Self-sufficiencies in Cyber Technologies: A requirement study on Saudi Arabia

Nawaf Alhalafi [1] and Dr. Prakash Veeraraghavan [1],
17814379@student.ltu.edu.au P.Veera@latrobe.edu.au
La Trobe University, Computer Science & Information Technology Department, Australia .

Abstract
Speedy development has been witnessed in communication technologies and the adoption of the Internet across the world. Information dissemination is the primary goal of these technologies. One of the rapidly developing nations in the Middle East is Saudi Arabia, where the use of communication technologies, including mobile and Internet, has drastically risen in recent times. These advancements are relatively new to the region when contrasted to developed nations. Thus, offenses arising from the adoption of these technologies may be new to Saudi Arabians. This study examines cyber security awareness among Saudi Arabian citizens in distinct settings. A comparison is made between the cybersecurity policy guidelines adopted in Saudi Arabia and three other nations. This review will explore distinct essential elements and approaches to mitigating cybercrimes in the United States, Singapore, and India. Following an analysis of the current cybersecurity framework in Saudi Arabia, suggestions for improvement are determined from the overall findings. A key objective is enhancing the nationwide focus on efficient safety and security systems. While the participants display a clear knowledge of IT, the surveyed literature shows limited awareness of the risks related to cyber security practices and the role of government in promoting data safety across the Internet. As the findings indicate, proper frameworks regarding cyber security need to be considered to ensure that associated threats are mitigated as Saudi Arabia aspires to become an efficient smart nation.

Keywords:
cybersecurity, cybercrime, cyberattacks, security frameworks, information technology (IT), e-government, smart city, e-learning

1. Introduction

Many businesses have demonstrated a keen interest in automating their processes to deliver services in cost-effective, fast, and easy ways, given the extensive development in communication technologies. In recent years, the use of communication technologies, including mobile technologies, has risen significantly. Approximately 53% of the global population does not have access to the internet, which indicates 47% adoption (see fig. 1). These numbers are anticipated to grow due to the rapid pace of technology deployment in developing nations.

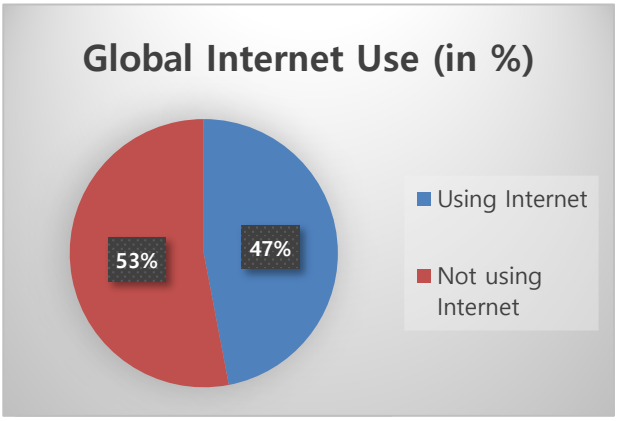

Fig. 1. Global Internet Use, 2016. Data Source: (International Telecommunication Union [ITU] 4)

Nations across the world have been facing greater threats of cyber-crimes. In 2018, the regions most affected by disastrous data breaches included Latin America and the Caribbean (8%), Europe, Middle East & Africa (27%), North America (30%), and Asia Pacific (35%) (Singh and Alshammari 638). Further, in 2019, the United States, India, Singapore, and Saudi Arabia experienced the most cyber-attacks, respectively (Singh and Alshammari 638). In particular, Saudi Arabia is prone to most cyber-attacks in the Arab region. Major cyber-attacks such as the 2017 Mamba Ransomware have occurred in the country, with forecasts suggesting that these attacks would cost the country's economy about US $8 billion (Singh and Alshammari 638). MENA countries significantly suffer from cyber-attacks relative to other regions around the globe. For instance, in 2009, the internet penetration rate in MENA nations stood at 29%, while the global average was 27%. Nonetheless, this rate has drastically risen in the MENA region, with a huge ratio difference compared to the rests pf the world. In 2019, the cyber-attack rate rose to over 60%, representing 50% increase since 2009 (see Fig. 2). Cyber-attack events bear considerable social and economic costs for all nations across the world. The Middle East

Manuscript received May 5, 2022
Manuscript revised May 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.5.29

region, in particular Saudi Arabia, is a primary victim of cyber-attacks.

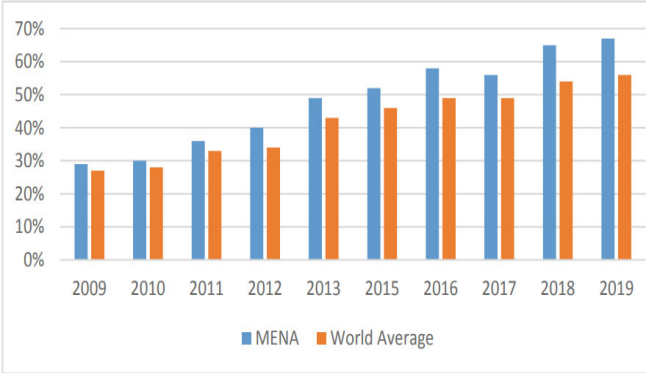

Fig. 2. Cyber –Attack Rate between MENA and the Rest of the World, 2009-2019. Data Source: (Mawgoud et al. 915)

Several primary institutions are responsible for cybersecurity administration in Saudi Arabia. In 2011, the Ministry of Communications and Information Technology (MCIT) started developing the nation's first National Information Security Strategy (NISS), a draft created by a group of global top consultants and experts, and presently in its seventh copy (Hathaway, Spidalieri and Alsowailm 8). The demand for a country-wide cyber security approach resulted from the acknowledgement that Saudi Arabia is prone to rising, diverse threats to its national security, economic prosperity, and cultural norms. At the moment, the roles for cyber security in this country are distributed among the MCIT, the Ministry of Interior (MoI), and other government agencies. The National Cyber Security Center (NCSC) plays the responsibility of a government computer emergency response team (CERT), and is tasked with safeguarding the national government, as well as Critical National Infrastructure (CNI) operators' data and communication routines (Hathaway, Spidalieri and Alsowailm 9). In particular, the NCSC has a number of functions, including planning national guidelines to protect Saudi Arabia's information infrastructure and critical assets, determining threats and generating risk intelligence, and supporting the flow of data and security indications between distinct sectors.

A clear difference exists between cyber incidents in Saudi Arabia before and during COVID-19 pandemic. Amid the pandemic, cybercriminals are developing attacks at a rapid rate, exploiting the uncertainty due to the unstable social and economic global environment. In particular, the MENA region highlighted the rising application of social media to propagate fake news linked to COVID-19, for example, the illicit sale of pharmaceutical products regarding the coronavirus (INTERPOL 7). In addition, there has been an increase in registration of malicious domains targeted at generating COVID-19 statistics, as well as a higher number of phishing and online fraud. In view of these incidents, INTERPOL's Cybercrime Directorate developed a report, Global Assessment Report, to offer a comprehensive synopsis of the cybercrime setting amid the COVID-19 pandemic (see Fig. 3)

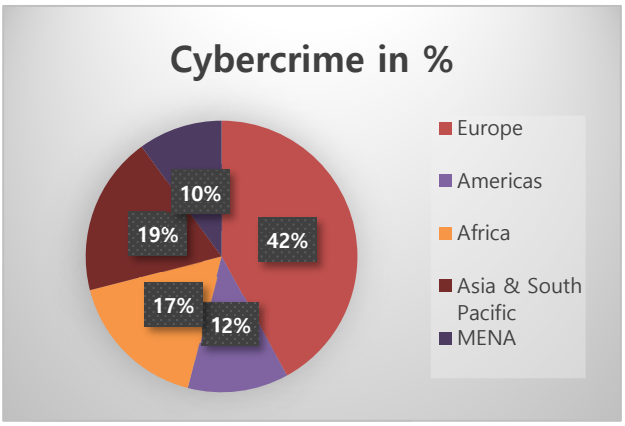

Fig 3. INTERPOL Global Cybercrime Report, 2020. Data adapted from: (INTERPOL 4)

Smart devices are continuously being utilized across various countries. By 2020, the number of smart devices that can be applied in diverse sectors and domains, including healthcare, smart grids, and transport, exceeded four billion (Alzubaidi 1). Nonetheless, the persistent use of these devices has resulted in new challenges and serious security risks since attackers can exploit them to access private and confidential data, or leverage them to organize more severe attacks. In Saudi Arabia, cybersecurity is considered a vital element of national safety. Additional geographical regions of Saudi Arabia are becoming incorporated into the global village, a move that necessitates extra projects geared towards linking the virtual disparity and mitigating cybersecurity (Talib et al. 316). A primary initiative is the creation and execution of a precise cybersecurity policy; essentially, Saudi Arabia's government needs to comprehend the sociocultural aspects of its wider community. This interconnection forms the basis of this study. In this regard, study outcomes will be monitored through formulation of a series of comprehensive policy frameworks for the Saudi government to assess its success in implementing the smart city paradigm (Alhalafi and Veeraraghavan 2). As a result, the purpose of a countrywide cybersecurity program is to facilitate a safer internet space by protecting associated human, economic, technological, organizational, and data sources.

2. Research Aims

This study is focused on Saudis and explores the observable shortage of local national proficiencies in cybersecurity, given that a large number of countries fail to rise except with the aid of their local skills. Moreover, is examines how Saudi Arabia and three other comparative nations work to realize the objective of educating the masses on problems pertaining to cybersecurity and potential risks.

Another intention of this study is to boost awareness and adoption of cyber competency and awareness initiatives in the realm of ICT, particularly the Saudi citizens who show a scarcity in local expertise. This shortage in ICT expertise in government agencies is due to declined interest among locals, coupled with the appeal of private firms which provide more competitive packages for associated professionals. Further, this study is geared towards the awareness of Saudi citizens with regard to cyber threats and the necessity for related programs to comprehend the current state.

In a nutshell, e-government systems across the globe are prone to various threats generated from cyberspaces. The case of Saudi Arabia offers an appropriate foundation for examining such uncertainties to propose effective interventions. As a nation, Saudi Arabia is establishing an increasingly complex IT infrastructure that requires protection to effectively deliver services to citizens. In addition, investigating some risks prevailing within the macro environment to make estimates regarding long-term threats. A comparison between the cybersecurity framework of Saudi Arabia and that of three other nations is important to analyze the need for transformations. This study provides a strong basis for assessing the cybersecurity context in Saudi Arabia.

3. Motivation for this work

Rapid development has been observed in the application of telecommunication advancements and the adoption of the Internet across the globe. Specifically, Saudi Arabia needs to direct significant focus on safeguarding IT structures across different entities to promote a smooth change towards digitalization. This transformation is even more critical amidst the COVID-19 pandemic, which has forced businesses and institutions to adopt digitalization. Saudi Arabia is prone to common cyberattacks, including malware and data theft, which pose negative impacts on the IT infrastructure.

Key stakeholders in the Saudi government must maintain focus on users' purchase intentions to enhance the level of perceived security in e-government applications. Delivering services via secure applications would encourage citizens to adopt these technologies.

Just like Singapore, India, and the United States, Saudi Arabia should consider establishing effective regulations to address potential cybercrimes.

Given cultural influences on cybersecurity models, the country should rely local standards to guide the execution of a robust framework.

4. Related Work

In recent times, cybercrime monitoring has gained significant attention, particularly in developed nations, given the rapid increase in cyber-attacks. This segment examines recent methods to the evaluation of user understanding on cyber threats globally, as well as reviews focused on Saudi Arabia.

Alotaibi et al. (2017) explored the cybersecurity awareness level among Saudi nationals by implementing a quantitative online-directed survey, with a sample of 629 participants (30% female, 70% male). These researchers noted that while the participants portrayed acceptable IT scholarship, their degree of awareness in terms of cybercrime, cybersecurity practices, and the role of government and institutions in maintaining the integrity of data online was scarce.

Other studies that have focused on examining the present cybercrime risks and awareness in certain locations. An elaborate example is Zayid and Nadir (2017) who assessed the cybersecurity awareness in the Alnamas region, a district in the southern area of Saudi Arabia. This study surveyed 132 undergraduates reflecting an IT background and found that 15% of the students had experienced cybercrime, over 80% were interested in obtaining further training to enhance their knowledge, and 69% of cybercrimes were propagated through social media.

By using a sample of sing 2325 participants, Alzahrani and Alomar (2016) administered an online questionnaire to ascertain the level of information security awareness. From the findings, the researchers found that the general awareness degree regarding information security was 35%, 37% for password security, 38% for wireless network security, 40% for social media use security, and 44% for secure cloud computing.

5. Cyber Security Models in Saudi Arabia

Officially recognized as the 'Kingdom of Saudi Arabia', Saudi Arabia is one of the Gulf nations located in the Western part of Asia. This country is purely a monarchy, ruled by a royal family. Islam and Arabic are the main religion and language respectively (Talib et al. 316). Like other members of the Gulf region, Saudi Arabia depends on oil, providing approximately 66% of the sector's oil (Almarhabi 14). Subsequently, key authorities and the government must ensure that security is highly upheld. Regarding the policy framework in Saudi Arabia, it is generally agreed that the state lacks adequate focus on the nationwide cybersecurity coverage.

Various organizations across the world direct attention towards supporting digital transformation successfully. In view of Vision 2030, Saudi government is geared towards establishing a digital foundation in the country. As Almomani et al. assert, this ambitious agenda is dependent on the protection of both data and related systems within the private and public spheres (11). In other words, government agencies should identify proper cybersecurity measures to protect both publica and private organizations from cybercrime. In addition, Sagar et al. observe that IT infrastructures need to be safeguarded to advance a seamless digital transformation (1). Such transformation is even more emphasized following the COVID-19 pandemic, where important organizational activities were moved online to minimize the infections (Almomani et al. 11). One of the sectors that was largely influenced by this unexpected change is education.

Online and remote learning is among the outcomes of COVID-19-related lockdowns. Several issues arise when attempting to digitize the learning process due to the unpreparedness of higher learning institutions in utilizing e-learning systems (Ali 20). Hence, through this pandemic, a vital lesson for most schools is the importance of remote learning infrastructure. In addition, a lack of technical capabilities, including cybersecurity skills, is evident in higher education institutions (Ali 20). Ultimately, key stakeholders must begin to adopt education applications and utilize them in instruction.

In Saudi Arabia, e-learning systems are robust in well-known institutions, for example King Abdul-Aziz University. Due to the COVID-19 pandemic, the adoption of e-learning or mobile education was inevitable. As guided by the Ministry of Education, all learning institutions switched to online teaching (Almomani et al. 12). However, several challenges occurred due to the application of evaluations and tutoring in digital platforms, as well as securing the e-learning offerings.

For organizations, various existing models and standards delineated at the domestic and global levels provide cyber security regulatory guidelines. Nonetheless, certain limitations hamper such progress, including poor understanding of the current Saudi Arabia cyber security models in general and in the context of higher learning and the lack of a cybersecurity maturity framework detailed enough to cover the accepted paradigms, for example the Essential Cybersecurity Controls by the National Cybersecurity Authority (NCA) (Almomani et al. 11). Importantly, these challenges necessitate the use of well-developed tools by organizations to conduct self-evaluations to monitor their cybersecurity maturity position. Institutions can identify constraints and establish a clear plan for enhancing their security levels and safeguard their systems from distinct security attacks.

IT advancements are critical for economic progress and improved quality of life for contemporary societies. As Aljabri notes, the Saudi government has embraced the long-term vision of "transformation into an information society and the digital economy to increase productivity and provide communications and information technology (IT) services for all sectors of the society in all parts of the country and build a solid information industry that becomes a major source of income" (321). Nonetheless, in the years preceding the late 90s, Internet access in the country was restricted; technical challenges associated with the utilization of Arabic on the Internet and other devices appeared to limit Internet use to only those individuals who could work in English. Saudi Arabia has made notable progress since the commencement of public access to the internet. The country had about 28.5 million internet users in 2018, with the number expected to rise to 35 million by 2023 (see fig. 2). This increasing number of users makes the country a primary target for cyber-attacks.

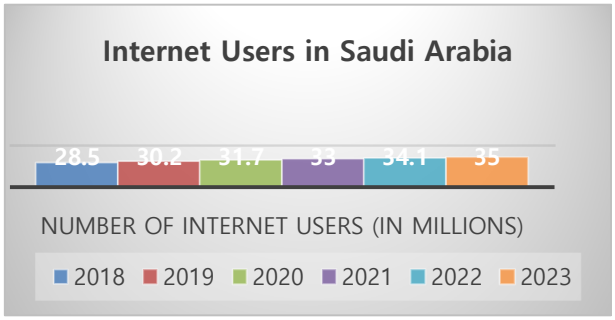

Fig. 2. Number of Internet Users in Saudi Arabia, 2018 to 2023. Source: (Aljabri 321)

Saudi Arabia has several legislations linked to cyber-security. These include the Telecom Act (2001), Anti-Cyber Crime Law (2007), and Electronic Transactions Law

(2007). The former, Telecom Act (2001), offers supervisory rules for the telecom sector. It established the Saudi Communications Commission (SCC), which is responsible for developing access rights, grant licenses, and directs the guidelines of competition (Singh and Alshammari 642). This law safeguards the confidentiality and privacy of individuals, and highlights breaches and penalties under article 37.

In addition, the Anti-Cyber Crime Law (2007) describes unauthorized access as deliberate access by any user to websites, computers and networks, and IT systems. This Act determines different cyber-crimes and ascertains their punishments (Singh and Alshammari 642). It includes penal provisions against safeguard of information interception, as required under Article 3. Guideliens pertaini9ng to the maintenance of public morals are also included.

The Electronic Transactions Law (2007) considers electronic transactions, records, signature, and others, and is geared towards regulating and establishing a legal framework for such transactions as in Article 2 (Singh and Alshammari 642). Further, this law provides legal validity to electronic records as set in Article 5. On the other hand, Saudi Arabia has also created the Information Security Policies and Procedures Development Framework for Government Agencies, comprises IS policies that enable government agencies to monitor related threats (Singh and Alshammari 642). Overall, nations need to collaborate and share information.

6. Comparisons of Saudi Arabia and Other Countries: USA, Singapore, and India

6.1 THEME 1: LACK OF TRUST

6.1.1 Saudi Arabia vs. United States

Certain distinctions exist between cyber security in Saudi Arabia and the United States. Alotaibi and others noted that perceived trustworthiness has a positive major impact on behavioral intention to use m-government services (208). This observation suggests that most participants in this research trust such applications and their merits since they have been deployed by the government. This result is consistent with the principle that when trust in the Internet and government is enhanced, intention to use e-government services increases. In addition, security may not be a problem for most individuals, who adopt government applications since they have been utilizing the Internet for a long time and are well familiarized with security and privacy concerns (Faqih 154). Privacy issues do not affect purchase intentions of cloud computing services in the United States (Alotaibi et al. 208). For this reason, Faqih concluded that more security does not result in greater intention to use online means for purchase (154). Therefore, decision makers in the Saudi government are advised to continue focusing on the aspect of purchase intentions to improve the level of perceived security in applications. Moreover, they should deliver services through secure applications to motivate users to embrace these technologies (Alotaibi et al. 208). Application developers need to ensure the security of these applications, and the Saudi government should enforce regulations to safeguard users in case of privacy and security breaches in e-government services.

In view of cybercrimes, related regulations in Saudi Arabia are influenced more by the Islamic and social principles, as well as local cultural contexts. These laws include the penalties for the different crimes and the fines that the religion considers consistent with the values they practice (Aljabri 323). Conversely, cybercrime in the United States is wider and more multifaceted due to greater Internet access in the country and broader ethical scopes.

Smart cities in the United States have experienced incidents of cyber insecurity. For example, in Dallas, a situation occurred where the Texas Health and Human Services Commission inadvertently revealed confidential information of 6617 healthcare clients (Alhalafi and Veeraraghavan 4). This incident occurred as the organization evolved to using a novel server. However, since the server was public and unsecured, this entity was susceptible to possible attacks. According to Alhalafi and Veeraraghavan, following the assessments grounded on the HIPAA standards, the commission was required to settle a fine of $1.6 million (4). This scenario prompted the U.S. federal government to intervene by focusing on an integrated and regimented approach to sustain cybersecurity. Similar events were mitigated by fostering the security infrastructures of databases and enhancing stakeholders' integrated response in addressing cyber security and risks. During investigations, Saudi Arabia's Communication and IT Commission provides the required technical support to the established security body to assist with the examination of diverse cybercrimes (Aljabri 323). However, in the United States, the Federal Bureau of Investigation is responsible for investigating such offenses, in line with the Constitution.

6.1.2 Saudi Arabia vs. Singapore

Singapore is a key target for cyber criminals, given its pioneering position among the global smart cities. Alhalafi and Veeraraghavan found that cybercrimes in Singapore comprised approximately 26% of all crimes (5). Furthermore, these researchers identified 3215 more incidences of cyber-attacks in 2019, when compared to the previous period (5). Of great concern is the prevalence of rip-offs in e-commerce, which represent the largest

proportion of cybercrimes in the country. Phishing attacks on websites, ransomware and agencies' spoofing are other examples of cybercrime cases highlighted. These threats have forced the government to introduce robust legal frameworks to protect Singapore's businesses and technology users.

Singapore recognizes cybersecurity as a primary driver of its objective for a smart nation. In 2015, the government created a National Cybersecurity Masterplan 2018, which was a 5-year program aimed at guiding the city's attempts of maintaining cybersecurity (Alhalafi and Veeraraghavan 5). This program targets the primary stakeholders in the city and seeks to develop a secure cyber-physical environment that is highly responsive to the needs of users.

Of greater importance is cloud computing, which is regarded a critical enabler of the country's Smart Nation agenda. Singapore's Prime Minister launched this vision in 2014 and 2017, with the intention of updating the country's aspirations towards technological innovation and execution (Ng 40). Over the years, Singapore has effectively developed its ICT infrastructure. This development is evidenced by the significant mobile subscription penetration rate of over 155% in 2013 (Ng 40). Furthermore, about 73% of the population use the internet, a figure comparable to the average internet users of over 70% in developed nations (Ng 40). These statistics highlight the considerable levels of connectivity and mobility among Singaporeans.

In the public realm, Singapore has adopted government projects to transfer various processes, which initially demanded direct interactions, and to embrace paperless transactions. Consequently, this country has been ranked prominently in e-government adoption; for example, in 2013, it became a pioneer in digital administration, ahead of more developed countries, including the United States (Ng 40). Regarding government-to-business contexts, a survey indicated that 99% of organizations utilized government websites, with over 90% citing satisfaction with the quality of information and reduced complexity in implementing online transactions (Ng 40). These efforts have received positive responses from individuals and business organizations.

Singapore directs focus on a coordinated strategy to address cybercrimes at the government level. Cybersecurity is being transformed from prevention to response and revitalization (Ng 45). Additionally, resilience and event-response capabilities are considered in infrastructural development and policy planning, especially in crucial data infrastructure sectors, such as health, telecommunications, and banking. Combined, the rising sophistication of cybercrimes and the need to safeguard against more severe cyber-attacks have prompted the government to embrace a private cloud platform. While the costs are considerably high, the government has certainly determined that the advantages outweigh the drawbacks.

6.1.3 Saudi Arabia vs. India

In India, smart cities have been prone to various online risks, which hamper service delivery and violate user confidentiality. In recent times, amidst the COVID-19 pandemic, cyber security threats towards these smart cities have been on the increase (Alhalafi and Veeraraghavan 5). These attacks appear in varied types and comprise high-level risks on vital systems, resulting in disordered industrial control infrastructures. In other instances, sensor data has been compromised, leading to panic. Overall, these data threats have been on the increase in Indian smart cities, a situation that demands intervention from responsible authorities in establishing a framework for mitigating cybersecurity uncertainties.

India experiences unique challenges given its huge population and coverage area. Authorities in this country are primarily focused on achieving the actual potential of cyber-physical systems (Ahmad et al. 12). Various flagship initiatives are being managed to facilitate the development of interdisciplinary cyber-physical systems. India's mission on international cyber-physical systems is geared towards the formulation of frameworks that address nation-related issues through integrated Internet of Things (IoT) systems for smart services. In addition, such attention is directed towards advancing entrepreneurship and social inclusion. An example of an institution keen on developing indigenous technologies is IIT-Guwahati (Ahmad et al. 12). Several initiatives in the country are aimed at mitigating community problems by adopting the notion of cyber-physical systems.

6.2 THEME 2: LACK OF AWARENESS AND TRAINING DEVELOPMENTS

6.2.1 Saudi Arabia vs. United States

In the Middle East region, security awareness of information, particularly among undergraduates, scholarly researchers, and staff, has been examined to determine their degree of knowledge of information systems. In a study, the researchers note that lack of scholarship of information system principles is the main impediment to security awareness (Al-Janabi, Samaher and Al-Shourbaji 23). In this research, the objective was exploring the effects of security risk and the lack of security awareness in the organizations. Several suggestions to minimize the severity of this situation were formulated, namely reinforcing awareness and training initiatives as well as embracing

safety measures across learning institutions to promote data security.

Various factors necessitate an examination of cyber security in e-government services. In the view of Saudi Arabia, the e-government paradigm of administrative systems is a relatively new idea, originating in the 1980s (Alrubaiq and Alhrabi 303). In government contexts, the execution of technology in providing diversified offerings is a costly plan that demands economic practicality. An effective model within which the electorate can access different services is necessary and must be protected to promote social welfare (Alotaibi et al. 208). Given e-government implementation in the country, significant advantages – such as the adoption of digital technologies and a minimization in the cost of public service – have been evident. Saudi Arabia is a nation maintaining a positive outlook on the international stage with the goal of securing varied economic interests.

6.2.2 Saudi Arabia vs. Singapore

Progressive collaborations to innovate on various issues should be established. A focus on establishing a center with transferable capabilities is vital amidst the transition of tech roles towards talent mega-centers. Ng observes that for a nation aspiring to become a technology hub, for example Singapore, a major problem would be training a considerable number of people to achieve long-term demands (46). Entities need foreknowledge to identify new instructive programs, which effectively address market needs. A memorandum of understanding signed by the Lee Kuan Yew School of Public Policy aimed at obtaining public-sector data to gain insights into the demand and supply of capabilities within distinct occupations (Ng 46). Such understanding empowers individuals to boost their skills, allows training institutions to develop efficient courses, and enables the government to run robust programs.

An assessment of Saudi Arabians indicates that their cybersecurity awareness level is considerably low. This situation can be attributed to the nature of the national culture (Khader et al. 420). Additionally, while the Saudi citizens exhibit a clear understanding of information technology (IT), their knowledge of cybersecurity risks and the government's role in facilitating information safety across the internet is quite limited. Therefore, state agencies should create awareness of these issues through training initiatives in learning institutions.

6.2.3 Saudi Arabia vs. India

India faces a serious shortage of cybersecurity experts, which poses adverse challenges on the country's capacity to address rapidly increasing cybercrimes. For example, a considerable number of IT security auditors are required to assess the stability of management controls in business processes and projects and validate their effectiveness (Kshetri 323). Important to note, most web pages of Indian government agencies are administered by the National Informatics Center, which was created by the government to advance IT culture across various agencies. These websites are susceptible to cyber-attacks due to a lack of capable staff, particularly IT security auditors. In 2011, Reserve Bank of India adopted several recommendations, including the establishment of independent information security teams within banking institutions and sustenance of efficient cyber security resources (Kshetri 323). Nonetheless, India still encounters problems enforcing the central bank's guidelines due to the lack of IT skilled professionals to audit organizations' cybersecurity practices.

6.3 THEME 3: IMPACTS OF CULTURE

6.3.1 Saudi Arabia vs. United States

American social customs are broad, coupled with distinct values based on the diverse populations and ethnic backgrounds. This convergence means that one religion cannot form the basis for governing the penalties for people found guilty of cybercrime offenses; therefore, a challenge in managing the practice appears (Aljabri 323). In addition, variations exist in the level of jail time for similar crimes in Saudi Arabia and the United States. For example, in the former, accessing a computer without the owner's approval is liable to a fine of not more than $5000 or imprisonment of one year (Aljabri 323). A similar crime would carry a jail term of less than a year in Saudi Arabia.

In Saudi Arabia, the rate of internet usage has rapidly increased. An estimated 13 million people use the Internet, comprising about 46% of the nation having such access. Among this proportion, approximately 1.9 million individuals are highly active Twitter users (Chaudhry 947). This situation makes the country the world's fastest-growing Twitter nation. 47% of all tweets in the Arab region are generated from Saudi Arabia (Chaudhry 947). Given an active Twitter and the Internet community in this nation, the government has an overwhelming responsibility in controlling online engagement practices.

6.3.2 Saudi Arabia vs. Singapore

In Singapore, public service is transitioning towards an absolute government strategy to policy making, offering a primary motivation for government cloud adoption. This strategy demonstrates that many modern challenges cannot be siloed. To create chances for these 'silos' to engage with each other, the government developed forums for executive leaders in distinct sectors to deliberate on policies (Ng 42).

A relevant illustration is the Social Forum, which convenes top leaders from different social agencies to establish mutual understanding for social guidelines. Such partnerships provide case studies for government cloud computing.

Cybersecurity and a prevention-oriented cultural inclination drive the prevalent utilization of a private cloud. Cross-cultural professionals, who recognize national cultures, have defined Singapore as characterized by strong social values and impatience for non-standard conduct. In a review of 33 nations, this country emerged in the top quartile of 'tightness' values (Ng 45). Additionally, Singapore is a prevention-directed community, where civil servants are detail-focused and emphasize positive outcomes, such as high vigilance on quality and professionalism. These empirical reviews on culture offer an insight into the government's quest for adopting a private cloud.

Phishing is the most dominant social engineering method in recent times. It entails stealing users' credit card numbers and login details to access their private data. This form of cyberattack accounted for 77% of all social engineering attacks in Saudi Arabia's educational sector in 2017 (Alsulami et al. 3). These attacks can be implemented through the internet and social media.

6.3.3 Saudi Arabia vs. India

Social harmony and human connections are a major emphasis among Asians. Efficiency and time management, on the other hand, are critical values for Westerners (Kshetri 323). Such cultural factors have a clear implication on cybersecurity. In India, for instance, call center personnel consider security checks dishonorable (Kshetri 323). Similarly, sharing of passwords is more typical in India than in the West, given the varied social contexts. This practice is associated with different cases of offenses. An example is Wipro, an IT business in India, in which a member of staff used a colleague's password to steal approximately $4 billion from the organization's bank account (Kshetri 323). The lack of clearly developed approaches and procedures results in reduced cybercrimes' guilt relative to traditional crimes. In developing regions, these conditions are more likely to be predominant, making cybercrimes more justifiable. An example is the issue of click fraud, which is quite prevalent in India, yet those involved may not be aware of its implications for businesses (Kshetri 323). Overall, a prevalent notion is that in many instances, criminals of cyber-attacks are not aware of the likely damage that their engagements can cause to others.

6.4 THEME 4: SHORTAGE OF LOCAL EXPERTISE

6.4.1 Saudi Arabia vs. United States

In Saudi Arabia, a lack of IT professionals to guide the execution of e-government in their entities is clear. A primary factor for such lack is the moving of IT expertise from the public sector to the private sector since government salaries are relatively low (Alshehri and Drew 1041). Further, a lack of IT personnel at all levels, including programmers and professional managers, is evident. Consequently, the training of existing employees, especially in the public sector, is vital to advance the adoption of any novel technology. In the United States, the Joint Task Force (JTF) on Cybersecurity Education (CSEC2017) is responsible for establishing comprehensive curricular guidance on cybersecurity scholarship (Carlton and Levy 22). Related efforts are geared towards dissemination to national and global programs, which provide a cybersecurity undergraduate degree. As a result, the United States focuses on developing students' cybersecurity capabilities during regular courses.

6.4.2 Saudi Arabia vs. India

In India, the problem of cybersecurity has received relatively limited focus from policymakers. Thus, the government has failed to address the nation's growing demands for an efficient cybersecurity framework. This country lacks robust offensive and defensive cybersecurity capabilities due to inaccessibility to mechanisms essential to handling sophisticated malware (Parmar 3). On the other hand, a significant proportion of Saudi Arabia population lack the requisite IT competency needed to advance smart cities. Therefore, this situation demands for dependence on expatriates to assist in the management of distinct elements of the smart city initiative (Alhalafi and Veeraraghavan 7). Overall, the government has a huge role of encouraging its citizens to acquire IT skills by taking associated courses.

6.4.3 Saudi Arabia vs. Singapore

Singapore's education system is a critical connection to the nation's progress. It has always been important in facilitating competency development among local populations, thereby ensuring a competent workforce. Further, the country's school system focuses on creating highly-skilled individuals capable of addressing future challenges. The National Cyber Security Masterplan 2018 (NCSM2018) was launched in 2013 to promote research and development, as well as arise cyber security expertise (Ipsos 20). Capital investment in hiring a development and

maintenance team is necessary to develop a single digital trust platform for a smart city. In particular, the cost of acquiring the technology and staff is anticipated to be high for Saudi Arabia (Alhalafi and Veeraraghavan 7). Generally, increasing the level of cyber competence among citizens requires significant investment of resources in public education and other programs.

7. Findings and Recommendations

Saudi Arabia's government mindset regarding privacy and security guidelines relative to the United States, India, and Singapore has been examined. This review reflects the state's lack of readiness in formulating clear policies to realize compliance with security and privacy policies in comparison to the other three nations (Talib et al. 318). Employees in public enterprises show a lack of awareness of information security. Moreover, Talib et al. found that the Bureau of Investigation and Public Prosecution disregards such guidelines since policies and regulations in Saudi Arabia are not linked with particular activities (318). Compared to what has been implemented in the other three countries, this approach remains inadequate. These comparative nations apply penalties and rewards to punish criminals, while motivating individuals who comply with set guidelines. While Saudi Arabia considers the sanctions principle, it has yet to apply the rewards strategy given the disparity in measuring the policy execution in government agencies (Talib et al. 318). This situation implies that the government should take drastic measures to improve adherence to privacy and security policies, for instance, by offering education and training personnel to enhance their awareness levels. To develop, execute, and analyze the security and privacy guidelines, sufficient finances should be allocated to the public entity. Despite varied cybersecurity legislations between the countries, a common fact that can be inferred from existing literature is that cybersecurity awareness is urgently required.

Throughout this literature review, four different smart city initiatives by Saudi Arabia, the United States, Singapore, and India have been covered. Related data is summarized in a table with a 'Y' indicating that their proposal is feasible and 'N' signifying a lack of response to a particular aspect. Key to note, the element of user acceptance was not addressed by any of the countries (see table 1). For the identified comparable countries, it may be effortless to persuade users to utilize new technologies due to the relatively diverse socio-economic contexts. Nonetheless, the opposite is clear in Saudi Arabia. Additionally, the nexus between public and private sectors is validated in comparable nations (Alhalafi and Veeraraghavan 6). Research and development projects through private-public sector programs is also well reflected. Since Saudi Arabia is at an infant phase, a potential challenge in successfully creating smart cities is clear.

Factors	Saudi Arabia	United States	Singapore	India
User acceptance	N	N	N	N
e-governance	Y	Y	Y	Y
IT/IS professionals	N	Y	Y	N
Digital technologies	Y	Y	Y	Y
e-learning	Y	Y	Y	Y
Smart healthcare	N	N	N	Y
Cyber awareness programs	N	Y	Y	Y

Table 1. Comparison of Cybersecurity Initiatives across the Countries

The above table shows the set of cybersecurity programs adopted in Saudi Arabia and three comparative nations, including the U.S., India, and Singapore. Seven aspects are considered and vary across the four nations. In terms of user acceptance, none of the nations portrays a significant focus on advancing user awareness. E-governance, e-learning, and digital technology initiatives are increasingly being applied across these countries. Saudi Arabia needs to focus on user acceptance, invest in highly competent IT or information system (IS) professionals, and promote smart healthcare.

In terms of e-government services, this literature review shows different problems and achievement aspects identified with related usage ventures in Saudi Arabia. Further, this analysis has included various approaches to the implementation of cybersecurity models. Talib et al. note that similar processes of development and e-government initiatives are being applied across different countries (316). In terms of innovation capabilities, Saudi Arabia needs to focus on leveraging the right expertise and information to ensure effective management. Alrubaiq and Alharbi add that since this country is not industry-oriented, a multifaceted perspective pertaining to training and innovation needs is necessary (309). Services can be efficiently and transparently provided through e-government systems in various segments. For Saudi Arabia,

such structures are susceptible to cybercrime uncertainties, thereby necessitating an all-inclusive information safety paradigm.

Decision-makers in the Saudi Arabian government, including the providers of these applications, should direct efforts towards establishing trust with the Saudi citizens to motivate them to utilize services through e-government systems. In addition, developers of these applications should create trustworthy technologies since trust has been shown to be a vital consideration for citizens using e-government applications (Alotaibi et al. 208). However, perceived security has no effect on behavioral intention to use these technologies. This finding might imply that participants are not worried about security as they trust applications provided by the government.

8. Conclusion and future work

Rapid development has been observed in the application of telecommunication advancements and the adoption of the Internet across the globe. Specifically, Saudi Arabia needs to direct significant focus on safeguarding IT structures across different entities to promote a smooth change towards digitalization. This transformation is even more critical amidst the COVID-19 pandemic, which has forced businesses and institutions to adopt digitalization. Saudi Arabia is prone to common cyberattacks, including malware and data theft, which pose negative impacts on the IT infrastructure. Key stakeholders in the Saudi government must maintain focus on users' purchase intentions to enhance the level of perceived security in e-government applications. Delivering services via secure applications would encourage citizens to adopt these technologies. Just like Singapore, India, and the United States, Saudi Arabia should consider establishing effective regulations to address potential cybercrimes. Given cultural influences on cybersecurity models, the country should rely local standards to guide the execution of a robust framework. However, from this study, it is clear that such a model doesn't exist in Saudi Kingdom. This study concludes that to promote user-participatory cyber culture, there is a strong need for technological self-sufficiency. In our future paper, we validate this claim through user-surveys. Our survey will involve citizens who are not IT-savvy, IT experts and Governmental agencies. We also evaluate various cultural, technical, and human resource barriers in achieving this goal.

9. References

[1] Ahmad, Onais M., et al. "Cyber-Physical Systems and Smart Cities in India: Opportunities, Issues, and Challenges." *Sensors*, vol. 21, no. 22, 2021, pp. 1-25. *MDPI,* doi: 10.3390/s21227714.

[2] Alhalafi, Nawaf and Prakash Veeraraghavan. "Cybersecurity Policy Framework in Saudi Arabia: Literature Review". *Frontiers of Computer Science*, vol. 3, no. 736874, pp. 1-8. *OPAL,* doi: 10.3389/fcomp.2021.7368.

[3] Ali, Wahab. "Online and Remote Learning in Higher Education Institutes: A Necessity in light of COVID-19 Pandemic." *Higher Education Studies*, vol. 10, 2020, pp. 16-25. *ERIC,* doi: 10.5539/hes.v10n3p.

[4] Aljabri, Sultan. "Cybersecurity Awareness in Saudi Arabia." *International Journal of Research Publication and Reviews*, vol. 2, no. 2, 2021, pp. 320-30, www.ijrpr.com/uploads/V2ISSUE2/IJRPR201.pdf. Accessed 15 Dec. 2021.

[5] Al-Janabi, Samaher and Ibrahim Al-Shourbaji. "A Study of Cybersecurity Awareness in Educational Environment in the Middle East." *Journal of Information & Knowledge Management*, vol. 15, no. 1, 2016, pp. 1-30. *World Scientific,* doi: 10.1142/S0219649216500076

[6] Almarhabi, Khalid. "Adherence to ICT Security and Privacy Policies in Saudi Arabia." *International Journal of Computer Applications,* vol. 147, no. 4, August 2016, pp. 13-18. *ResearcgGate,* doi: 10.5120/ijca2016910974.

[7] Almomani, Iman et al. "Cybersecurity Maturity Assessment Framework for Higher Education Institutions in Saudi Arabia." *PeerJ Computer Science*, vol. 7, e703, 9 Sep. 2021, pp. 10-26. *PeerJ,* doi:10.7717/peerj-cs.703

[8] Alotaibi, Raed, et al. "Factors Influencing Users' Intentions to Use Mobile Government Applications in Saudi Arabia: TAM Applicability." *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 8, no. 7, 2017, pp. 200-11. *Griffith Research Online,* doi: 10.14569/IJACSA.2017.080727.

[9] Alrubaiq, Abdullah and Talal Alhrabi. "Developing a Cybersecurity Framework for e-Government Project in the Kingdom of Saudi Arabia." *Journal of Cybersecurity and Privacy*, vol. 1, 2021, pp. 302-18. *MDPI,* doi: 10.3390/jcp1020017.

[10] Alshehri, Mohammed and Drew, Steve. "Challenges of e-Government Services Adoption in Saudi Arabia from an e-Ready Citizen Perspective". *World Academy of Science, Engineering and Technology*, vol. 42, 2010, pp. 1039-45

[11] Alsulami, Majid H., Alharbi, Fawaz D., Almutairi, Hamdan M., Almutairi, Bandar S., Alotaibi, Mohammed M., Alanzi, Majdi E., Alotaibi, Khaled G., and Sultan S. Alharthi. "Measuring Awareness of Social Engineering in the Educational Sector in the Kingdom of Saudi Arabia". *Information*, vol. 12, no. 5, 2021, pp. 1-13.

[12] Alzahrani, Ahmed and Alomar, Khalid. "Information security issues and threats in Saudi Arabia: A Research Survey." *International Journal of Computer Science Issues*, vol. 13, no. 6, 2016, p. 129.

[13] Alzubaidi, Abdulaziz. "Measuring the Level of Cyber-Security Awareness for Cybercrime in Saudi Arabia". *Heliyon*, vol. 7, e06016, 2021, pp. 1-13. *ScienceDirect,* 10.1016/j.heliyon.2021.e06016.

[14] Carlton, Melissa and Levy, Yair. "Cybersecurity Skills: Foundational Theory and the Cornerstone of Advanced Persistent Threats (APTS) Mitigation." *Online Journal of Applied Knowledge Management*, vol. 5, no. 2, 2017, pp. 16-28.

[15] Chaudhry, Irfan. "#Hashtags for Change: Can Twitter Promote Social Progress in Saudi Arabia". *International Journal of Communication*, vol. 8, 2014, pp. 943–961.

[16] Faqih, Khaled. "An Empirical Analysis of Factors Predicting the Behavioural Intention to Adopt Internet Shopping Technology among Non-Shoppers in a Developing Country Context: Does Gender Matter?" *Journal of Retailing and Consumer Services*, vol. 30, 2016, pp. 140-64. *ScienceDirect,* doi: 10.1016/j.jretconser.2016.01.016.

[17] GOV.SA. "Digital Transformation." January 18, 2022, www.my.gov.sa/wps/portal/snp/aboutksa/digitaltransformation

[18] Hathaway, Melissa, Spidalieri, Francesca, and Alsowailm, Fahad. "Kingdom of Saudi Arabia: Cyber readiness at a Glance." Potomac Institute for Policy Studies, September 2017, www.belfercenter.org/sites/default/files/files/publication/cri-2.0-ksa.pdf
[19] International Telecommunication Union. *ICT Facts and Figures 2016*, 2016, www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf. Accessed 14 Dec. 2021.
[20] Ipsos. "Addressing Cybersecurity Skill Shortages in the GCC Region." March 2021, www.ipsos.com/sites/default/files/ct/news/documents/2021-09/Addressing%20Cybersecurity%20Skill%20Shortages%20in%20the%20GCC%20Region.pdf
[21] Kshetri, Nir. "Cybercrime and Cybersecurity in India: Causes, Consequences and Implications for the Future." *Crime, Law and Social Change*, vol. 66, no. 3, 2016, pp. 313-38. *SpringerLink,* doi: 10.1007/s10611-016-9629-3.
[22] Little, Arthur D. "Digital KSA: Assessment and Way Forward for the Digital Economy." Ministry of Communications and Information Technology (MCIT), August 2021, www.adlittle.nl/sites/default/files/reports/ADL_Digital_KSA.pdf
[23] Mawgoud, Ahmed A., & Taha, Mohamed H., Khalifa, Nour E., and Loey, Mohamed. "Cyber Security Risks in MENA Region: Threats, Challenges and Countermeasures." In book: Proceedings of the International Conference on Advanced Intelligent Systems and Informatics 2019 (pp.912-921), 2020, doi: 10.1007/978-3-030-31129-2_83
[24] Ng, Reuben. "Cloud Computing in Singapore: Key Drivers and Recommendations for a Smart Nation." *Politics and Governance*, vol. 6, no. 4, 2018, pp. 39-47. *Cogitatio Press,* doi: 10.17645/pag.v6i4.1757.
[25] Parmar, Sushma D. "Cybersecurity in India: An Evolving Concern for National Security." www.academicapress.com/journal/v1-1/Parmar_Cybersecurity-in-India.pdf
[26] Sagar, Ramani, et al. "Applications in Security and Evasions in Machine Learning: A Survey." *Electronics*, vol. 9, no. 1, 2020, pp. 1-42. *MDPI,* doi: 10.3390/electronics9010097
[27] Talib, Amir M., et al. "Ontology-Based Cyber Security Policy Implementation in Saudi Arabia." *Journal of Information Security*, vol. 9, 2018, pp. 315-33. *Scientific Research,* doi: 10.4236/jis.2018.94021.
[28] Zayid, Elrasheed I. M. and Nadir Abdelrahman A. F. "A study on cybercrime awareness test in Saudi Arabia - Alnamas region." *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)* (2017): 199-202.

Dr. Prakash Veeraraghavan
Assoc Prof, Comp Sci and IT, Computer Science & Information Technology

Nawaf Alhalafi PhD Student at La Trobe University, Computer Science & Information Technology Department.

List of Acronyms

The table below describes the significance of various acronyms used throughout the paper.

Acronym	Meaning
MENA	Middle East and North Africa
KSA	Kingdom of Saudi Arabia
NCA	National Cybersecurity Authority
MoI	Ministry of Interior
CERT	Computer Emergency Response Team
HIPAA	Health Insurance Portability and Accountability Act
MCIT	Ministry of Communications and Information Technology
NCSC	National Cyber Security Center
CNI	Critical National Infrastructure
NISS	National Information Security Strategy
ICT	Information and Communications Technology
IT	Information Technology