Volume 31 (Special Issue) October 2024 ISSN 0216-423X (Print)
ISSN 2622-2667 (Online)

JABM
JOURNAL *of*
ACCOUNTING, BUSINESS and MANAGEMENT

Journal of Accounting, Business and Management (JABM) vol. 31 Special Issue 2024 76-83

Crucial Elements in the Development of Cyber Security Strategies in Saudi Arabia

Nisar Ahmad Zafar*
Shahzad Ali Khan†

Abstract

The digital world has gained significant importance in recent years, owing to its many advantages as well as the sheer volume of users, which is constantly increasing, including in both public and private organizations. Numerous hazards and vulnerabilities associated with this growth and advancement have been interfering from time to time. As a result, cybersecurity and protection measures have been implemented in different digital domains. The national security, the economy, business, and the everyday lives of people are constantly under threat due to the innate weaknesses in cyberspace and the continually growing threat of cyber attacks. The research paper highlights essential elements in developing and managing cyber security strategies in Saudi Arabia to strengthen security measures. To achieve this motive, a literature review has been done to explore the significance of cyber security elements such as security awareness through education, risk prevention, data management, network security in business and smart cities, and constant monitoring of security measures by analyzing previous studies so that Saudi Arabia can better develop its cyber security policies by incorporating these elements into latest policies. The use of artificial intelligence (AI) in cyber security is also being explored in this study due to the fast penetration of AI worldwide. This paper is also helpful for policymakers in designing national cyber security policies by examining the guidelines given at the end of the study.

Keywords: cyber security, strategies, Saudi Arabia, artificial intelligence.

I. INTRODUCTION

The virtual Kingdom of cyberspace has become a crucial component of modern society. The states and global community make significant efforts to guarantee specific conditions and measures in this society. Due to this increased demand for practical strategies and security alerts, numerous national cyber security plans, such as the European Union (EU) and the North Atlantic Treaty Organization (NATO), have quickly gained significant prominence on the political agendas of the present day (Klaic, 2016).

In contrast to the early internet's simple electronic services that eventually spread worldwide, today's cyberspace has fundamentally altered people's personal and professional lives. It has also changed most business sectors' infrastructure and transformed business concepts in our society. Many nations have realized that the widespread use of information and communication technology and the extreme involvement of digital tools have made their national information infrastructure extremely vulnerable to cyber-attacks, resulting from high-profile cyber-attacks in the past. Some of these cyber-attacks include the attacks on Estonia's internet infrastructure

* Swiss School of Business Research (SSBR), Nüschelerstrasse 31, 8001, Zurich, Switzerland. E-mail: Nisar.zafar@gmail.com.
† International Islamic University. E-mail: Shahkhan192@gmail.com.

in 2007, the physical war between Georgia and Russia that escalated into a cyberwar in 2008, and the Stuxnet worm attack on Iran's nuclear program in 2010 (Shafqat & Masood, 2016). These major attacks threatened the cyber world immensely and pushed users to develop robust policies to avoid such acts in the future.

The terms "cyber-attack" and "cyber assault" refer to the intents and needs to cause harm or adverse effects on someone's personal information and the entire network system, while "cyber security" and "cyber defense" refer to the need to safeguard information and network from malicious acts and attacks. The "cyber war" idea is becoming increasingly popular as countries create and execute plans and regulations to compete for cyber-attacks and defense. These malicious acts made governments think of protecting their data and networks by designing security policies at a national level. As a result, governments are working very hard in cyberwarfare, cybersecurity, and cyber deterrence. They are attempting to assess important matters in light of technological advancements, taking action by recognizing threats and hazards, setting goals based on the needs by forecasting the future, creating plans and policies, and carrying them out successfully (Senol & Karacuha, 2020).

Like other developed countries' governments, Saudi Arabia is currently engaged in internal initiatives to enhance its cyberspace capacities. The COVID-19 pandemic and the sharp decline in energy prices have expedited this process. In the first quarter of 2020, when the coronavirus pandemic started, the Middle Eastern countries saw a 22% and 36% spike in malware and spam attacks, respectively. Companies in Saudi Arabia that were transitioning to remote work found it incredibly challenging during this time. Because of Saudi Arabia's critical location in the region, cyber incidents threaten ICT infrastructure in the public and commercial sectors (Olech & Siekierka, 2022). This era sparked the need to develop security boundaries to protect the Saudi digital world and economy.

Now, investment in cybersecurity is a significant business objective in Saudi Arabia, and over half of the Saudi directors of information affairs view security management as the most critical technology issue. Additionally, the need to maintain cybersecurity has emerged as one of the primary markers of business performance and the nation's digital success, with an increase in the annual budget for digital technology management and data protection (Alzubaidi, 2021). This measure was very much needed after a significant loss of $693 million in 2012 because of a cyber-attack in Saudi Arabia (Alasmari, 2021). Over 22.5 million cyberattacks were reported in Saudi Arabia in 2020, with an estimated cost of $6.5 million per attack to the government. In the first quarter of 2021, over 7 million cyber-attacks were reported (Olech & Siekierka, 2022).

There was constant security attacks took place, which harmed Saudi Arabian government authorities and businesses to a great extent. Those attacks cause significant information leakage and theft of data. The Kingdom of Saudi Arabia fell prey to an abortive spying campaign in May 2020, spearheaded by the Iranian organization Chafer APT (Arsene & Rusu, 2020). Furthermore, recent developments in Saudi Arabia suggest that cyber terrorists are turning to social media as a substitute to sabotage inter-citizen communication and impede economic activity by infiltrating users' communication channels.

Numerous pieces of evidence are available in research papers, news, and social media websites showing severe issues regarding cyber-attacks in Saudi Arabia for many different purposes. This provoked the Saudi government to design and develop cyber security strategies to protect their data and information on essential platforms. Hence,

there is still a great need to investigate the crucial elements of cyber security so that they can be utilized effectively to combat the latest technological challenges.

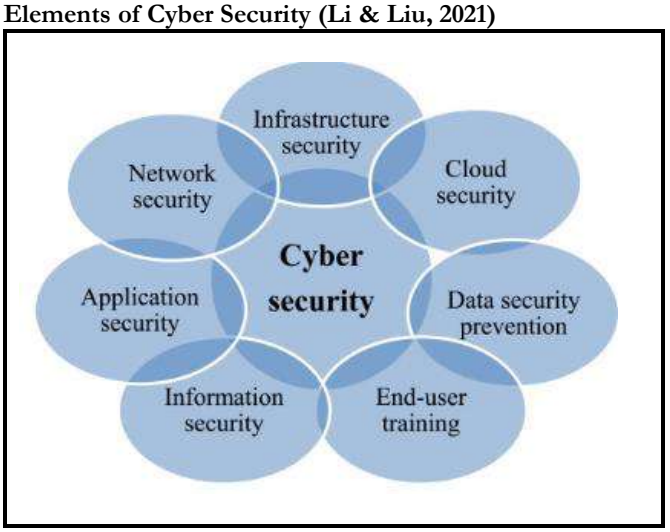
II. LITERATURE REVIEW

Royal decree founded the national cyber security authority (NCA) in Saudi Arabia on October 31, 2017, in response to severe cybersecurity concerns. The primary objective of the NCA is to enhance the state's digital security by developing internal analysis and legal measures. In addition to carrying out operational and regulatory duties regarding cybersecurity, NCA works closely with both public and private organizations to enhance national security, safeguard vital infrastructure, and create a cyberspace conducive to the 2030 strategy's execution (NCA, 2018). The goals of Saudi Arabia are reflected in the national cybersecurity vision that the NCA developed. These goals include fostering an environment in cyberspace that upholds security, fosters self-reliance in authorities, and promotes technological advancement. Later, the NCA was revised in 2023 by the Saudi Data and AI Authority.

Saudi Arabia has recently experienced modernization, especially in technology and legislation. The Kingdom is pursuing technological improvements to thrust itself into the digital era with its enormous Saudi Vision 2030. This change emphasizes the importance of strong data protection and cyber security regulations to protect individuals and businesses. As a result of this advancement and modernization, the Saudi data and AI authority (SDAIA) introduced the personal data protection law (PDPL) in 2023. It made clear that the PDPL will serve as the primary legislation governing the processing of personal data. The PDPL also calls for establishing sector-specific regulations for credit information, financial services, and the health sector (GDPC, 2023).

Researchers have studied some crucial elements in Figure 1 to strengthen the concept of cyber security.

Figure 1
Elements of Cyber Security (Li & Liu, 2021)



These elements can work as a shield against almost every security threat attacking Saudi Arabia's cyberspace. These security dimensions are pivotal in preventing fraud and theft by hackers and viruses.

2.1. Network, Information, and Data Security

Network security refers to a group of tools that assist businesses in protecting their computer networks from malware, hackers, and criminal acts. It has been discussed

frequently in business and smart city development as an essential tool in maintaining networks' security. Network security is comprised of several intricate anti-hacking measures. It incorporates unique anti-invasion procedures, software, hardware, and configurations. Experts must be guided by well-designed tactics regarding network security (Mughal, 2022).

In business procedures, network security is crucial to secure personal data and clients' information, enhance network performance, avoid ransomware challenges, obey security rules, etc. On the other hand, network security has proven to be an effective tool in smart buildings and cities as it helps manage cyber security risks such as data theft (security plans, traffic flow plans, etc.) (Ajmi et al., 2019). Since Saudi Arabia has recently become heavily involved in developing smart cities, network security is an excellent operation tool.

2.2. Infrastructure Security

As Saudi Arabia moves forward with its ambitious vision 2030 plan, safeguarding vital infrastructure becomes a primary concern. Because of the increasing reliance on interconnected systems in this digital age, strengthening these essential structures, especially in business and smart city construction, is more important than ever (Alhalafi & Veeraraghavan, 2021).

2.3. Application and Cloud Security

A robust digital ecosystem is built on the foundation of cloud security. It comprises a range of procedures, tools, and guidelines to shield infrastructure, data, and apps against online dangers. The global adoption of cloud services is expected to persist, with cloud-based solutions remaining highly popular in Saudi Arabia. Because of this, the NCA has determined that it is imperative to address cybersecurity concerns in the context of cloud computing through cloud-focused methods (Al Nafea & Almaiah, 2021).

2.4. End-user Training

End-user training plays a significant role in managing cyber-security issues. Previous studies have focused enormously on this aspect. Alotaibi et al. (2016) used 629 participants (70% male and 30% female) in a quantitative online survey to investigate cybersecurity knowledge among Saudi citizens. The survey discovered that while the participants possessed strong IT skills, they needed to be better informed about cybersecurity procedures, cybercrime, or the government's and organizations' roles in protecting the integrity of online information.

In another study, Innab et al. (2018) provided awareness and training to 116 workers of governmental and private organizations in Riyadh regarding phishing emails. This study primarily focused on Saudi Arabian individuals without prior IT-related experience. The study concluded that, given the low level of knowledge and anti-phishing training, it is imperative to raise awareness by implementing anti-phishing training initiatives. Employees within the company should receive sufficient training on phishing awareness, especially since email is the most convenient medium for carrying out phishing assaults.

2.5. Artificial Intelligence (AI) and Cyber Security

The use of AI in cybersecurity has become a hot topic these days. Intrusion detection systems are today's most demanding artificial intelligence tool in cyber security. AI makes real-time cyber threat detection, analysis, and response possible. Artificial intelligence (AI) algorithms can scan the entire network for vulnerabilities to stop common types of cyber-attacks and analyze vast volumes of data to identify patterns

suggestive of a cyber threat (De Azambuja et al., 2023). Saudi Arabia rapidly adopts AI tools to increase productivity and efficiently manage internal and external threats (Zeadally et al., 2020).

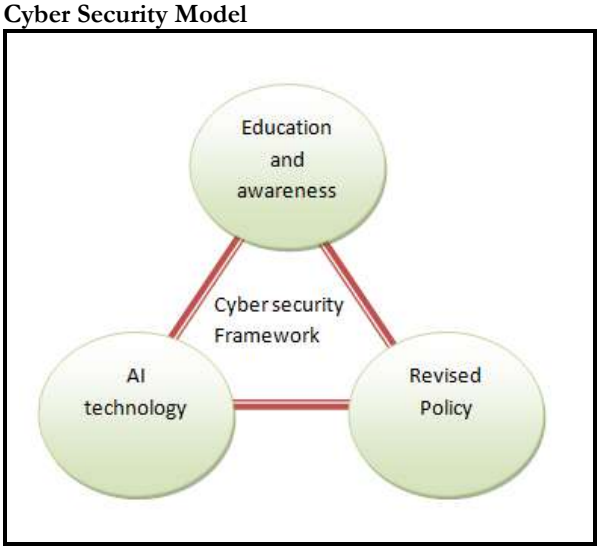
III. RESEARCH AND METHODOLOGY

The study solely depends upon a substantial literature review. The literature has been gathered through previous articles, reports, and research in cyber security. The search engines that were mainly used included Google Scholar, Research Gate, MDPI, and Web of Science, using keywords such as cyber security, cyber threats, cyber-attacks, elements of cyber security, etc. The authors scrutinized and evaluated each paper to select the most pertinent information. A code sheet was constructed to document significant study-related information to aid this procedure. The study was completed in a stepwise process. In the initial stage, the data was extracted through relevant keywords and analyzed by going through the abstract/summary of the previous research first. Then, the results and methodologies were assessed. Meaningful data was collected from almost 43 studies that were published from the year 2015 to 2024. The studies from the last ten years were preferred to maintain the authenticity and reliability of data. The gathered data was then synthesized and summarized logically to make it comprehensive for readers.

IV. RESULTS AND DISCUSSION

An in-depth literature review suggested a holistic approach is needed to address cybersecurity issues in Saudi Arabia. A framework is being developed to incorporate essential tactics for dealing with arising security threats in various fields.

Figure 2
Cyber Security Model



This framework predominantly focuses on three factors: education and awareness, adoption of AI technology, and Revision of cyber policies.

4.1. Education and Awareness

Findings show that users need to be more aware of security threats and solutions that make them incompetent to deal with everyday security issues. Effective cybersecurity education and training are essential to equipping and training professionals to handle real-life security situations. These training and awareness campaigns can be provided to them from school to professional levels. Saudi Arabia is also putting effort into offering

courses on cyber security issues in different universities with practical learning. It is a great measure that can enhance understanding of cyber threats and their solutions.

4.2. Artificial Intelligence

Both artificial intelligence (AI) and cybersecurity are broad concepts that private and government organizations can use to reduce risks and boost income by identifying fraud and cyber threats. Since it's getting harder to stay on top of new viruses and malware updates with old cyber tools, cybersecurity with artificial intelligence technology will make it easier to identify risks and respond to malware by analyzing data from cyberattacks to determine the best action. Numerous AI applications, such as SIEM, spam filtering, secure user authentication, and hacking incident forecasting, are being utilized in cyber security solutions. These programs analyze malware actions based on previous history.

Given the dynamic nature of cybersecurity threats, prompt and automated reaction is needed, which is only possible through AI applications. Various AI techniques, including machine learning techniques, which do not always require prior training, can easily be incorporated into modern cyber security plans.

4.3. Revised Policies

Since constant cyber threats have already provoked Saudi Arabia, learning new systems and advanced technologies to boost cyber security policies is crucial. These policies can be based on educational and awareness campaigns that trained staff can provide to general IT users and professionals. These educational plans can target different age groups depending on their engagement in IT services.

Revised policies can also incorporate AI tools and processes to meet the latest technological needs to deal with sensitive cyber attacks. AI tools can effectively deal with severe cyber threats, so understanding AI is critical in designing cyber policies.

Moreover, some significant developments have been made in Saudi Arabia, especially in the tourism sector, to attract 100 million tourists by 2030. It is essential to focus on cybersecurity issues to avoid any unpleasant consequences in the context of security. Saudi Arabia plans to host the 2030 World Expo and the Football World Cup to enhance tourism and boost the economy. All these events need sensitive physical and digital security measures that the effective use of AI can do. The present study will assist in developing further security plans on local and international levels.

V. CONCLUSION

This paper helped find the critical elements in the digital world to deal with cyber threats. Since entering the digitalized world, cybersecurity has become a significant part of our lives. Cybersecurity management systems are now required at the state and corporate levels and dominate all spheres of our lives: political, social, and economic.

It was found that some new additions to the field of cyber security can enhance its productivity, such as education and awareness regarding cyber threats and cyber-attacks, alliance of AI and cyber security measures, and development of new policies that can effectively address modern threats.

5.1. Recommendations

The study aimed to investigate the key elements of an efficient cyber security system, but future studies can still reveal much.

1) IT professionals and security software developers must do research and create automated solutions to assist end users and organizations in mitigating cyber risks with the least amount of human participation.

2) It is essential to study the unhelpful factors creating barriers to cyber security measures in Saudi Arabia and other countries to control them tactfully.
3) AI-based studies would also be appreciated to make cyber security more powerful and effective in dealing with dangerous threats and viruses.

5.2. Limitations and Future Research Directions

The study exclusively focuses on Saudi Arabia, which may limit the findings' application to other countries with differing cyber-security landscapes or legal frameworks. Future studies can focus on the cyber-security strategies of different eastern and eastern countries to learn from their experiences.

1) The study does not primarily focus on a particular industry, such as finance or energy, that is not directing outcomes in a particular domain. Future studies can choose certain sectors to enhance their cyber-security criteria.
2) The world of cyber security is always changing, thanks to the introduction of new technology, tactics, and threats. Therefore, the study's results could be quickly out of date when new information comes to light.
3) Modifications to national cyber security laws or regulations made either during or after the study may impact the applicability and accuracy of the study's conclusions. Ongoing research is needed in the area of cyber security evolving matters so that the latest technologies can be adapted.
4) The study design (literature review) only represents past data, which is not enough to study the latest trends in the Saudi Arabian cyber-security department. Therefore, a survey design or a qualitative study can be done in the future to find unambiguous findings and accurate information.

REFERENCES

Ajmi, L., Alqahtani, N., Rahman, A. U., & Mahmud, M. (2019, May 1-3). *A novel cybersecurity framework for countermeasure of SME's in Saudi Arabia* (pp. 1-9). Paper presented at 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia. IEEE.

Al Nafea, R., & Almaiah, M. A. (2021, July 14-15). *Cyber security threats in cloud: Literature review* (pp. 779-786). Paper presented at International Conference on Information Technology (ICIT), Amman, Jordan. IEEE. Doi: 10.1109/ ICIT52682.2021.9491638.

Alasmari, A. (2021). *Key role of diplomacy in promoting international cybersecurity: A case study of Kingdom of Saudi Arabia*. Dissertation, Marymount University.

Alhalafi, N., & Veeraraghavan, P. (2021). Cybersecurity policy framework in Saudi Arabia: Literature review. *Frontiers in Computer Science*, *3*, 1-8. https://doi.org/10.3389/fcomp.2021.736874.

Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2016, December 5-7). *A survey of cyber-security awareness in Saudi Arabia* (pp. 154-158). Paper presented at 11th International Conference for Internet Technology and Secured Transactions (ICITST), Barcelona, Spain. IEEE. Doi: 10.1109/ICITST.2016.7856687.

Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon*, *7*(1), 1-13. https://doi.org/10.1016/j.heliyon.2021.e06016.

Arsene, A. L., & Rusu, B. (2020). *Iranian chafer APT targeted air transportation and government in Kuwait and Saudi Arabia*.

De Azambuja, A. J. G., Plesker, C., Schützer, K., Anderl, R., Schleich, B., & Almeida, V. R. (2023). Artificial intelligence-based cyber security in the context of industry 4.0—a survey. *Electronics*, *12*(8), 1920.

GDPC (Global Data Privacy and Cybersecurity Handbook). (2013). *Global data privacy and cybersecurity handbook*. Retrieved on https://resourcehub.bakermckenzie.com/en/resources/global-data-privacy-and-cybersecurity-handbook/emea/saudi-arabia/topics/key-data-privacy-and-cybersecurity-laws

Innab, N., Al-Rashoud, H., Al-Mahawes, R., & Al-Shehri, W. (2018, April). *Evaluation of the effective anti-phishing awareness and training in governmental and private organizations in Riyadh* (pp. 1-5). Paper presented at the 21st Saudi Computer Society National Computer Conference (NCC). IEEE.

Klaic, A. (2016). A method for the development of cyber security strategies. *Information & Security*, *34*(1), 37-55.

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176-8186.

Mughal, A. A. (2022). Well-architected wireless network security. *Journal of Humanities & Applied Science Research*, *5*(1), 32-42.

NCA (National Cybersecurity Authority). (2018). *Essential cybersecurity controls* (pp. 6-10).

Olech, A., & Siekierka, K. (2021). *Cybersecurity in Saudi Arabia*. Retrieved July 14, 2022.

Quadri, A., & Khan, M. K. (2019). *Cybersecurity challenges of the Kingdom of Saudi Arabia*.

Senol, M., & Karacuha, E. (2020). Creating and implementing an effective and deterrent national cyber security strategy. *Journal of Engineering*.

Shafqat, N., & Masood, A. (2016). Comparative analysis of various national cyber security strategies. *International Journal of Computer Science & Information Security*, *14*(1), 129-136.

Tsai, C. F., Hsu, Y. F., Lin, C. Y., & Lin, W. Y. (2009). Intrusion detection by machine learning: A review. *Expert Systems with Applications*, *36*(10), 11994-12000.

Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. *Ieee Access*, *8*, 23817-23837.