Journal of Contemporary Issues in Business and Government Vol. 29, No. 03, 2023
https://cibgp.com/

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2023.29.03.032

Contemporary Issues in business and government
ABDC AUSTRALIAN BUSINESS DEANS COUNCIL
ISSN: 1323-6903

A SYSTEMATIC LITERATURE REVIEW ON THE CYBERSECURITY GAPS IN SAUDI CURRICULUM THAT AFFECT THE BANKING SECTOR.

Dr Renu Mishra[1*], Antoine H. Hanna[2]
[1*]Assistant Professor, Gulf American University / Capital University College, UAE
[2]Antoine H. Hanna, Doctoral Candidate, Westcliff University, CA-USA

Abstract
The accessibility of top-notch cybersecurity education directly impacts knowledge of potential hazards from cyberattacks, which could raise awareness among bank employees and account holders when utilising bank applications and portals. This paper outlines a systematic literature review (SLR) of peer-reviewed conference and journal articles published from 2005 to 2022. It focuses on the role of Saudi Arabia's Vision 2030 in enhancing the educational system, the high demand for cybersecurity experts due to the country's economic transformation, and the role of universities in raising cybersecurity awareness before identifying gaps in existing research. Eighty-seven documents discussing cybersecurity in the Kingdom were found after four digital libraries were checked. The findings show that additional survey research is required to establish a theoretical knowledge of higher education's contribution to addressing cybersecurity issues in the banking industry. The three primary variables of this research (cybersecurity, education, banks) developed in this paper can serve as a guide for researchers and bank managers.

***Keywords**: Cybersecurity, Awareness, Banking Sector, Higher Education, Curriculum, Vision2030, Systems Security, Artificial Intelligence, Systematic Literature Review*

INTRODUCTION

The economy of Saudi Arabia has constantlybeen growing over the years. The increased economic activities have facilitated the growth of the banking sector (Alghazo, Kazmi & Latif, 2017). Cybercrime cases in Saudi Arabia have escalated, threatening the banking sector's growth. Saudi Arabia is the leading nation in the Middle East region that has faced numerous cyber-attacks (Singh andAlshammari, 2020). The banks in Saudi Arabia have developed a security frameworkto prevent cyber-attacks from hackers. However, the staff and customers lack information on cybersecurity, increasing the possibility of infiltration of the banks' systems through security breaches. Customers who conduct bank transactionsthrough internet banking platforms risk breaching security measures by sharing theirlogin credentials with others. The lack ofawareness or ignorance by the customers using internet banking platforms threatensthe Security of Saudi Arabia banks (Alghazo,Kazmi & Latif, 2017). The banks have implemented artificial intelligence to ensure that customers get notifications when they login into their accounts through the internetbanking platform. Machine learning technology helps banks notify customers once they log in to a different laptop or computer (Singh and Alshammari, 2020). It allows customers to validate whether theyaccess their bank accounts through such electronic devices.

Saudi Arabia is a Middle Eastern country experiencing cybersecurity issues. However, universities and other educational institutions still need to produce adequate security specialists. There has been a low percentage of women in cybersecurity positions in Saudi Arabia. Women

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2023.29.03.032

represent five per cent of thetotal cybersecurity experts in the Middle East(Malek, 2019). The low number of women cybersecurity specialists signifies that universities in Saudi Arabia must effectively produce sufficient security experts. Dr Fatmah Baothman is one of the experts in cybersecurity with advanced knowledge of artificial intelligence and lectures at King Abdul Aziz University (Malek, 2019). The increased number of students pursuing artificial intelligence will help address cyber- attacks in Saudi Arabia's banks. Universities are responsible for teaching students to acquire cybersecurity knowledge. In addition, the universities in Saudi Arabia engage in cybersecurity awareness to reduce cyber threats that affect the banking systems. The attention targets students and other society members who consistently use the internet when accessing their bank accounts.The low cybersecurity standards raised the need to establish the Prince Mohamed bin Salman College of Cybersecurity to improve education standards (Malek, 2019). The increased cyber-attacks overwhelm cybersecurity experts in Saudi Arabia, requiring an increment of security specialists. Thus, the universities in Saudi Arabia should improve cybersecurity education to increase the number of security specialists to serve inthe banking sector.

Saudi Arabia intends to become one of the global economic hub countries. Developing an economic hub requires adequate skilled labour to work in rapidly growing economic sectors. The financial industry plays a significant role in supporting the expansion of all economic sectors (Riegger et al., 2021). The increased economic growth has attracted many cyber-attacks in the Saudi Arabian banking sector that could undermine the financial support necessary to spur further economic activities. The banks can avert cyber-attacks through increased cybersecurity awareness in the education curriculum (HKA, 2021).

Cybersecurity encourages national security that maintains the stability of nations. Common cyber threats include phishing and social engineering that intend to cause financial losses and dent the reputation of Saudi Arabian banks (Slavchev, 2021). Developing a cybersecurity framework is vital in addressing cyber threats in Saudi Arabia. Vision 2030 acts as an umbrella for economic and educational changes as it focuses on improving curriculum to increase the labour force in private institutions. An advanced curriculum dramatically contributes to increasing cybersecurity awareness among banking employees in Saudi Arabia (Chaudhry, Aniol and Shegos, 2020).

This section focuses on a deep understanding of cybersecurity in Saudi Arabia, focusing significantly on its banking sector. In addition, it analyses the level of cybersecurity awareness exhibited by Saudi Arabian University students. Finally, there is a critical analysis of national cybersecurity programs and initiatives intended to improve cyberspace in the Kingdom. The cybersecurity programs are achievable by developing commissions that aim to improve the Saudi Arabian global cybersecurity index.Saudi Arabian universities should offer cybersecurity to increase the population of cybersecurity specialists (Latifi, 2020). In essence, the literature work intends to improve cybersecurity awareness among professionals working in the growing Saudi Arabian banking industry.

PROBLEM STATEMENT

Banks in Saudi Arabia have been facing cybersecurity issues. As a result, cybercrimes have made banks lose finances (Alqurashi, 2020). The problem is attributable to the lack of highly competent cybersecurity experts. In addition, the banks' employees and customers lack awareness of cybersecurity matters.

Hence, the banking sector in Saudi Arabia aims at being free from cyber threats. Phishing and social engineering are majorcyber threats affecting the banking sector in Saudi Arabia because of online banking. Phishing involves convincing hackers to share passwords and PINs that help hackers to access bank accounts (Malek, 2019). Hackers usually require information regarding debit

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2023.29.03.032

and credit cards to facilitate online transactions. Educated and non- educated bank account holders are highly vulnerable to phishing attacks as they lack cybersecurity knowledge to avoid cyber-attacks. Phishing dents the banking sector's image as account holders question the security of banks' finances. Social engineering involves using account users to share their bank details to obtain financial favour such as lottery money (Alqurashi, 2020). Victims usually expect funds toreceive money in their accounts. However, the hackers use the shared confidentialinformation to defraud their accounts. The universities in Saudi Arabia, government cybersecurity agencies, and banks collaborate to increase awareness of the best online banking practices that reduce phishingand social engineering attacks. The bank account holders should always have secure, complex login passwords that assure cybersecurity. Personal computers should have updated operating systems to protect hackers from infringing internet banking security. The combination of upper, lower, and unique case letters helps to assure password security to protect internet banking. The complex passwords ensure the safety of the bank systems. The universities in Saudi Arabia engage in cybersecurity awarenessduring open days. The understanding alsodemonstrates the risk of sharing their debit and credit card information. Cybersecuritystudents in universities in Saudi Arabia should develop antivirus software to promote the security of personal computers (Aljohni et al., 2021). Therefore, the universities in SaudiArabia and government agencies should increase cybersecurity awareness to protect banks from phishing and social engineering.

Regulations will require financialorganisations in Saudi Arabia to keep up withcybersecurity trends and new dangers. For several years now, ransomware has been a massive nuisance for businesses all over the globe, and it does not seem that this willchange anytime soon. Banking corporations hit by ransomware attacks may experience prolonged system crippling, especially if theydo not have backups. Cloud-based assaults have increased as more software systems anddata are being hosted there, a trend that has attracted hackers. Banks must ensure that thecloud infrastructure is set up appropriately to prevent damaging attacks. Social engineering is one of the greatest dangers to banking andfinance. Customers are often the weakest linkin the security chain since they may be dupedinto providing essential information and login credentials.

PURPOSE OF THE STUDY

The study aims to create awareness of the cybersecurity issues affecting Saudi Arabian banks (Alzubaidi, 2021). It will highlight common cyber-attacks, such as phishing andmalware, that compromise the security features implemented in the banks (Alzubaidi, 2021). In addition, the study intends to educate the banks' employees on the importance of adhering to cybersecurity measures to protect the financial banks in Saudi Arabia from losing their finances. Moreover, the customers will be enlightenedon safe access to their bank accounts to avoidexposing the bank systems to cyber threats (Alghazo, Kazmi & Latif, 2017). The study will seek information from cybersecurity experts and cybersecurity tutors in Saudi Arabia to identify the cyber-attacks and the best strategies to counter them. In addition, itwill highlight the application of machine learning and artificial intelligence technologies in promoting cybersecurity in the banking sector in Saudi Arabia. The research will recommend the best security features installed in banking systems to avoid cyber threats (Singh and Alshammari, 2020).It will encourage the security of networks to promote the bank's reputation due to third- party members' lack of access to customer data.

University students are major internet users and often engage in online banking. The universities in Saudi Arabia should encourage cybersecurity awareness to ensurestudents do not become victims when transacting online using bank products such as debit and credit cards (Aljohni et al., 2021). The students will learn to access their bank accounts using personal computers securely. The universities in Saudi Arabiawill educate on antivirus software installed into private computers to ensure cybersecurity in online banking. The banks will consider hiring competent security

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2023.29.03.032

specialists to protect the banking systems.The increased awareness among university students will help improve cybersecurity for many people as they will educate their peers and family members to protect banks from cyber threats. Family members and peers arebank account holders and will not become cyber victims. The universities will improve the curriculum by including cybersecurity courses. To ensure information security, the students will not become vulnerable to phishing and social engineering attacks. In addition, Saudi Arabia's universities will demystify the cultural practices that create cybersecurity ignorance (Aljohni et al., 2021). Therefore, higher education students will be aware of cybersecurity to protect banks from attacks.

The primary purpose of the research is to understand how to create or raise awareness against cybersecurity breaches in banking through increasing knowledge and learning in Saudi universities, which can bridge the gap in the banking industry. The research will utilise secondary methods to obtain adequateinformation regarding possible data breaches.The study shall use questionnaires that help provide feedback regarding matters of concern for cybersecurity in banks. Cybersecurity's primary focus is to protect internet-connected systems from threats that risk customers' and banks' finances from malware. Due to increased technological development, taking security measures through artificial intelligence requires adequate knowledge regarding the vulnerabilities of banking services that cyber attackers may utilise. Universities play a crucial role in educating students about the matter in the real world. Increasing the knowledge in the country's higher education systems will give the students the expertise necessary to counter any malware that may compromise banking safety, especially when using online services. Hence, the study aims to enable increased awareness against cybersecurity breaches in banking using secondary research through knowledge acquired in machine learning in highereducation among university students in SaudiArabia to bridge the gap in the banking industry.

Furthermore, the study shall highlight theapplication of machine learning and artificialintelligence by indicating how machine learning facilitates the effective prediction ofoutcomes. The study will encourage machinelearning to increase network security and promote banks' reputations. Machine learning in levels more explicit programmingthrough accurate forecast buy software applications. In managerial aspects, machinelearning facilitates the combination of large sets of data and enables high computing power to understand patterns and relationships of particular algorithmseffectively. The study will also increase awareness among the staff to mobilise customers through advertisements that help them learn how to protect their accounts. The research can help bridge the banking servicesgap by finding significant cybersecurityconcerns for banks. As a result, the study willhighlight the application of machine learningin artificial intelligence, which will encourage the banking systems to secure their finances through appropriate soft wares, promoting a better reputation for Saudi banks.

THEORETICAL FRAMEWORK

The Saudi government created programs to advance cybersecurity. It established the Communications and Information Technology Commission (CITC) to develop guidelines for advancing cybersecurity and information technology. The commission is also in charge of licensing IT businesses in Saudi Arabia. Additionally, CITC advocates for greater business use of IT services. (Quadri and Khan, 2019). Internet usage is correlated with a rise in IT services. As a result, CITC supports Saudi Arabia's efforts to strengthen cybersecurity. To boost cybersecurity, Vision 2030 asked the ministry of education to involve Saudi Arabian universities. Protecting the complete IT infrastructure, including all applications, systems, software, hardware, and data, helps to reduce cyber risk. At King Saud University, the Centre of Excellence in Information Assurance, known as CoEIA,provides cybersecurity solutions. (Aljohni etal., 2021). King Saud University and CoEIA collaborate to take part in cyber awareness activities. To address cybersecurity issues, including

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2023.29.03.032

Network Security and Security Governance, King Abdulaziz City for Science and Technology (KACST) cooperates with the National Centre for Cybersecurity Technology. (Alghazo, Kazmi & Latif, 2017). Colleges are invited to participate in the commission established by the Kingdom of Saudi Arabia to further cybersecurity research. The Saudi Arabian Monetary Authority (Sama) changed its name to Saudi Central Bank in 2020. (S.C.B.) formally built under Vision 2030's specifications. SCB urged that all financial sector organisations (banks and private businesses) implement cybersecurity standards and work with the education sector to advance cybersecurity expertise among ITstaff. On December 4, 2021, taxpayers must use the electronic invoicing system. To meet cybersecurity requirements, all organisations must update their systems. (zatca.gov.sa, 2017).

Beginning in 2024, Saudi Arabia will not execute contracts with foreign businesses unless its regional headquarters are established in Riyadh city, the capital of KSA (Halse, 2021). The decision intends to encourage foreign companies with the Saudi government to set up shops in the Kingdom. Agencies, institutions, and government- owned money will be subject to the rule. Additionally, it will guarantee that most of the goods and services that the government agencies buy come from the Kingdom, boost expenditure efficiency, and create jobs. The action follows Saudi Arabia's announcementof a strategic strategy to elevate Riyadh'seconomy to among the top ten cities in the world during the Future Investment Initiative (FII). According to the statement, the new decision will not hinder any investor's capacity to enter the Saudi market or carry onwith their private-sector operation. Still, this decision requires the data related to the businesses to be well secured with a robust cybersecurity infrastructure while connecting headquarters in Saudi Arabia with regional offices and when transactions and correspondences are made with the main offices in the mother countries.

Due to the rise of cyberattacks in the banking sector in Saudi Arabia (Saudigazette, 2022), new security and privacy information are needed to adapt to the evolving safety and privacy standards in the banks, which can be spread through education to improve awareness campaigns. Public organisational security policies capture security and privacyas good practice.' However, publishing a security policy only ensures that the person will act according to what it prescribes because some will resist such instructions. Thus, they must be made aware of its existence and the behaviours it defines. Usually, education programs are used to transfer this kind of knowledge to employees.These training programs try to alter employeebehaviour by teaching them about secure security procedures. (Bauer, Bernroider and Chudzikowski, 2017). However, security and privacy risks cannot be eliminated (Flowerday and von Solms, 2005). A well- planned security educational program may help lessen the risk to acceptable levels. Organisations anticipate that certain behaviours will become the norm afterimplementing measures for education and awareness (Goo, Yim and Kim, 2014).

Improving industries like ICT, hospitality,tourism, healthcare, and finance is necessary.Expanded IT infrastructure susceptible to cyber threats will be needed to develop othersectors to realise Saudi Vision 2030. (Alghazo, Kazmi & Latif, 2017). The Saudi Vision 2030 targets 90 per cent of all households to access high-speed internet (Quadri and Khan, 2019). However, access to unsafe websites puts the financial industry's cybersecurity at risk, increasing vulnerabilityto hacking. To help realise the aim, the National Authority for Cybersecurity (NCA) wants to encourage cybersecuritybreakthroughs (Quadri & Khan, 2019). As a result, Saudi Vision 2030 would promote strengthening the infrastructure for cybersecurity. In Saudi Arabia, the adoption and penetration of information technologyhave increased. Information technology is used in education, healthcare, and retail settings. According to CITC, between 2007 and 2009, Saudi Arabia's computer penetration increased by 8%. (Alzubaidi, 2021). IT penetration has reduced communication costs to facilitate smooth business operations. To raise the cybersecurity index, Saudi Arabia has also invested

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2023.29.03.032

significantly in information technology-enabled services (ITES) (Quadri & Khan, 2019). Saudi Arabia has a high rateof both individual and commercial computerpenetration.

LITERATURE FINDINGS

Cybersecurity Definitions

Cybersecurity protects computerised systems and data from being accessed by unauthorised individuals who can commit cyber-attacks. It promotes the confidentiality and integrity of data. Cybersecurity helps

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2023.29.03.032

manage cyber espionage, cyber warfare, and cyber-terrorism threats. Cyber-warfare involves a country with high-tech experts who penetrate the systems of other countries to acquire confidential information. Cyberterrorism is whereby terrorist groups commit cybercrimes for political purposes, such as demonstrating their strength and organisation (Seemma et al., 2018). On the other hand, cyber espionage is the secret obtaining of information by hackers through information technology.

Cybercriminals access data and computer systems without authority from relevant organisations. They can obtain credit card details for financial fraud, defame individuals to lower self-esteem, and ignore copyright licenses (Seemma et al., 2018). Cybercrimes happen due to competition, revenge, politicalinfluence, and financial gains. Organisationsuse end-user protection over cyber-attacksfrom cyber criminals.

Ransomware, malware, social engineering, and phishing are different cyber threats. Phishing uses emails by cybercriminals that appear to be from reliable and reputable organisations that help them access passwords and login details, while social engineering is whereby hackers trick computer users into sharing their passwords and other information willingly with them.

Malware uses harmful files such as Trojan horses and worm viruses to damage computers to allow easy access by cybercriminals. GeeksforGeeks states that a computer virus is a computer program that connects to another program to harm a computer system. Worms replicate themselves to cause slow down the computer system. Trojan Horse, rather than duplicating, captures essential information about a computer system or network. Finally, ransomware is where hackers lock an organisation's computer systems and ask for financial resources to help unlock them (Seemma et al., 2018). Thus, cyber threats such as phishing, social engineering, and ransomware commit computer crimes.

The Importance of Cybersecurity for aModern-Day Society

Cybersecurity is the leading global problem. Institutions have huge expenditures in safeguarding their financial resources because of increased cybercrimes. Climate change, income inequality, and infectious pandemics have a lower economic impact than cybersecurity (Lynch, 2021). The Convention on Cybercrime, supported by over sixty-five countries, discourages cyber warfare whereby high-tech governments infiltrate into the systems of nations with little knowledge of IT security (Lynch, 2021). Therefore, the convention recommends the establishment of legal institutions to solve cybercrimes.

Cybersecurity is essential in national security as it solves economic challenges in world politics. China, the United States of America, and Russia pay great attention to cybersecurity. The United States of America embraced cybersecurity in its efforts to revolutionise the military department in 1991(Tsakanyan, 2017). The federal government ensures the use of cybersecurity for economic and national security prosperity. The Federal Bureau of Investigation (FBI) aims at improving cyberspace by analysing crime groups, state sponsors, and terrorist groups to ensure data protection (Tsakanyan, 2017). The US Department of Defense (DoD) defends cybersecurity against insiders, foreign governments, and criminal groups. In addition, cybersecurity provides excellent operations in the healthcare, financial, energy, telecommunications, and transport sectors.

China protects its cyberspace from software made by foreign IT experts. The Chinese government committed to cybersecurity infrastructure by establishing Central Cybersecurity and Informatization Leading Group in 2014 (Tsakanyan, 2017). It has strict regulations on the IT services offered to China to avoid weakening the local cybersecurity infrastructure. On the other hand, the Russian Federation promotes cybersecurity through the defence and information security ministry to spur the nation's economic prosperity (Tsakanyan, 2017). Thus, the Chinese, Russian and Federal governments ensure cybersecurity for financial and national security purposes.

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2023.29.03.032

Insurance companies offer cyber insurance policies to manage cybercrimes that face organisations. The increased cyber insurance premiums indicate that private institutions commit to improving cyberspace. The commercial incentive structure inspires private organisations to secure insurance policies as a cyber-risk management strategythat enables businesses to minimise financialloss risks (Levite, Kannry and Hoffman, 2018). Insurance companies offer cyber insurance coverage to companies that pay premiums to compensate a few businesses that face cybercrimes. In addition, leading insurers offer cybersecurity advice to reduce the occurrence of cybercrimes in institutions (Levite, Kannry and Hoffman, 2018). Therefore, insurers ensure cyber risk management in organisations to avoid high compensation claims related to cyber-attacks.

Cyber insurance ensures data protection and averts financial loss to organisations. Data protection ensures that hackers do not get sensitive information that can infiltrate information systems. System penetrationfacilitates the occurrence of cyber-attacks in that cybercriminals solicit financial resources from organisation owners (Levite, Kannry and Hoffman, 2018). Therefore, insurers encourage organisations to protect sensitive data.

Insurers share the best cybersecurity practices to eliminate the occurrence of cyber risks. Cloud computing and machine learning technologies could manage cyber risks (Levite, Kannry and Hoffman, 2018). Cloud computing protects against data loss for businesses. The quantification allows the insurance company to create an expected total claim costs pool once the risks occur (Levite, Kannry and Hoffman, 2018). Diversifying investment opportunities makes organisations incur a less financial loss in case of cyber risks. In addition, cybersecurityprograms minimise cyber threats because individuals have high cyber awareness (Levite, Kannry and Hoffman, 2018). Therefore, the implementation of security technologies reduces claim cases for insurers.

Cyber threats affect all economic sectors, including health care, education, manufacturing, hospitality, and finance. Overforty per cent of Small and Micro Enterprises (SMEs) were likely to collapse by 2017 (Benson, 2017). Organisations with more than ten thousand workers have a higher riskof cybersecurity threats than those with few workers. Organisations have a limited number of cybersecurity specialists, making them vulnerable to cyber threats. WannaCry Ransomware interfered with ICT systems installed in government institutions, finance, and health care. In addition, cybersecurityissues undermined the general elections in theUnited Kingdom, the USA, and France (Benson, 2017).

Furthermore, The public sector has a higher possibility of experiencing cyber threats thanprivate institutions because of many incidences of privilege misuse. Payment cardhackers target the retail and financial- economic sectors to defraud them. Increasedcyber espionage between 2016 and 2017 targeted the manufacturing sector globally. The occurrence of cybercrimes in the manufacturing industry reduces the ability ofcompanies to expand, which would have created more employment opportunities. Privilege errors in the medical sector make itpossible for healthcare facilities to lose vital data. The increased internet usage in accessing websites escalated the number of cyber threats because of the outdated operating systems in personal computers. Study shows that employees can access oversix hundred websites in a day increases the likelihood of facing cyber viruses (Benson, 2017). The social engineering attacksaffected internet service companies such as Reddit and Netflix with originality in theUSA and European nations (Benson, 2017). Mobile malware has escalated on the African continent because of increased internet penetration. The organisational management advocates hiring highly competent ITsecurity experts to build robust cyberspace that protects data and avoids financial losses in businesses. Therefore, all economic sectors should have a strong cybersecurity infrastructure to minimise cyber-attacks.

Cybersecurity is essential in avoiding financial loss for organisations. For instance, expected cybercrime costs for 2022 are six trillion American dollars (Yang, 2022). Despite increased efforts to counter cyber threats, hackers have employed technologically advanced techniques to commit

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2023.29.03.032

digital fraud. Hackers use social media accounts to commit identity theft and credit card fraud. Cloud storage solutionsensure the safety of sensitive information such as account details for bank customers and payment cards such as debit and credit ones. Hackers have even embraced artificial intelligence to conduct cybercrimes that outcompete cyber protection measures. However, the formulation of solid cybersecurity policies and end-encryptedauthentication strategies counters the risk of a cyber-attack.

Furthermore, the ad-blocking apps ensure that hackers do not share worms or viruses through ads to infiltrate websites and mobileapps. Yang (2022) states that best cybersecurity practices include data encryption, providing cyber training to workers, having secure browser extensions, and constantly updating the software and operating systems. In addition, protecting confidential data and passwords makes it difficult for cybercriminals to infiltrate the ICT systems of organisations (Yang, 2022). Avoiding password sharing ensures that individuals are not easily defrauded on online platforms. Therefore, organisations avertfinancial loss through safe cybersecurity practices such as using social media accounts, data encryption, avoiding passwordsharing, and ad-blocking apps.

The Saudi Vision 2030 and the Role ofTechnology in it

Prince Mohammad bin Salman launched Saudi Vision 2030 in 2016 to ensure thegrowth of the Saudi Arabian economy in all economic sectors, such as tourism, health care, education, and finance (Kosárová, 2020). Saudi Arabia's Vision 2030 targetsdiversifying the economy to reduce dependence on petroleum products and generate development revenue. Thediversified economy will address the frequentdrop in oil prices and increases in the population of Saudi Arabia. The cost of the oil barrel declined from one hundred andfifteen American dollars to forty American dollars during 2014-2015 (Kosárová, 2020). The price decline meant a financing problemfor the financial budget.

Furthermore, the Saudi Arabian 2016population data revealed that the nation had around seventy per cent of its citizens aged below thirty years. In addition, fifty per cent of the projected Saudi Arabian population by 2030 is most likely to be young people aged below twenty-five years (Kosárová, 2020). The growing number of young adults necessitates the Saudi Arabian government todiversify the economy under the Vision 2030plan. Therefore, fluctuations in oil prices andthe increasing population in Saudi Arabiapushed for the establishment of Vision 2030.

The Saudi Vision 2030 targets to spur the economy through the private sector to realisesixty per cent of the country's total Gross Domestic Product (GDP). The Saudi Arabiangovernment intends to increase tourism to ensure that over thirty million pilgrims visit the country for prayers (Kosárová, 2020). In addition, female tourists should dressmodestly instead of wearing Abaya. Second,Saudi Arabian government will reduce regulations to allow many private investors toventure into health care, air travel, and real estate businesses. The growth in private investment will attract more foreign entrepreneurs to promote GDP growth byseven per cent (Kosárová, 2020). In addition, the Saudi Arabian government intends to have women occupy more than thirty per centof the available employment opportunities (Kosárová, 2020). Vision 2030 targets organising regular cultural festivals whereby the world will appreciate the Saudi Arabian culture. Therefore, the increased privatesector involvement will promote GDP growth in Saudi Arabian economy.

The Saudi Arabia Vision 2030 effectivelymanages robust ICT infrastructure through the National Transformation Program (NTP). The Improved ICT infrastructure targets to support private investors in establishingprofitable business ventures that cause positive growth in the nation's GDP. TheSaudi Arabia government establishedNational Authority for Cybersecurity (NCA)in 2017 to ensure the country is free from cyber-attacks (Quadri & Khan, 2019). NCA supports private and public organisations to grow to create employment for the growing young population in Saudi Arabia. In addition, NCA intends to encourage innovation to increase the nation's GDP. NCA was

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2023.29.03.032

established due to increased ransomware attacks targeting government entities in Saudi Arabia in 2016 (Quadri and Khan, 2019). NCA is mandated to formulateand implement cybersecurity policies that protect business ventures in Saudi Arabia. It ensures that organisations have technical assistance when installing the ICT infrastructure. The Saudi Vision 2030 provides that the manufacturing sector implements the Internet of Things (IoT) to increase production levels. In addition, NTP ensures that Saudi Arabian government has digitised payment systems that increase the collection of customs (Woishi, 2019). The Saudi Arabian legal systems have digitised records that require high protection through quality cybersecurity infrastructure. The lackof cybersecurity in legal systems could modify the presented evidence to change the final judgment (Woishi, 2019). NCA ensures a digital strategy that supports the timely payment of pension benefits to elderly members of the Saudi Arabian community. Therefore, NTP provides high-level security in manufacturing, taxation, pension, and legal systems to promote public and private sectors to help achieve Vision 2030 goals.

The significance of having a well-establishedcybersecurity infrastructure matches highly accessible internet speed under SaudiArabia's Vision 2030. Improved cybersecurity infrastructure is essential to Saudi Arabia's developing tourism, financial, and healthcare sectors. Vision 2030 intends to transform Saudi Arabia into a global economic hub that relies a little on petroleum. National Cybersecurity Authority (NCA) aims to create a robust cybersecurity infrastructure that attracts foreign investmentto spur the gross domestic product (GDP) of Saudi Arabia (Quadri and Khan, 2019). Cybersecurity ensures that investors do not lose the capital to start or expand businesses.The higher cybersecurity index ranking instils faith in entrepreneurs that systems installed in their business ventures will not bevulnerable to cyber-attacks. Therefore, cybersecurity will facilitate the realisation of Saudi Vision 2030 in economic success.

Internet banking increases the vulnerability of the Saudi Arabian banking systems; this could impact Vision 2030 in the financial sector. Account holders often log out after using the internet banking platform or download documents from unsecured websites, increasing the chances of getting the account credentials (Alghazo, Kazmi & Latif, 2017). Moreover, most account holders neglect password management strategies by sharing confidential pins. University studentsin Saudi Arabia face cybersecurity vulnerabilities due to access to internet services (Aljohni et al., 2021). Cyber- criminals place malware on often-visited websites where they steal students' data. The identification of possible cyber-attacks helpsreduce the banking system's vulnerability.High internet penetration increases cybersecurity vulnerabilities globally, affecting Saudi Arabia. Over sixty million cybercrimes got recorded in Saudi Arabia in 2015 (Singh and Alshammari, 2020). Thus, internet banking and unsafe internet usage increase the cyber-attacks on the banking systems in Saudi Arabia.

National Cybersecurity Programs andInitiatives in Saudi Arabia

The leadership of KSA has already established commissions that supportcybersecurity programs to build safe cyberspace. Computer Emergency ResponseTeam (CERT) ensures that organisations gain cybersecurity awareness to prevent and identify cyber threats (Quadri and Khan, 2019). Another commission is the Centre of Excellence in Information Assurance(CoEIA) provides cybersecurity solutions to private and public institutions to ensure innovative strategies in cyber risk management. National Cybersecurity Center(NCSC) assesses the cybersecurity levels by focusing on the observation of international cyber laws and policies. National Center for Cybersecurity Technology works with King Abdulaziz City for Science and Technology (KACST) to investigate additional IT security in the country (Quadri and Khan, 2019). Implementing a new digitalised system would increase output and reduce shadow costs (Nahas, 2022), but the newsecurity criteria should protect thisimplementation. Saudi Arabian Federationfor Cybersecurity, Programming, and

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2023.29.03.032

Drones (SAFCSPD) encourages establishing skilled cybersecurity professionals who promote innovation in domain technology. In addition, it will increase the number of specialists in programming and drone usage in the Kingdom of Saudi Arabia (Quadri andKhan, 2019). Therefore, cybersecurity programs and initiatives target building resilient cybersecurity in Saudi Arabia.

Cybersecurity Strategy of KSA.

The increasing number of cyber-attacks in Saudi Arabia pushed for establishment of the National Cybersecurity Authority (NCA). The Saudi Arabian cybersecurity strategy aims to provide legal solutions that regulate and increase the efficiencies of the entities. The President of State Security is in charge ofNCA and works with officers from the ministries of defence and internal affairs (Olech, 2021). NCA's strategy focuses on sixaspects: risk management, optimal functioning, harmonisation, robust security, international partnership, and cyberspace development. Risk management protects cyberspace from damage to prevent private and public entities from data breaches and financial losses. Harmonisation ensures coordinated approaches to cybersecurity standards and compliance.

Furthermore, the international partnership facilitates the exchange of advanced technologies that improve the systems and security levels. NCA achieves cyberspace development through quality education, training, and intensive research. It has accelerated data storage and artificial intelligence efforts by establishing the Saudi Data and Artificial Intelligence Authority (SDAIA) (Olech, 2021). Therefore, NCA embraces innovation to improve KSA's national cybersecurity.

Saudi Arabia Cybersecurity Rankings

The cybersecurity rankings of the KSA have improved since the creation of the NCA. The Global Cybersecurity Index 2020 results ranked Saudi Arabia in second position. Saudi Arabia occupied the 46th position in 2017 (Devi, 2021). However, in 2018, Saudi Arabia ranked 52nd position globally interms of cybersecurity (Quadri and Khan, 2019). The rise in the global security ranks is attributable to the significance of the NCA inpromoting cybersecurity in the Kingdom. The NCA administration appreciated the governmental support in regulation and legislation that ensured a high compliance rate with cybersecurity policies and guidelines (Devi, 2021). Thus, NCA promotes cybersecurity in KSA's globalcybersecurity rankings.

Cybersecurity in Finance Sector: Saudi Arabian Banking Sector

Finance industry companies highly use technological systems for operational efficiencies. The finance sector comprises banks, credit cards, investment, and credit unions. Financial institutions often have customers' details such as phone numbers, homes, and email addresses that attract the attention of cybercriminals, as they can use such sensitive information to commit cyber fraud (Cybersecurity Guide, 2021). The global finance sector had a market value of twenty-two trillion American dollars as of 2019 (Cybersecurity Guide, 2021). The finance sector uses technological systems to support internet banking and non-cash payments. Over the years, the financial industry has grown due to increased non-cashcharges attributable to high internet penetration in third-world countries (Cybersecurity Guide, 2021). In addition, digital payments are high because of the increased usage of mobile phones. However,technological systems have vulnerabilities that increase the risk of cyber-attacks. Therefore, technology contributes to financial institutions encountering cyber-attacks.

Financial institutions can reduce cybersecurity risk by employing qualified security professionals and ensuring the effective implementation of cybersecurity policies. The financial sector's demand for cybersecurity professionals increases as institutions protects their clients' data (Cybersecurity Guide, 2021). Financial institutions require adequate security professionals to maintain high vigilance against cyber threats. In addition, cybersecurity experts constantly update the finance companies' management on the new cybersecurity trends to increase awarenessefforts. Furthermore,

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2023.29.03.032

they help formulate cybersecurity rules to improve IT security infinancial companies. Data breaches cause considerable losses to the financial sector.

For instance, in the 2019 IBM Security According to the Cost of a Data Breach Report, financial institutions suffered losses of USD 5,860,000 for each security breach. (Cybersecurity Guide, 2021). Thus, competent cybersecurity experts and adopting IT security policies help finance companies avoid financial losses.

The banking sector in Saudi Arabia abides by cybersecurity regulations set by the Saudi Arabian Monetary Authority (SAMA). The Saudi Arabia banks adopted the cybersecurity framework developed by the SAMA that comprises effective leadership and governance, adhering to risk management and compliance policies, efficient operations and technology, and highvigilance when hiring third parties (O'Connell, 2018). The Saudi Arabian banking sector leaders should create cybersecurity departments within their institutions. The cybersecurity departments are responsible for developing cybersecurity documents that ensure every employee has IT security knowledge. In addition, the banking sector leaders should allocate sufficient financial resources to create cybersecurity awareness among all staff and account holders. The cybersecurity departments can collaborate with human resource officials to train employees on current cybersecurity trends. The Saudi Arabian banks adopt cyberrisk management strategies of local and international standards to safeguard their information assets. The compliance with cybersecurity policies set by SAMA ensures that banks avert cyber-attacks that could dent their reputation. Risk management also involves identifying possible cyber-attacks and developing the best strategies to counter them. In addition, bank employees get information on how to report cyber-attacks once they identify them (O'Connell, 2018). In Saudi Arabian banks, efficient operations and technology involved protecting data centres and rooms through CCTV surveillance cameras and controlled access. Saudi Arabian banks highly protect their wireless networks and servers and constantly update the operating systems of the computers used by their workers. In addition, banking IT experts ensure maximum databases and firewall protection to prevent cybercriminals from accessing sensitive information (O'Connell, 2018). The Saudi Arabian banks work with third parties, such as cloud computing and technology vendors, to improve operational efficiencies. They have high vigilance when outsourcing their services to avoid exposing their systems to unauthorised parties who canundermine data integrity. Thus, the Saudi Arabian banking sector follows the SAMA *cybersecurity framework to avert cyber- attacks.*

The Scenario of the Banking Industry in Cybersecurity

The Saudi Arabian education curriculum focuses on memorisation and increasing religious knowledge. It, therefore, poses challenges to managing cybersecurity risks. Saudi Arabian high school students post lowmathematics, science, and reading scores (Kosárová, 2020). TIMMS 2015 examination results demonstrated that Saudi elementary and high school students have little knowledge of mathematics and sciences, as they posted the lowest scores (Kosárová, 2020). The poor education system in Saudi Arabia has pushed private-sector companies to hire foreign workers to execute various functions. In addition, it contributes to Saudi Arabian banks having few cybersecurity specialists (Kosárová, 2020). The shortage ofsecurity professionals limits the ability of the Saudi Arabian banking sector to manage cyber threats effectively. The curriculum improvement by Saudi Vision 2030 will helpincrease technical know-how incybersecurity matters. Therefore, the Saudi Arabian banking sector can address cyberthreats by adopting a cybersecurity curriculum that provides detailed informationon mathematical and scientific concepts.

Cybersecurity awareness among Saudi Arabia nationals depends on their education levels. The

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2023.29.03.032

individuals who have attained postgraduate and undergraduate levels of education have higher cybersecurity knowledge than students in elementary and secondary schools (Alzubaidi, 2021). Highereducation levels expose individuals to cybersecurity practices that increase their IT security information. Education status helps people to access information through the internet that helps to further their cybersecurity knowledge (Alzubaidi, 2021). Educated people learn through online platforms that guide safe cybersecurity practices by installing antiviruses on computers, avoiding emails from suspicious sources, updating software regularly, and keeping password information confidential. Cybersecurity awareness reduces the possibility of individuals being cybercrime victims (Alzubaidi, 2021). Therefore, improved cybersecurity knowledge ensures that account holders and employees do not increase vulnerabilities in the banking systems.

Saudi Federation for Cybersecurity, Programming, and Drones (SAFCPD) promotes cybersecurity education to protect banks from losing funds. However, like othercountries, Saudi Arabia has few cybersecurity specialists who concentrate on the firm's daily operations (HKA, 2021). Thus, the inadequate supply of cybersecuritypushes Saudi Arabian banks to outsource cybersecurity services, which could lead to data breaches and financial losses.

Cybersecurity in other Economic Sectors apart from Banking Industry

Apart from the banking industry, the energy and healthcare sectors in Saudi Arabia have faced cybersecurity issues. For example, the Shamoon virus inconvenienced the functionality of over thirty thousand computers in the Saudi Aramco company thatran on the Windows operating system in 2012 (Dawson, 2022). Saudi Aramco is an energy sector company that deals with petroleum and national gas production and distribution in Saudi Arabia and the global market. The Shamoon virus attack leaked Saudi Aramco data on drilling and supply chain strategies that are vital in the highly competitive global oil market (Dawson, 2022). However, this cyber-attack did not stop drilling or cause oilspillage.

On the other hand, the healthcare sector in KSA faced a Denial of Service (DoS) attack in 2018. The ministry of health website was not functional due to a DOS attack. As a result, it remained inaccessible to all individuals for hours on that day (Dawson, 2022). In addition, the DoS attack inconvenienced the health care operations. Therefore, the Shamoon virus and DoS attackdenied the process of energy and healthcare activities, respectively.

Cybersecurity Awareness amongSaudi Arabian University Students

Saudi Arabian university learners have average cybersecurity awareness. Female students were more concerned about understanding cybersecurity concepts than their male counterparts (Aljohni et al., 2021). University students highly use the internet and should have cybersecurity awareness to avert malicious cyber-attacks (Aljohni et al., 2021). The students studying in universities based in rural settings had lower knowledge of cybersecurity matters than those in urban environments. In addition, students pursuingcomputer or information technology courses had a higher understanding of cybersecurity than their schoolmates pursuing other undergraduate programs (Aljohni et al., 2021). Thus, universities should establish a cybersecurity awareness culture for all Saudi Arabian students.

Most Saudi Arabian university students are unfamiliar with phishing and social engineering attacks. On the other hand, computer science students have a basic understanding of cybersecurity (Elnaim and Al-Lami, 2017). The lack of knowledge on phishing and social engineering attacks makes Saudi Arabian university students vulnerable to cyber-attacks as they browse the internet. In addition, Saudi Arabian university students need more information onthe safe websites they can use to access data (Elnaim and Al-Lami, 2017). Therefore, Saudi Arabian universities are responsible for providing cybersecurity education to allstudents to avoid phishing and social engineering attacks.

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2023.29.03.032

Cybersecurity Awareness amongBanking Staff

The Saudi Arabian banking staff has low cybersecurity awareness. The banking staff does not educate account holders on safeinternet banking usage, making the banking systems vulnerable to phishing and social engineering attacks (Alghazo, Kazmi & Latif, 2017). Thus, the banking staff needs to educate on safe internet banking usage. In addition, the banking staff needs to educate internet banking users on the need to constantly update their personal computers' operating systems and secure websites. Inaddition, they need to educate accountholders on the importance of regularly changing their internet banking passwords to enhance their accounts' security. Furthermore, clients need information on maintaining a high confidentiality level of their internet banking passwords to avoid social engineering attacks (Alghazo, Kazmi & Latif, 2017).

The banking staff comes from Saudi Arabian universities as IT and Non-IT students with little cybersecurity knowledge. As a result, they are vulnerable to unsafe internet usage, increasing the vulnerability of banking systems by accessing dangerous websites where hackers could have worms or viruses that damage the computers (Garba et al., 2021). In addition, they cannot differentiate phishing emails from those from reputable management officials, making it easy for cybercriminals to access their login details. Hackers can, therefore, comfortably infiltratethe banking systems, steal sensitive data, or commit financial fraud that causes the banks to lose financial resources. In addition, they need to educate account holders on the importance of keeping their debit cards away from others who can use them for illegalonline transactions (Garba et al., 2021). Thus,the banking staff lacks cybersecurity knowledge due to failure to get general IT security education.

The lack of cybersecurity knowledge makes the banking staff highly vulnerable to phishing attacks. Spear-phishing involves hackers sharing viruses through email addresses targeting the banking staff. Once the bank staff clicks or opens such emails, they are exposed to the sensitive informationneeded by cybercriminals to infiltratebanking systems (Aljeaid et al., 2020). SomeSaudi Arabian bank staff falls into the phishing trap as hackers create emails to appear from the bank's top management team. The phishing attacks enablescybercriminals to complete transaction whereby the banks lose financial resources. Therefore, weak cybersecurity educationleads banking staff to face cybersecurity threats.

Alzubaidi (2021) states that a lack of awareness escalates the number of cybersecurity attacks in the Saudi Arabian banking sector. Bank staff, part of the Saudi Arabian population, have little knowledge ofcybersecurity aspects such as cloud computing and mobile malware. As a result, they access unsafe websites using bank computers, increasing their vulnerability to cyber-attacks. Failure to have sufficient information on email phishing makes the staff expose the banking systems to cybercrimes. In addition, banking staff only sometimes observes password security measures as they share their system credentials with colleagues. The failure toupdate the operating systems of the bank computers provides room for hackers to access sensitive information that they use to conduct malicious cyber activities that distortthe reputation of the banks. Thus, cybersecurity threat reduction can be possiblethrough creating awareness achievable through a quality education system.

The Role of Education in Addressing Cybersecurity Problems

Saudi Arabian universities have a significant role in providing quality education that instils cybersecurity knowledge. The education helps develop an improved cybersecurity infrastructure that ensures that there are cybersecurity policies (Venter et al., 2019). The adoption of international and local cybersecurity standards in education facilitates the development of a robustcybersecurity framework. In addition, instruction ensures that individuals comply with cybersecurity regulations and guides them to avert the possibility of cyber-attacks. Furthermore, organisations learn to adopt cybersecurity risk management strategiessuch as purchasing insurance covers (Venteret al., 2019).

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2023.29.03.032

Thus, education creates a robustcybersecurity infrastructure in Saudi Arabia.

Education enlightens the residents of Saudi Arabia on safe cybersecurity practices. People learn to keep their passwords confidential (Venter et al., 2019). The exposure of passwords or pins makes the account holders increase banks' vulnerabilities through internet banking and using credit and debit cards. In addition, it ensures that people constantly update softwares to hinder loopholes for cybercriminalsfrom infiltrating the banking systems. Furthermore, education informs the securefile-sharing platform that protects internet users from worms or viruses designed byhackers. Moreover, it insists that computer users install antiviruses that easily identify viruses set by cybercriminals that might havecompromised access to banking systems (Venter et al., 2019). Hence, educationensures maintenance of passwordconfidentiality, constant update of software, secure file sharing platforms, and installationof antiviruses in computers.

Adequate and competent cybersecurityspecialists help build a robust IT securityinfrastructure that minimises cyber threats(Venter et al., 2019). The provision of cybersecurity education increases the availability of security professionals in SaudiArabia. In addition, it ensures that available IT security experts in the banking sector get adequate time to rest to avoid an overwhelming situation of low productivity. Thus, education produces a sufficient numberof cybersecurity experts in a nation.

The education centres organise cybersecurity awareness programs that target students and community members. The cybersecurity awareness programs increase IT security knowledge to people can practice safe cybersecurity measures (Venter et al., 2019). Thus, increased awareness ensures that banksdo not face numerous cyber-attacks.

Cybersecurity Programs in Saudi Arabian Universities

The establishment of a competent workforcein IT security requires quality cybersecurity education. The Saudi Arabian higher learning institutions offer cybersecurity programs at undergraduate and graduate levels. University of Prince Mugrin and Imam Abdurahman bin Faisal University offer only undergraduate studies in cybersecurity and digital forensics (Latifi, 2020). However, higher learning institutions such as Prince Sultan University and Jeddah University provide both undergraduate and graduate studies in cybersecurity. Graduate security and information science programs are thecritical areas of emphasis at the King Fahd University of Petroleum and Minerals (KFUPM) (Latifi, 2020). The cybersecurity programs in Saudi Arabian universities are few, lowering the ability of the country to have adequate cybersecurity specialists. Saudi Arabia should emulate the United States of America, whereby the Ministry of Interior (MOI) has a standard cybersecurity education program (Dawson, 2022). The cybersecurity curriculum in Saudi Arabia should undergo adjustments to manage cyber-attacks. King Abdullah Center for Science and Technology and Prince Mohammed bin Salman College teach artificial intelligence and other improved cybersecurity programs (Garba et al., 2021). National Center for Cybersecurity Technology (C4C) promotes innovation in cybersecurity. In addition, it collaborates with the Ministry of Education in KSA to encourage a high intake of students into cybersecurity programs (Garba et al., 2021).Hence, adopting excellent cybersecurity curricula in Saudi Arabian universities will increase the number of security specialists.

The cybersecurity undergraduate course at Imam Abdurahman bin Faisal University teaches network security, information systemauditing, and applied cryptography. The University of Prince Mugrin offers an undergraduate cybersecurity program that entails ethical hacking, security risk management, and web security (Latifi, 2020).The graduate cybersecurity programs have credit and thesis hours to ensure that studentsresearch emerging trends that might increasecyber threats (Latifi, 2020). Thus, the cybersecurity programs in Saudi Arabian universities are essential in improving the ITsecurity professionals currently in high demand in KSA.

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2023.29.03.032

The Effects of Vision 2030 on the Transformation of Education in SaudiArabia

Saudi Vision 2030 aims at achieving a diversified economy in the Kingdom of SaudiArabia (KSA). Economy diversification requires adequate human capital with the right skills and knowledge to work indifferent sectors such as healthcare, ICT, andmanufacturing. Vision 2030 developed Human Capital Development Program (HCDP) to ensure an adequate labour force through quality education. In addition, SaudiArabian education has embraced American and European curricula to equip students highorder thinking skills (Mirghani, 2020). Learning institutions in Saudi Arabia should teach the English language to help students become global citizens who can communicate with other English speakers effectively. In addition, the cybersecurity curriculum adopted from America and Europe exists in English (Mirghani, 2020) states. Thus, Saudi Arabian students will comprehend IT security concepts. Effective training delivery will ensure that Saudi Arabia has sufficient teachers who can impartknowledge to students. Failure to which the Saudi Arabian community will remain too low cybersecurity awareness. Therefore, quality education will help Saudi Arabia haveadequate workers in all economic sectors.

Saudi Arabia continues to experience cyber threats. For instance, different economic sectors in Saudi Arabia experienced over twenty-two million and five hundred thousand cyber-attacks in 2020, with afinancial loss of 6.5 million dollars (Olech, 2021). The efforts to establish a robust cybersecurity infrastructure pushed NCA to partner with Saudi Arabia's Ministry of Education to increase training and develop cybersecurity research programs in May 2021. The increased number of cyberattacks in Saudi Arabia in 2020 was attributable to the COVID-19 pandemic that encouraged remote working. In addition, the advanced internet usage in homes made many ICT infrastructures vulnerable to cyber-criminals. Therefore, NCA has expressed outstanding commitment to improving cybersecurity through the ministry of education.

Vision 2030 guides Saudi Arabian students to gain relevant skills for future employment opportunities. The Kingdom of Saudi Arabiaaims to develop educational curricula andinfrastructure in the universities to ensure thatat least five local higher learning institutionsrank in the top two hundred globally (D. Alshrari, Hassan Omer and Salmen Aljaaidi,2021). Vision 2030 also aims to produce great academic scholars. The Saudi Arabian curriculum aims to advance mathematical capabilities and develop high morals for students to ensure ethical behaviour. Ethics ensures that community members do not engage in cybercrimes. Saudi Arabia teacherssupport Vision 2030 by having excellent teaching tools that match international standards. Therefore, Saudi Arabian can produce a competent workforce in a diversified economy (Allmnakrah and Evers,2019).

The Role of Vision 2030 in Creating Cybersecurity Jobs in the Banking Sector

Digital transformation has increased thedemand for cybersecurity skills. In Saudi Arabia, the number of cybersecurity specialists is low in technical aspects such asartificial intelligence and blockchain.Cybersecurity professionals are essential in banks to protect against financial losses and avoid reputation denting caused by cyber-attacks. Account-holders often lose faith in banks if their get loses through cyber-crimesas they condemn the vulnerability of bankingsystems (Kumar, 2018). Therefore, the available and limited number of cybersecurityspecialists in the Saudi Arabian banking sector get overwhelmed by cyber- attacks.

Saudi Arabian education should match job market demands according to Vision 2030. Saudi children should access education standards that promote innovation and creativity to help solve emerging problems. In addition, the Saudi Arabia curriculum fosters critical thinking and prepares students for current trends attributable to globalisation (Makhlouf, 2021). The Saudi Arabia government has had huge educational expenditures to achieve learning outcomes. Still, most

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2023.29.03.032

students need more employable skills because English limits them from working in Arabic-speaking countries. Hence, Vision 2030 ensures that students in all learning centres get relevant job skills to meet labour force demand.

The Research in Significance and Gap

Saudi Vision 2030 aims to improve the cybersecurity infrastructure in all economic sectors, including the local banking industry. It is an umbrella that encourages creativity and innovation to overcome cybersecurity challenges by implementing improved curricula. The low number of cybersecurity experts in the Saudi Arabian banking sector is solvable through quality training on IT security provided in universities. Quality education in Saudi Arabian learning institutions guarantees the development of a competent labour force capable of working in a diversified economy.

The research is significant to the Saudi Arabian economy as it aims to improve cybersecurity awareness. In addition, the study elaborates on the role of Saudi Vision 2030 in the finance and education sectors to promote the GDP growth of Saudi Arabia (Kosárová, 2020). The research will educate on safe cybersecurity practices, such as avoiding password sharing and updating operating systems. It increases cybersecurity awareness among IT and non-IT students in Saudi Arabian higher learning institutions to prepare them to exercise safe cybersecurity practices in manufacturing, health care, and hospitality. The study intends to investigate if the Saudi Arabian banking sector has adequate and qualified cybersecurity professionals to minimise security breaches that cause high financial implications. In addition, the research targets to provide skilled professionals for the private sectorthrough a quality education system(Kosárová, 2020).

Furthermore, the banking employees in Saudi Arabia will have high cybersecurity knowledge that they can transfer to account holders to create secure cyberspace. Also, quality education in Saudi Arabia will educate IT and non-IT students on emerging cybersecurity issues to create awareness. The research gap exists through a lack of education that increases cybersecurity awareness among all banking employees. Indeed, the literature review intends to promote cybersecurity in the Saudi Arabian banking industry through quality education offered in higher learning institutions.

The Variables in the Literature Sources

Variables			
1	Saudi Arabian Cybersecurity Rankings.	4	Cybersecurity Educational Programs in Saudi Arabian Universities.
2	Cybersecurity Awareness among Saudi Arabian University Students.	5	Cybersecurity in the Saudi Arabian Banking Sector.
3	Cybersecurity Awareness among Banking Staff.	6	The Role of Education in Addressing Cybersecurity Problems.

Table of Literature Gaps in the Literature Sources

	Literature Gaps
1	Failed to show the financial losses attributable to cybersecurity.
2	Ignored the banking sector but focused on cybersecurity importance to achieve national security.
3	Not reveal insurance premiums payable by banks.
4	We need to enlighten the measures of Saudi Vision 2030 to attain a robust cybersecurity infrastructure.
5	We need to specify the population of cybersecurity professionals in Saudi Arabia.
6	Not highlight learning institutions NCA has collaborated with to promote cybersecurity in Saudi Arabia.
7	Need to describe cybersecurity programs and initiatives to increase Saudi Arabia's

	cybersecurity index.
8	Not provide cybersecurity protection strategies.
9	Failed to state the risks associated with non-compliance to cyber laws.
10	Describe the Saudi Arabian education relevance to promoting cybersecurity.
11	Need to determine the cybersecurity awareness of the professors in Saudi Arabian universities.
12	Failed to acknowledge the importance of Saudi Vision 2030 in transforming the education sector.
13	Need to be enlightened on the necessary cybersecurity professional certifications that graduate students pursuing IT security should take.

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2023.29.03.032

RESEARCH QUESTIONS

1. What initiatives should Saudi Arabia's government implement towards developing the cybersecurityinfrastructure to achieve vision 2030?

The government's contribution is critical in ensuring that cybersecurity infrastructure is sustainable and effective. One needs to understand the government's impact on making the banking services' experience better and more secure through understanding the contribution toward vision 2030. Through observing major indicators, one can understand how the government has played a role in effective change. Observation of significant changes that the government continues to meet towards cybersecurity enables adequate assessment ofmodifications needed for the future based on successes and failures over time. Therefore, it is vital to comprehend how the government has contributed to cybersecurity infrastructure through effective execution and how its involvement has changed thebanking experience.

2. What factors contribute to the cybersecurity issues in Saudi Arabia's banking sector?

Many known factors can contribute to cybersecurity breaches in the banking sector in Saudi Arabia, such as malware and vulnerabilities that attackers exploit. As aresult, there is a need to know the contributing factors to cybersecurity issues in banking to facilitate effective strategising toward future data breaches. Other factors include inadequate planning and a lack of strategies to curb any unforeseen events in thedata breach for the bank services. Additionally, it's essential to determine whether unskilled employees and overzealous security measures are the leading causes of cybersecurity problems in Saudi Arabian institutions.

3. What is the role of Saudi universities in promoting university students' cybersecurity knowledge according to vision 2030?

Higher education, especially in universities, enables more security in the banking sector. Due to the continued demand for better safetystandards for people's finances, there is aneed to understand how educational institutions equip students with information technology knowledge in the banking sector for a more effective strategy in the future. In addition, there is a need to understand whether the universities have the proper programs to enable students to provide betterbanking services and improved security. Therefore, the research mainly seeks to understand Saudi Arabian universities' role inequipping their students with knowledge regarding cybersecurity in banking.

SIGNIFICANCE OF STUDY

The study findings could improve the cybersecurity infrastructure in Saudi Arabia.The research will ensure that all economic sectors have improved the information sectorto realise Saudi Vision 2030 (Quadri andKhan, 2019). The Saudi Vision 2030 willmake Saudi Arabia less reliant on petroleum products for economic growth. The research might help Saudi Arabia's government put more effort into improving cybersecurity in the banking sector. The government can empower the commissions established to realise cybersecurity in Saudi Arabia. In addition, the research outcomes will enable Saudi Arabian universities to introduce mandatory security courses to students undertaking undergraduate programs in information technology. They will also include these courses for non-IT students to generate cybersecurity awareness for alluniversity students, whatever their majors. As a result, undergraduate students will get professional certifications that affirm them ascybersecurity specialists (Aljuryyed, 2022). Therefore, the study might develop an excellent cybersecurity infrastructure in Saudi Arabia with adequate security specialists.

The study might positively grow the economy of Saudi Arabia. The robust cybersecurity infrastructure will attract more investors in economic sectors such as tourism and health care (Aljuryyed, 2022). The increased investments will provide adequate employment opportunities to

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2023.29.03.032

the people of Saudi Arabia to reduce unemployment rates. Businesses will comfortably engage in online transactions without fear of losing their finances. This confidence will encourage firms to expand to different regions or areas in Saudi Arabia. The expansion indicates positive growth of economic activities. The university students undertaking information technology-related courses will have ready job vacancies as each company might have cybersecurity departments (Quadri and Khan, 2019). The people of Saudi Arabia might not lose their money in bank accounts as they are aware of cybersecurity matters. Thus,research will improve the economy of Saudi Arabia.

CONCLUSION

A quality education system can impart cybersecurity knowledge to banking employees. It educates safe cybersecurity practices such as avoiding password sharing, installing antiviruses, and updating computer operating systems. In addition, quality education produces adequate and qualified cybersecurity professionals who collaborate to build a resilient cybersecurity infrastructure. The Saudi Vision 2030 supports improving the curriculum to achieve acceptable skilled professionals who will work in a diversified economy. Furthermore, it supports the financial sector by establishing NCA, which intends to create a safe cyberspace environment. The poor education system and lack of awareness by account holders and bank workers are key variables escalating cyber threats in the Saudi Arabian banking sector. SAMA (Saudi Central Bank) established a cybersecurity framework that all Saudi Arabian banks follow to minimise cyber risk. An advanced curriculum will help increase cybersecurity awareness among Saudi Arabian banking employees to ensure economic growth. Saudi Arabian university students have average knowledge of cybersecurity. They are vulnerable tophishing and social engineering attacks because they are unaware of safe cybersecurity practices.

Only students pursuing computer or information technology courses have high cybersecurity knowledge. The Shamoon virus attacked an energy sector company, Saudi Aramco, causing data breaches in drilling and marketing strategies. The Saudi Arabian health sector got inconvenienced by a Denial of Service attack that blocked access to the public health website. CERT, CoEIA, and NCSC are commissions established by the Saudi Arabian government to support cybersecurity promotion efforts. Higher learning institutions like the University of Prince Mugrin and Jeddah University are committed to offering cybersecurity education to attain an adequate IT security labour force in the Kingdom. NCA collaborates with Saudi Arabian government to implement the cybersecurity strategy. However, bank employees should increase cybersecurity awareness efforts to realise safe cyberspace.

References

1. Alghazo, J.M., Kazmi, Z. and Latif, G. (2017). *Cyber security analysis of internet banking in emerging countries: User and bank perspectives.* [online] IEEE Xplore. doi:10.1109 /ICETAS.2017.8277910.
2. Aljeaid, D., Alzhrani, A., Alrougi, M. and Almalki, O. (2020). Assessment of End-User Susceptibility to Cybersecurity Threats in Saudi Arabia by Simulating Phishing Attacks. *Information*, 11(12), p.547. doi:10.3390/info11120547.
3. Aljohni, W., Elfadil, N., Jarajreh, M. and Gasmelsied, M. (2021). Cybersecurity Awareness Level: The Case of Saudi Arabia University Students. *International Journal of Advanced Computer Science and Applications*, 12(3). doi:10.14569/ijacsa.2021.0120334.
4. Aljuryyed, A. (2022). Cybersecurity Issues in the Middle East. *Cybersecurity Capabilities in Developing Nations and Its Impact on Global Security*, pp.62–82. doi:10.4018/978-1- 7998-8693-8.ch004.
5. Allmnakrah, A. and Evers, C. (2019). The need for a fundamental shift in the Saudi education

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2023.29.03.032

system: Implementing the Saudi Arabian economic vision 2030. *Research in education*, p.003452371985153. doi:10.1177/0034523719851534.

6. Alqurashi, R.K. (2020). Cyber Attacks and Impacts: A Case Study in Saudi Arabia. *InternationalJournal of Advanced Trends in Computer Science and Engineering*, 9(1), pp.217–224. doi:10.30534/ijatcse/2020/33912020.
7. Benson, V. (2017). The state of global cybersecurity: Highlights and key findings. [online] Available at: https://www.researchgate.net/publication/318310907_THE_STATE_OF_GLOBAL_CYBER_SECURITY_HIGHLIGHTS_AND_KEY_FINDINGS. [Accessed 3 Dec. 2022].
8. Cybersecurity Guide. (2021). *Cybersecurity in the financial services industry*. [online] Availableat: https://cybersecurityguide.org/industries/financial/. [Accessed 4 Dec. 2022].
9. D. Alshrari, A., Hassan Omer, W.K. and Salmen Aljaaidi, K. (2021). Saudi Arabian 2030 Visionand Entrepreneurial Intention Among University Students. *AD-minister*, (38), pp.43–62. doi:10.17230/ad-minister.38.2.
10. Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon*, 7(1), p.e06016. doi:10.1016/j.heliyon.2021.e06016.
11. Bauer, S., Bernroider, E.W.N. and Chudzikowski, K. (2017). Prevention is better than cure!
12. Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers & Security*, 68, pp.145–159. doi:10.1016/j.cose.2017.04.009.
13. Chaudhry, A.F., Aniol, H. and Shegos, C.J. (2020). [online] Available at: https://www.consultant360.com/article/consultant360/congenital-hypothyroidism-due- thyroid-agenesis. *Consultant*. doi:10.25270/con.2020.05.00011. [Accessed 3 Nov. 2022].
14. Dawson, M. (2022). An Argument for Cybersecurity in Saudi Arabia. *Land Forces Academy Review*, 27(1), pp.78–83. doi:10.2478/raft-2022-0011.
15. Devi, A. (2021). *Saudi Arabia ranks No. 2 globally in its commitment to cybersecurity*. [online] Security MEA Available at: https://securitymea.com/2021/06/30/saudi-arabia-ranks-no- 2-globally-in-its-commitment-to-cybersecurity/ [Accessed 10 Dec. 2022].
16. Elnaim, B.M. and Al-Lami, H.A.S.Wsmi. (2017). The Current State of Phishing Attacks against Saudi Arabia University Students. *International Journal of Computer Applications Technology and Research*, 6(1), pp.042–050. doi:10.7753/ijcatr0601.1008.
17. Flowerday, S. and von Solms, R. (2005). Real-time information integrity=system integrity+data integrity+continuous assurances. *Computers & Security*, 24(8), pp.604–613. doi:10.1016/j.cose.2005.08.004.
18. Garba, A., Jeribi, F., Al-Shourbaji, I., Alhameed, M., Reegu, F. and Alim, S. (2021). *An Approach To Weigh Cybersecurity Awareness Questions In Academic Institutions Based On Principle Component Analysis: A Case Study Of Saudi Arabia*. [online] Available at: http://www.ijstr.org/final-print/apr2021/An-Approach-To-Weigh-Cybersecurity- Awareness-Questions-In-Academic-Institutions-Based-On-Principle-Component- Analysis-A-Case-Study-Of-Saudi-Arabia.pdf [Accessed 9 Oct. 2022].
19. Goo, J., Yim, M.-S. and Kim, D.J. (2014). A Path to Successful Management of Employee Security Compliance: An Empirical Study of Information Security Climate. *IEEE Transactions on Professional Communication*, 57(4), pp.286–308. doi:10.1109/tpc.2014.2374011.
20. Halse, L. (2021). *New Law In Saudi Arabia To Require Regional Headquarters For International Companies*. Government Contracts, Procurement & PPP - Saudi Arabia.[online] Available at: https://www.mondaq.com/saudiarabia/government-contracts-procurement-ppp/1041884/new-law-in-saudi-arabia-to-require-regional-headquarters-for- international-companies [Accessed 22 May. 2022].

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2023.29.03.032

21. HKA. (2021). *The Growth and Development of Saudi Arabia's Cybersecurity Landscape*. [online] Available at: https://www.hka.com/the-growth-and-development-of-saudi- arabias-cybersecurity-landscape/. [Accessed 2 Dec. 2022].
22. Kosárová, D. (2020). *Saudi Arabia's Vision 2030*. [online] Available at: https://www.researchgate.net/publication/346531524_SAUDI_ARABIA'S_VISION_203 [Accessed 14 July. 2022].
23. Kumar, N. (2018). *The skills gap exacerbates the cybersecurity problem as the Middle East faces threats*. [online] Avai;able at https://thearabweekly.com/skills-gap-exacerbates-cybersecurity-problem-middle-east-faces-threats [Accessed 31 May. 2022].
24. Latifi, S. (2020). *17th International Conference on Information Technology–New Generations (ITNG 2020)*. [online] *Google Books*. Springer International Publishing. Available at: https://books.google.dk/books/about/17th_International_Conference_on_Informa.html?id
25. =saRTzQEACAAJ&hl=en & output=html_ text & redir_ esc=y [Accessed 10 Dec. 2022]. Levite, A.E., Kannry, S. and Hoffman, W. (2018). *The Role of the Cyber Insurance Industry*.
26. [online] JSTOR. Available at: http://www.jstor.org/stable/resrep20984.6 [Accessed 10 Dec. 2022].
27. Lynch, K. (2021). *Council Post: Cybersecurity Is A Global Problem, So Where's The Global Response?* [online] Forbes. Available at: https://www.forbes.com/sites/forbestechcouncil/2021/05/20/cybersecurity-is-a-global- problem-so-wheres-the-global-response/?sh=3e26bbfb5e41 [Accessed 10 Dec. 2022].
28. Makhlouf, A. (2021). Saudi Schools' Openness to Change in Light of the 2030 Vision. *AmericanJournal of Educational Research*, 9(1), pp.52–60. doi:10.12691/education-9-1-6.
29. Malek, C.(2019). *Saudi Arabia's war against hackers*. [online] Available at: https://www.arabnews.com/node/1483661/saudi-arabia. [Accessed 17 Feb. 2022].
30. Mirghani, T.M. (2020). The Growing Demand for Education in Saudi Arabia: How Effective Is Borrowing Educational Models from the West? *Journal of Education and Learning*, 9(6),p.59. doi:10.5539/jel.v9n6p59.
31. Nahas, P. (2022) *DIGITALISATION IMPACTS ON INDIVIDUAL AND ORGANISATIONAL BEHAVIORS IN FACTORIES: HOW DO GENERATIONAL APPROACH AND MANAGERIAL SUPPORT MEDIATE THE CHANGE'S SUCCESS?* [online] Available at: http://www.iseor-formations.com/pdf/ACTESCOLMCD2021/NAHAS.pdf [Accessed 10 Dec. 2022].
32. O'Connell, E.A. (2021). Revitalising Language through Education: Ireland's Use of International Law to Drive Linguistic Preservation. *DePaul Journal of Art, Technology and Intellectual Property Law*, [online] 31, p.68. Available at: https://heinonline.org/HOL/LandingPage?handle=hein.journals/dael31&div=3&id=&pag e= [Accessed 10 Dec. 2022].
33. Olech, A. (2021). Cybersecurity in Saudi Arabia. Retrieved July 14, 2022, [online] Available at:https://ine.org.pl/en/cybersecurity-in-saudi-arabia/.[Accessed 14 Jul. 2022].
34. Quadri, A., & Khan, M. (2019). *Cybersecurity challenges of the Kingdom of Saudi Arabia*. [online] Available at: https://www.researchgate.net/publication/331009167_CYBERSECURITY_CHALLENGES_OF_THE_KINGDOM_OF_SAUDI_ARABIA [Accessed 10 Dec. 2022].
35. Riegger, A.-S., Klein, J.F., Merfeld, K. and Henkel, S. (2021). Technology-enabled personalisation in retail stores: Understanding drivers and barriers. *Journal of Business Research*, [online] 123, pp.140–155. doi:10.1016/j.jbusres.2020.09.039.
36. Saudigazette. (2022). *SAMA seeks proactive steps to confront growing cyber threats*. [online] Available at: https://saudigazette.com.sa/article/620722 [Accessed 10 Dec. 2022].

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2023.29.03.032

37. Seemma, P., Nandhini, S., & Sowmiya, M. (2018). Overview of Cybersecurity. *PEARCE*, *7*(11),125-128. doi:10.17148/ijarcce.2018.71127
38. Singh, H.P. and Alshammari, T.S. (2020). An Institutional Theory Perspective on Developing a Cyber Security Legal Framework: A Case of Saudi Arabia. *Beijing Law Review*, 11(03), pp.637–650. doi:10.4236/blr.2020.113039.
39. Slavchev, V. (2021). Using Cyber Ranges in Cybersecurity Management Educational Programmes. *Information & Security: An International Journal*, 50, pp.161–168. doi:10.1 1610/isij.5007.
40. Tsakanyan, V.T. (2017). The role of cybersecurity in world politics. *Vestnik RUDN. International Relations*, [online] 17(2), pp.339–348. doi:10.22363/2313-0660-2017-17-2- 339-348.
41. Venter, I.M., Blignaut, R.J., Renaud, K. and Venter, M.A. (2019). Cyber security education is asessential as 'the three R's'. *Heliyon*, 5(12), p.e02855. doi:10.1016/j.heliyon.2019.e02855.
42. Woishi, W. (2019). THE IMPACT OF DIGITISATION ON THE ECONOMY OF KSA IN THE
43. CONTEXT OF VISION 2030. *International Journal of Engineering Applied Sciences and Technology*, 04(04), pp.312–316. doi:10.33564/ijeast.2019.v04i04.051.
44. Yang, J. (2022). *Importance of Security in the digital world*. [online] Available at https://techpresident.com/importance-of-security-in-digital-world/.[Accessed 14 Jul. 2022].
45. ZATCA Report and Plans (2017). *E-Invoicing*. [online] Available at: https://zatca.gov.sa/en/E-invoicing/Pages/default.aspx [Accessed 10 Dec. 2022].