data, SPSS was utilised to measure students' awareness about cyber security. With a wide range of graphs, methods and charts, SPSS provides many types of statistical analysis for quantitative research. The techniques of screening and cleaning data within SPSS are useful for future analysis. Because the issue of cyber security is an important topic in Saudi Vision 2030, this study was conducted in Saudi Arabia. Cyber security in Saudi Arabia still faces many challenges that need to be addressed. The sample selected for this study comprises Saudi students in a business college in a Saudi university. Questionnaires were distributed by both an online link and in hard copy to Saudi students. The online link was sent to students' emails, while hard copies of the questionnaire were distributed in classrooms. Table II lists the questionnaire items used in this study.

TABLE II. QUESTIONNAIRE ITEMS

I usually change my password.
I use different passwords for different systems.
I usually change the default password of the administrator account.
I use wireless encryption.
I keep the wireless device firmware up to date.
I share my personal information on social networks.
I trust the applications in social networks.
I check links before clicking on them on social networks.
I share my files, documents, and photo online.
I set a password to access shared files.
I read about the security and privacy policies of services providers.
I understand the risk of emailing passwords.
I understand the risk of email attachments.
I understand the risk of clicking on email links.
I understand the risk of smartphone viruses.
I have an anti-virus program for my smartphone.

IV. Results

To achieve the objectives of this research given the nature of the data collected, five analysis tools were utilised: the frequency distribution of variables, multiple response analysis, factor analysis for grouping different types of security, a reliability test, and descriptive analysis. The following paragraphs provide more details for each tool. Table III shows the demographics of the survey participants, revealing that the majority of respondents were 18–30 years old (94.5 percent) or 31–40 years old (4.7 percent). Overall, most respondents were between the ages of 18 and 30, indicating that a younger generation was more engaged in this study. Table III shows that the female population (52.0%) was somewhat greater than the male population (50.0%). (48.0 percent). In terms of educational attainment, the biggest cohort (96.2 percent) had a bachelor's degree, followed by a master's degree (96.2 percent) (3.8 percent). Finally, 46.5 percent of participants had 6–10 years of experience using the Internet, followed by 26.3 percent with 1–5 years of experience, and 15.3 percent with 11–20 years of experience.

The results in Table IV show that 82.5% of students do not know what cyber security means. The results in Table V also show that 97.4% of students are not attending any training or educational programs in cyber security.

TABLE III. Respondent Details

Variable	Group	Frequency	Percentage (%)
Age	18–30 years old	518	94.5
	31–40 years old	26	4.7
	41–50 years old	4	0.7
	51–60 years old	0	0
	Total	**548**	**100.0**
Gender	Male	263	48.0
	Female	285	52.0
	Total	**548**	**100.0**
Education level	Bachelor's degree	527	96.2
	Master's degree	21	3.8
	Total	**548**	**100.0**
Internet experience	1–5 years	144	26.3
	6–10 years	255	46.5
	11–20 years	84	15.3
	21–30 years	9	1.6
	None	56	10.2
	Total	**548**	**100.0**

TABLE IV. Results for "Do you Know what Cyber Security means?"

	Frequency	Percent (%)	Valid (%)	Cumulative (%)
Yes	96	17.5	17.5	17.5
No	452	82.5	82.5	100.0
Total	548	100.0	100.0	

Considering the behaviour of maintaining up-to-date protection software, the results (Table VI) show a variation in the participants' responses. Here, 38.1% of the participants automatically update their protection software. However, 40% fail to update their software. In addition, just over 10% annually update their software.

A multiple response analysis was utilised to answer the question, "What types of protection software do you use?" As shown in Table VII, 43.6% of respondents do not know what protection software they are using for protection. In addition, 36.6% of respondents use an anti-virus program for software protection, and 11.5% of respondents use a firewall for software protection. Only 6.4% use anti-spyware software, and 1.9% use anti-spam software.

Table VIII presents the results of Kaiser–Meyer–Olkin (KMO) and Bartlett's tests. The KMO measure of sampling adequacy and Bartlett's test of sphericity were used in this research. KMO must be greater than 0.7 to be considered good. In Table VIII, the value of KMO is 0.795, which indicates that factor analysis is appropriate for these data. In addition, Table IX presents the total variance explained results, where all the variables are grouped into four components with eigenvalues greater than 1.

TABLE V. Results for "Are you Attending any Security Training or Education Programs?"

	Frequency	Percent (%)	Valid (%)	Cumulative (%)
Yes	14	2.6	2.6	2.6
No	534	97.4	97.4	100.0
Total	548	100.0	100.0	

TABLE VI. Results for "How often do you Update Protection Software?"

	Frequency	Percent	Valid Percent	Cumulative Percent
Automatically	209	38.1	38.1	38.1
Weekly	33	6.0	6.0	44.2
Monthly	84	15.3	15.3	59.5
Annually	41	7.5	7.5	67.0
Never	181	33.0	33.0	100.0
Total	548	100.0	100.0	

TABLE VII. Results for "What types of Protection Software do You use?"

	Responses		Percent of Cases (%)
	N	Percent (%)	
Anti-virus	229	36.6	42.1
Firewall	72	11.5	13.2
Anti-spam	12	1.9	2.2
Anti-spyware	40	6.4	7.4
I don't know	273	43.6	50.2
Total	**626**	**100.0**	**115.1**
a. Dichotomy group tabulated at value 1.			

TABLE VIII. Results for KMO and Bartlett's Test

KMO measure of sampling adequacy		.795
Bartlett's test of sphericity	**Approx. chi-square**	1766.468
	Df	136
	Sig.	.000

TABLE IX. TOTAL VARIANCE EXPLAINED RESULTS

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	3.851	22.653	22.653	3.851	22.653	22.653	3.124	18.376	18.376
2	1.859	10.933	33.586	1.859	10.933	33.586	1.819	10.701	29.077
3	1.442	8.483	42.069	1.442	8.483	42.069	1.648	9.693	38.770
4	1.057	6.219	48.288	1.057	6.219	48.288	1.618	9.518	48.288
5	.946	5.563	53.851						
6	.910	5.356	59.206						
7	.848	4.989	64.195						
8	.810	4.764	68.959						
9	.774	4.554	73.513						
10	.731	4.300	77.813						
11	.674	3.966	81.779						
12	.652	3.834	85.613						
13	.615	3.615	89.228						
14	.573	3.368	92.596						
15	.512	3.012	95.608						
16	.461	2.712	98.320						
17	.286	1.680	100.000						
Extraction Method: Principal Component Analysis.									

TABLE X. ROTATED COMPONENT MATRIX

	Component			
	Cyber Risk	Cyber security	Cyber trust	Cyber Awareness
I understand the risk of emailing passwords.	.722			
I understand the risk of email attachments.	.775			
I understand the risk of clicking on email links.	.776			
I understand the risk of smartphone viruses.	.642			
I keep the wireless device firmware up-to-date.	.521			
I check links before clicking on them on social networks	.546			
I usually change my passwords.		.695		
I use different passwords for different systems.		.612		
I usually change the default password of the administrator account.		.643		
I use wireless encryption.		.537		
I share my personal information on social networks.			.743	
I trust the applications in social networks.			.782	
I share my files, documents, and photos online.			.637	
I set passwords to shared access files.				.518
I read about security policies and privacy.				.712
I have an anti-virus program for my smartphone.				.720
Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization.				
a. Rotation converged in five iterations.				

Table X presents the rotated component matrix, which presents the four groups (components) along with their items. As shown in Table X, cyber risk has six items, and cyber security has four items. The reliability of a group of variables is tested with Cronbach's alpha method. If Cronbach's alpha is greater than 0.7, then the data are reliable as shown in Table XI. Both cyber trust and cyber awareness have three items. The results of descriptive statistics (Table XII) show a high cyber risk score with a mean of 3.19 and a lower score for cyber security (mean = 2.01). In addition, both cyber awareness (mean = 2.37), cyber trust (mean = 2.41) have low scores. Overall, the findings of this study highlight a lack of awareness of basic information related to cyber security among Saudi students.

TABLE XI. RELIABILITY STATISTICS

Variables	Cronbach's Alpha	No. of Items
Cyber Risk	.786	6
Cyber Security	.753	4
Cyber Trust	.757	3
Cyber Awareness	.4712	3

TABLE XII. DESCRIPTIVE STATISTICS

	N	Minimum	Maximum	Mean	Std. Deviation
Cyber Risk	548	1.00	5.00	3.1934	1.05231
Cyber Security	548	1.00	5.00	2.0132	.79557
Cyber Trust	548	1.00	5.00	2.4148	.87477
Cyber Awareness	548	1.00	5.00	2.3710	1.01231
Valid N (listwise)	548				

In addition, the number of students attending training programs was very low: 92% have never taken any type of security training. Considering other security issues, this study reveals that while Saudi students are aware of cyber risk, they are not aware of cyber security and the important steps and processes needed to protect their personal information. Thus, Saudi students need to increase their awareness about cyber security to become educated about protecting their online data.

V. DISCUSSION

This study provides a deeper understanding of students' awareness and their basic understanding of cyber security issues. Additionally, this study contributes significantly by investigating students' behaviour about the major topics related to cyber security: the security issues related to passwords, emails, wireless, social networks, and smartphones. SPSS was employed to analyse students' awareness and reveal their behaviour. The following subsections first discuss the results of general information about cyber security and then discuss major topics related to cyber security. Finally, some strategies are recommended to increase student awareness about cyber security. The results of this survey indicate that the participants' level of awareness about cyber security was generally unsatisfactory. A total of 82% of the participants were not aware of cyber security. The results also show that 97% of the participants have not had any related training, which suggests a lack of training programs available to the students.

The knowledge about cyber risks of the participants was very good. Most of the participants from all demographic distributions had a good understanding of the importance of password security rules, had an accurate knowledge of password security, and recognised that passwords should not contain only real words or significant dates or names. There were, however, some aspects of wireless technology about which many students lacked knowledge. An excellent level of participant awareness about social security was recorded. Most of them are aware that they should not share their personal information on social applications. Even though a minority of the participants use cloud storage to save their files, most do not use passwords to secure their data while sharing them. In addition, most of the participants are aware of the risk of using smartphones. However, few of them use anti-virus programs to protect them.

To summarise, this section discussed in-depth Saudi students' awareness of and their behaviour towards cyber security. The study results show that students in higher education need to increase their awareness about cybercrime and cyber security by involving them in training programs, workshops, and lessons. Universities in Saudi Arabia must take on more responsibility in encouraging CSA and practice. Several strategies were recommended for individuals, network users, and organisations to enhance CSA and practice.

Currently, the cyber-threats are very complicated for all countries in general and Saudi Arabia in specific. As a result, the Saudi Arabian government established several decrees and programs to promote cybersecurity awareness and human resources. They gave Decree No. 99/QĐ-TTG and 153/QĐ-TTg to develop human cybersecurity resources, attract experts or students, individuals in government offices, and increase the number of students studying abroad in ICT from 2014 to 2020. Moreover, the Saudi Arabian Information Security Association also organised annual national contests and conferences for students of all universities and colleges to introduce artificial intelligence to safeguard cybersecurity and information security in ICT, IoT and protect critical databases or infrastructure.

In summary, Saudi Arabia is a developing country that quickly approaches ICTs and innovative technologies, but it is a newbie in cybersecurity protection. A series of cyber-attacks on government, companies, agencies, and airport websites greatly damaged data loss, data leakage, and finance. Hence, the Vietnamese government paid attention to making cyber laws, legal documents, and legal infrastructure to ensure the safety of critical infrastructure protection. Regarding the connection between government organisations and private sectors, it helps strengthen the safety of critical infrastructure systems and cyber resilience capacity, develop research and training, and promote cybersecurity solutions, products or services. Besides, the Vietnamese government also considered the important role of international cooperation as a key factor to boost cybersecurity development to a new level in the same region.

The cyber risks and challenges in the industry are diverse, spanning technological and organisational competencies, stemming from purpose-built components that operate in an ecosystem where cybersecurity is an afterthought. Practical and xi reasonable recommendations to address these problems are discussed to close the gap, some specific and unique to the manufacturing industry. In contrast, other fundamental applications discussed with a manufacturing industry lens are commonly ignored due to perceived complexity, cost, or lack of awareness. Lastly, several of these recommendations were selected for further evaluation and implementation; challenges, approaches, benefits, and outcomes are shared, showing measureable improvements to the organisation's cybersecurity posture.

VI. Study Implications

This study provides some significant implications for research. First, it extends the literature on cyber security by providing a critical and comprehensive literature review as the primary theoretical contribution of this study. The findings of this review reveal an insufficient number of research studies in the field of CSA. Most researchers focus only on the technical aspects of information technology, with limited consideration of users' security awareness and their security behaviour. Gefen et al. [32] agree that it is important to study the issue of cyber security from the aspect of users' security awareness to have a clear understanding of the concept of CSA and to address the issue of security behaviour as a whole successfully. Thus, more research should address the issue of cyber security from the perspective of users' awareness as the existing research on this topic has somewhat ignored this issue.

Second, a quantitative survey was developed to consider basic information about CSA and investigate other security issues related to cyber security, such as passwords, emails, cloud storage, social networks, wireless networks, and smartphones. Analysing the collected data using SPSS revealed a lack of awareness of basic information related to cyber security among Saudi students. In addition, the number of students attending training programs was very low.

This study also has some fundamental implications for Saudi universities. Universities in Saudi Arabia need to empower their students by increasing their awareness of cyber security. Thus, Saudi universities must adopt mass media for educational purposes and introduce cyber security concepts. In addition, universities could offer seminars, lectures, and workshops on the negative impacts of cybercrimes and the importance of cyber security. This approach would encourage students to practice effective security behaviours and then increase the cyber security culture among students. In addition, Saudi Universities could publish such information in newsletters, and magazines, which would help to increase student's awareness about cyber security and encourage them to adopt secure behaviour.

Training Compromises via social engineering techniques are an ever-evolving threat landscape. The attackers devise sophisticated schemes to gain personal information and/or entry into an environment. A specific counter-action cannot mitigate these attack schemes; however, preventing and protecting against breaches can be accomplished by applying a defence-in-depth approach and an effective security awareness training program. Specific to the educational institutes, as part of creating a comprehensive security awareness program, organisations need to deliberately and consciously educate individuals. As part of this comprehensive approach, organisations need to educate personnel on the threat vectors and downstream effects of using social media and how compromising can lead to other lateral advances.

1) Security awareness training: Relative to a security awareness program, studies by Gartner showed that there are four key objectives when deploying an effective security awareness program that drives real meaningful actions [16].

2) Build a knowledge base: Creation of a referenceable and easy to understand security and risk knowledge base across the workforce results in a shared understanding of what is important to the organisation (e.g. password management, encryption of removable media). Make it available to end-users and market its' usefulness.

3) Ability to comply with regulatory requirements: Where required, a regulated enterprise must maintain a cybersecurity training program to ensure that the culture is aligned with the regulatory body requirements. This involves the identification of specific provisions for compliance, capturing specific criteria to satisfy the regulation(s) and applying the necessary controls/provisions to demonstrate adherence.

4) Define a behavioural baseline: To hold an individual accountable for adhering to the organisation's security policies, the organisation's expectations must be clearly defined. Additionally, proper education must be provided with objective evidence (signing an acknowledgement form, etc.) indicating the employee has been educated on the required policy and related practices.

5) Motivate secure behavior: Encouraging positive actions while disapproving of undesired behaviours is necessary to achieve the desired representative behaviours. Using classical conditioning techniques via reward and penalty systems, the desired and undesired behaviours must be identified and described in enough detail to enable targeted monitoring and reinforcement. Educational institutes need to begin applying the same importance and rigour to cybersecurity with overall human safety. It can be expected that in some organisations, cybersecurity training is either not addressed or only executed to "check the box" for insurance or regulatory purposes.

6) Communication/Social media exposure to the network: Organisations should ensure that there is a clear separation between the functions (email, internet access, etc.) that can be performed on P.C.s with access to the factory operations network(s) and those that should be conducted outside of the network entirely.

In addition, Saudi universities need to adopt effective training programs for students, with the major consideration being students' security behaviours. In addition, it is important to involve students in the training programs by researching cyber security. If students were involved in the development process, they would be regularly asked how to develop a secure system and the important steps to encourage students to adopt secure behaviours. Having the students participate in the process and consulting them for their views will create a cyber security culture among students. According to Chun et al. [33], citizens are not just recipients of e-government. They are also the key chain that guides policy formulation through their opinion and views. Carter and Bélanger [34] state that 74.2% of government agencies in the U.K. have a website. However, 90.5% of these agencies have not surveyed to see what online services their citizens and businesses want. Thus, the students' levels of CSA would increase when they are informed of the importance and strategies of cyber security.

VII. Conclusion

The purpose of this research was to look into and analyse cyber security concerns in Saudi Arabia. According to the conclusions of this survey, Saudi students are unaware of the importance of cyber security. This research indicated a poor score for training and awareness, with 92 percent of respondents have never received any form of cyber security training. According to the findings of this study, Saudi institutions should teach their students about anti-cybercrime legislation and the key information security awareness issues discovered in this study. Much more research is needed to establish how students' knowledge levels might be increased by implementing appropriate awareness-raising initiatives. Further research may be needed to identify how best practices might improve the issue areas identified in this study.

Acknowledgment

The author thanks Taif University as this work was supported by the Deanship of Scientific Research, Taif University, KSA [grant number 1-439-6058].

References

[1] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, and M. Xu, "A Survey on Machine Learning Techniques for Cyber Security in the Last Decade," IEEE Access, vol. 8, pp. 222310-222354, 2020.

[2] A. H. Cordesman, J. G. Cordesman, and J. G. Cordesman, Cyber-threats, information warfare, and critical infrastructure protection: defending the US homeland: Greenwood Publishing Group, 2002.

[3] K. Shaukat, S. Luo, S. Chen, and D. Liu, "Cyber Threat Detection Using Machine Learning Techniques: A Performance Evaluation Perspective," in 2020 International Conference on Cyber Warfare and Security (ICCWS), 2020, pp. 1-6.

[4] L. Kim, "Cybersecurity matters," Nursing management, vol. 49, pp. 16-22, 2018.

[5] S. Musman and A. Turner, "A game theoretic approach to cyber security risk management," The Journal of Defense Modeling and Simulation, vol. 15, pp. 127-146, 2018.

[6] K. E. Eichensehr, "Public-private cybersecurity," Tex. L. Rev., vol. 95, p. 467, 2016.

[7] A. Alzahrani and K. Alomar, "Information security issues and threats in Saudi Arabia: a research survey," International Journal of Computer Science Issues (IJCSI), vol. 13, p. 129, 2016.

[8] H. Kruger, L. Drevin, and T. Steyn, "A vocabulary test to assess information security awareness," Information Management & Computer Security, 2010.

[9] H. A. Kruger and W. D. Kearney, "A prototype for assessing information security awareness," Computers & security, vol. 25, pp. 289-296, 2006.

[10] C. McPhee and T. Bailetti, "Editorial: Cybersecurity," Technology Innovation Management Review, vol. 4, pp. 3-4, 2014.

[11] I. Gupta and P. Mishra, "Special Issue on Cyber Security," Defence Science Journal, vol. 66, p. 557, 2016.

[12] K. Parsons, A. McCormac, M. Pattinson, M. Butavicius, and C. Jerram, "A study of information security awareness in Australian government organisations," Information Management & Computer Security, 2014.

[13] J. Liu, Y. Xiao, S. Li, W. Liang, and C. P. Chen, "Cyber security and privacy issues in smart grids," IEEE Communications Surveys & Tutorials, vol. 14, pp. 981-997, 2012.

[14] E. Kritzinger and S. H. von Solms, "Cyber security for home users: A new way of protection through awareness enforcement," Computers & Security, vol. 29, pp. 840-847, 2010.

[15] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, S. Chen, D. Liu, et al., "Performance comparison and current challenges of using machine learning techniques in cybersecurity," Energies, vol. 13, p. 2509, 2020.

[16] T. I. Baig, T. M. Alam, T. Anjum, S. Naseer, A. Wahab, M. Imtiaz, et al., "Classification of human face: Asian and Non-Asian people," in 2019 International Conference on Innovative Computing (ICIC), 2019, pp. 1-6.

[17] S. A. Alashi and H. A. Aldahawi, "Cybersecurity Management for Virtual Private Network (VPN) Applications: A Proposed Framework for the Governance of their Use in the Kingdom of Saudi Arabia," Journal of Information Security and Cybercrimes Research, vol. 3, pp. 31-57, 2020.

[18] T. M. Alam and M. J. Awan, "Domain analysis of information extraction techniques."

[19] R. Von Solms and J. Van Niekerk, "From information security to cyber security," computers & security, vol. 38, pp. 97-102, 2013.

[20] Y. Rezgui and A. Marks, "Information security awareness in higher education: An exploratory study," Computers & security, vol. 27, pp. 241-253, 2008.

[21] S. Atkinson, S. Furnell, and A. Phippen, "Securing the next generation: enhancing e-safety awareness among young people," Computer fraud & security, vol. 2009, pp. 13-19, 2009.

[22] I. Frank and E. Odunayo, "Approach to cyber security issues in Nigeria: challenges and solution," International Journal of Cognitive Research in science, engineering and education, vol. 1, 2013.

[23] E. B. Kim, "Recommendations for information security awareness training for college students," Information Management & Computer Security, 2014.

[24] T. M. Alam, M. Mushtaq, K. Shaukat, I. A. Hameed, M. U. Sarwar, and S. Luo, "A Novel Method for Performance Measurement of Public Educational Institutions Using Machine Learning Models," Applied Sciences, vol. 11, p. 9296, 2021.

[25] A. E. M. Aloufi, A Cognitive Theory-based Approach for the Evaluation and Enhancement of Internet Security Awareness among Children Aged 3-12 Years: Rochester Institute of Technology, 2015.

[26] K. Shaukat, S. Luo, N. Abbas, T. Mahboob Alam, M. Ehtesham Tahir, and I. A. Hameed, "An analysis of blessed Friday sale at a retail store using classification models," in 2021 The 4th International Conference on Software Engineering and Information Management, 2021, pp. 193-198.

[27] T.-M. Alam, K. Shaukat, A. Khelifi, W.-A. Khan, H.-M.-E. Raza, M. Idrees, et al., "Disease Diagnosis System Using IoT Empowered with Fuzzy Inference System," Computers, Materials \& Continua, vol. 70, pp. 5305--5319, 2022.

[28] M. N. Saunders and F. Bezzina, "Reflections on conceptions of research methodology among management academics," European management journal, vol. 33, pp. 297-304, 2015.

[29] K. Shaukat, T. M. Alam, M. Ahmed, S. Luo, I. A. Hameed, M. S. Iqbal, et al., "A Model to Enhance Governance Issues through Opinion Extraction," in 2020 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2020, pp. 0511-0516.

[30] A. Bryman and E. Bell, "Business research methods (Vol. 4th)," Glasgow: Bell & Bain Ltd, 2015.

[31] K. Shaukat, T. M. Alam, I. A. Hameed, W. A. Khan, N. Abbas, and S. Luo, "A Review on Security Challenges in Internet of Things (IoT)," in 2021 26th International Conference on Automation and Computing (ICAC), 2021, pp. 1-6.

[32] D. Gefen, G. M. Rose, M. Warkentin, and P. A. Pavlou, "Cultural diversity and trust in IT adoption: A comparison of potential e-voters in the USA and South Africa," Journal of Global Information Management (JGIM), vol. 13, pp. 54-78, 2005.

[33] S. Chun, S. Shulman, R. Sandoval, and E. Hovy, "Government 2.0: Making connections between citizens, data and government," Information Polity, vol. 15, pp. 1-9, 2010.

[34] L. Carter and F. Bélanger, "The utilization of e ‐ government services: citizen trust, innovation and acceptance factors," Information systems journal, vol. 15, pp. 5-25, 2005.