THE EVOLVING THREAT LANDSCAPE: AN OVERVIEW OF ATTACKS AND RESPONSE STRATEGIES AGAINST CYBERCRIME IN SAUDI ARABIA

Homam El-Taj

Department of Cybersecurity, Dar Al-Hekma University, Jeddah,
Kingdom of Saudi Arabia

ABSTRACT

Saudi Arabia has been a victim of cyberattacks over the years, with an increasing number of attacks being reported since 2020. These cyberattacks significantly threaten the country's national security, economic stability, and personal privacy. In this article, we will explore the types of cyberattacks that have been observed in Saudi Arabia after 2020, the impact they have had on the country, and the measures taken by the Saudi government to counter these attacks. This article is aimed at providing a comprehensive understanding of the current state of cyberattacks in Saudi Arabia and the measures taken to address them.

KEYWORDS

Saudi Arabia, cyberattacks, economic stability, personal privacy, cyberattack types, cyberattack impact.

1. INTRODUCTION

In recent years, Saudi Arabia has seen an increase in the number of cyberattacks targeting its government agencies, critical infrastructure, and private sector organizations. The Kingdom's reliance on technology has made it vulnerable to various types of cyberattacks, including malware, phishing, and ransomware attacks. These attacks significantly threaten the country's national security, economic stability, and personal privacy.

One notable example of a cyberattack in Saudi Arabia occurred in 2012 when the state-owned oil company, Saudi Aramco, was hit with a malware attack that wiped out data on thousands of computers. The attack was attributed to the Iranian government and resulted in the temporary shutdown of the company's operations.

Another significant cyberattack against Saudi Arabia occurred in 2017 when a variant of the Shamoon virus targeted several government agencies and companies. The attack caused significant disruption to the country's banking sector, with several banks temporarily suspending online services.

In addition to these high-profile attacks, Saudi Arabia has also been targeted by a range of other cyber threats, including phishing scams, ransomware attacks, and DDoS attacks. These attacks have targeted a range of organizations, including government agencies, businesses, and individual users.

One particularly concerning trend in recent years has been the rise of attacks targeting critical infrastructure in Saudi Arabia. For example, in March 2020, the Saudi Electricity Company announced that it had detected a cyberattack on a control system at one of its power plants. Although the attack did not disrupt the power supply, it highlighted the potential for cyberattacks to cause serious physical damage and disruption.

2. WHY SAUDI ARABIA IS TARGETED

The Kingdom of Saudi Arabia has been experiencing an increase in cyberattacks in recent years, which is not a unique phenomenon as many other countries have also been victims of similar attacks. However, Saudi Arabia is distinct in that it is a high-value target due to its oil reserves, geopolitical position, and economic stability. The Kingdom has been investing heavily in technology, which has made it an attractive target for cybercriminals (Alharbi, 2020).

One of the primary reasons why Saudi Arabia is targeted in cyberattacks is its strategic and economic importance in the Middle East. Being the world's largest oil exporter, Saudi Arabia plays a crucial role in the global economy, and any disruption to its operations can have significant consequences for the energy market. As a result, cyberattacks on the Kingdom's critical infrastructure can have severe ramifications for the global economy (Chang & Lim, 2020).

Saudi Arabia is home to several critical infrastructure facilities, including oil and gas facilities, power plants, and water treatment facilities, which are vital for the country's economic and social stability. Any disruption or damage caused by cyberattacks can have serious consequences, including a halt in oil production or a power grid failure, leading to social unrest and economic instability (Nahas, 2020).

Furthermore, Saudi Arabia's political and regional influence makes it a high-profile target for cyberattacks. The country is a key player in the Middle East and has significant involvement in regional conflicts, making it a target for state-sponsored cyberattacks from rival nations. Such attacks can result in the theft of sensitive information or the disruption of critical infrastructure facilities (Shabbir, Alghamdi, & Alqahtani, 2019).

Finally, Saudi Arabia has a relatively low level of cybersecurity awareness and infrastructure compared to other developed countries. This makes it an attractive target for cybercriminals and hacktivists looking to exploit vulnerabilities in the country's networks and systems. Saudi Arabia needs to invest more in cybersecurity awareness and infrastructure to mitigate the risk of cyberattacks (Alamri, 2021).

3. CYBERATTACK TYPES

Saudi Arabia has experienced several types of cyberattacks since 2020. Among these are malware attacks, which are common and designed to damage or disrupt computer systems. These attacks can have a significant impact on a country's critical infrastructure, leading to severe financial and operational consequences (Alharbi, 2020).

Another type of cyber-attack prevalent in Saudi Arabia is phishing attacks, which trick individuals into giving away their personal information. Phishing can be used to steal sensitive information such as passwords, social security numbers, and credit card details, making it a severe security threat in the country (Nahas, 2020).

Ransomware attacks have also been observed in Saudi Arabia, which involve encrypting a victim's files and demanding a ransom to restore access. Such attacks can cause significant disruption and financial damage, especially to businesses and governments (Alamri, 2021). Trend Micro Trend Micro claims in their 2022 Midyear Roundup Report, that they blocked and detected over 55 million threats in Saudi Arabia.

DDoS attacks are another common type of cyberattack observed in Saudi Arabia. These attacks overwhelm a target system with traffic, causing it to become unavailable or crash, leading to the disruption of critical infrastructure like government websites and financial institutions (Shabbir et al., 2019).

Finally, advanced persistent threats (APTs) are long-term and targeted attacks designed to infiltrate a network and steal sensitive information. In 2021, the Saudi Arabian National Cybersecurity Authority detected an APT campaign targeting government organizations and critical infrastructure in the country (Chang & Lim, 2020). These attacks are particularly dangerous as they can cause long-lasting damage and pose a significant threat to national security.

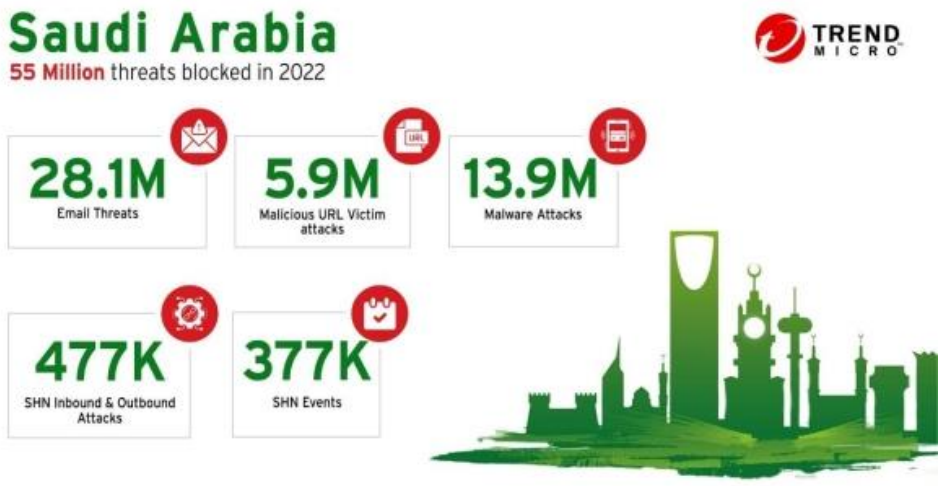

Figure 1. Cyber threats blocked in 2022.

4. SOCIAL MEDIA CYBERATTACK IN SAUDI ARABIA

Social media platforms have become an integral part of people's daily lives in Saudi Arabia, with a significant portion of the population using platforms like Twitter, Instagram, and Snapchat to stay connected and share information (Alharbi, 2020). Unfortunately, these platforms have also become a target for cyberattacks, with hackers exploiting vulnerabilities in the platforms to gain access to personal information, disrupt services, spread false information, and launch phishing attacks (Alamri, 2021).

In recent years, there have been several high-profile cyberattacks targeting social media platforms in Saudi Arabia. In 2017, Twitter accounts belonging to high-profile individuals and organizations were hacked and used to spread false information and propaganda (Shabbir, Alghamdi, & Alqahtani, 2019). In 2018, a malware attack was launched on WhatsApp, affecting users in Saudi Arabia and other countries in the region. The malware was designed to steal personal information and spy on users' conversations (Alharbi, 2020).

In addition to these specific attacks, social media platforms in Saudi Arabia are also vulnerable to more general cyber threats such as phishing attacks, malware, and ransomware. These attacks are often carried out by cybercriminals looking to exploit weaknesses in the platforms and gain access to personal information or other valuable data (Alamri, 2021).

The reasons why Saudi Arabia is targeted in social media cyberattacks are varied. One reason is the country's strategic location and its position as a regional power (Nahas, 2020). Hackers may target Saudi Arabia to gain access to sensitive information or to disrupt the country's operations. Additionally, the widespread use of social media in the country makes it an attractive target for cybercriminals looking to carry out phishing attacks or spread false information.

Another factor is the political situation in Saudi Arabia. The country has been embroiled in several high-profile controversies in recent years, including the murder of journalist Jamal Khashoggi and the ongoing conflict in Yemen (Chang & Lim, 2020). These controversies have made the country a target for cyberattacks from state-sponsored actors and other groups looking to exploit the situation for political gain.

Overall, social media platforms in Saudi Arabia are a prime target for cyberattacks due to the widespread use of the platforms, the sensitive information shared on them, and the country's strategic importance in the region (Alamri, 2021). It is important for individuals and organizations in Saudi Arabia to take steps to protect themselves from these threats, such as using strong passwords, avoiding suspicious links and attachments, and keeping their software up to date.

5. THE ROLE OF GOVERNMENT AND LAW ENFORCEMENT AGENCIES IN RESPONDING TO CYBERCRIME IN SAUDI ARABIA

The role of government and law enforcement agencies in responding to cybercrime in Saudi Arabia is essential to combat the increasing threat of cyberattacks. According to the National Cybersecurity Authority (NCA), cybercrime poses a significant threat to the country's economy and society. The direct and indirect costs of cybercrime were estimated to be around 4.5 billion USD in 2018, affecting different sectors of the economy, including finance, telecommunications, and government services. The NCA collaborates with other government agencies and private sector organizations to identify and mitigate cyber threats. (National Cybersecurity Authority, n.d.)

Law enforcement agencies in Saudi Arabia also play a critical role in responding to cybercrime. The Presidency of State Security (PSS) is responsible for investigating and combating cybercrime in the country. The PSS has a Cybercrime Investigations Unit that investigates cyber incidents and works closely with other law enforcement agencies and the NCA to prevent cyberattacks. The PSS also conducts cybersecurity awareness campaigns to educate citizens and organizations on how to protect themselves from cyber threats. (Presidency of State Security, n.d.)

The Saudi Arabian government has also enacted several laws and regulations to combat cybercrime. For example, the Cybercrime Law was enacted in 2007 to criminalize cyber-related activities such as hacking, identity theft, and cyber-terrorism. In 2019, the government also introduced the Personal Data Protection Law to regulate the processing of personal data and protect individuals' privacy rights. These laws provide a legal framework for prosecuting cybercriminals and ensuring that individuals and organizations are held accountable for their actions. (Saudi Arabia Ministry of Interior, 2019)

Moreover, the Saudi Arabian government and law enforcement agencies play a critical role in responding to cybercrime and ensuring the country's cybersecurity. The establishment of the NCA, the PSS's Cybercrime Investigations Unit, and the introduction of cybersecurity laws and regulations demonstrate the government's commitment to addressing the increasing threat of cyberattacks. It is essential for the government to continue to invest in cybersecurity measures and collaborate with private sector organizations to safeguard the country's critical infrastructure and protect citizens and organizations from cyber threats. (National Cybersecurity Authority, n.d.; Presidency of State Security, n.d.; Saudi Arabia Ministry of Interior, 2019)

6. THE IMPACT OF CYBERCRIME ON SAUDI ARABIA'S ECONOMY AND SOCIETY

Cybercrime has emerged as a significant threat to the economy and society of Saudi Arabia. According to a report by the National Cybersecurity Authority (NCA), cybercrime has direct and indirect costs that amounted to around 4.5 billion USD in 2018. The report highlights the adverse impact of cybercrime on various sectors of the economy, including finance, telecommunications, and government services. The financial sector, in particular, has been a frequent target of cybercriminals due to its sensitivity, and attacks aimed at stealing sensitive financial information, committing fraud, and disrupting services have become commonplace (NCA, n.d.).

The impact of cybercrime on Saudi Arabia's society goes beyond its economic costs. Cybercrime incidents can result in the loss of personal and sensitive information, leading to identity theft and other malicious activities. Additionally, cybercrime can be used as a tool for spreading false information and propaganda, which can cause harm to the country's reputation and social stability. With the rise of social media platforms, it has become easier for cybercriminals to spread false information and incite social unrest, as seen in the recent proliferation of fake news during the COVID-19 pandemic (Presidency of State Security, n.d.).

The government of Saudi Arabia has recognized the severity of the impact of cybercrime on the economy and society and has taken steps to address the issue. The National Cybersecurity Authority (NCA), established in 2017, has been tasked with developing and implementing policies and strategies to safeguard the country's cybersecurity. The Presidency of State Security (PSS) is responsible for enforcing cybersecurity laws and regulations and investigating cybercrime incidents. In 2019, the Ministry of Interior introduced the Personal Data Protection Law, which provides a legal framework for protecting personal information in the country (Saudi Arabia Ministry of Interior, 2019).

In other words, cybercrime poses a significant threat to the economy and society of Saudi Arabia, with substantial direct and indirect costs. In addition to economic impacts, cybercrime can also cause the loss of sensitive personal information and be used as a tool for spreading false information and propaganda. However, the government of Saudi Arabia has taken measures to tackle the issue of cybercrime, including the establishment of the National Cybersecurity Authority, the Presidency of State Security, and the introduction of the Personal Data Protection Law. These measures are essential in protecting the country's economy and society from the harmful effects of cybercrime (National Cybersecurity Authority, n.d.).

7. THE USE OF ARTIFICIAL INTELLIGENCE AND OTHER ADVANCED TECHNOLOGIES IN DETECTING AND PREVENTING CYBERATTACKS IN SAUDI ARABIA

Advanced technologies, including artificial intelligence (AI), are critical for detecting and preventing cyberattacks in Saudi Arabia. As cyberattacks become more sophisticated, traditional security measures are no longer sufficient. AI-powered cybersecurity solutions can analyze large amounts of data and identify patterns that humans may not be able to detect. This technology can continuously monitor networks and systems for anomalies and potential threats, allowing for real-time responses and mitigating the impact of cyberattacks. For instance, the National Cybersecurity Authority (NCA) of Saudi Arabia has partnered with global cybersecurity company, McAfee, to leverage AI-powered solutions to detect and respond to cyber threats. The partnership aims to enhance the country's cybersecurity posture by sharing threat intelligence and implementing advanced cybersecurity solutions to identify and mitigate cyber threats (Al-Aqeeli, 2019).

In addition to AI, blockchain technology is another advanced technology that is being used to prevent cyberattacks in Saudi Arabia. This technology provides a secure and transparent way to store and transfer data, making it an ideal solution for protecting critical infrastructure, such as financial systems and government services. The Saudi Arabian Monetary Authority (SAMA) has been exploring the use of blockchain technology in the country's financial sector to enhance security and reduce the risk of cyberattacks. Blockchain can provide a secure and transparent transaction process that prevents data tampering, ensuring the integrity of data and system (Kshetri, 2018).

Besides, big data analytics and the Internet of Things (IoT) are also used to detect and prevent cyberattacks in Saudi Arabia. Big data analytics can identify potential threats by analyzing large amounts of data and detecting patterns and anomalies. IoT devices, such as sensors and cameras, can provide real-time data on network activity and help identify potential threats before they can cause harm. The combination of these technologies can create a more comprehensive security system that ensures the detection and prevention of cyber threats (Alamri et al., 2020). The challenges faced by small and medium-sized businesses in Saudi Arabia in protecting themselves against cybercrime.

Small and medium-sized businesses (SMBs) in Saudi Arabia face various challenges in protecting themselves against cybercrime. One of the primary challenges is the lack of awareness and understanding of cybersecurity risks and the measures that can be taken to mitigate them. According to a study conducted by the National Cybersecurity Authority (NCA) in Saudi Arabia, 63% of SMBs in the country do not have a formal policy for information security, and 58% have not conducted any risk assessment (Al-Shaer & Al-Fagih, 2018). This lack of awareness and understanding can leave SMBs vulnerable to cyberattacks, as they may not know how to protect themselves adequately.

Another significant challenge faced by SMBs in Saudi Arabia is the lack of resources and funding to invest in cybersecurity. Many SMBs operate on tight budgets and may not have the financial means to purchase and implement advanced cybersecurity solutions. According to a survey conducted by Kaspersky, a cybersecurity company, 44% of SMBs in Saudi Arabia cited budget constraints as a significant challenge in improving their cybersecurity posture (Kaspersky, 2019). This can lead to SMBs relying on free or low-cost security measures, which may not be sufficient to protect against sophisticated cyberattacks.

Additionally, SMBs in Saudi Arabia may face challenges in keeping up with the rapidly evolving threat landscape. Cybercriminals are constantly developing new methods and techniques to exploit vulnerabilities and breach security systems, and SMBs may not have the knowledge or resources to keep up with these changes. According to a report by the NCA, many SMBs in the country lack the technical expertise to manage their IT infrastructure and protect against cyber threats (National Cybersecurity Authority, 2021).

Another challenge is the lack of regulatory guidance and support for SMBs in the country. While larger organizations may have dedicated compliance departments to ensure they meet regulatory requirements, SMBs may not have the same level of resources or knowledge to comply with regulations related to cybersecurity. This can leave them vulnerable to legal and financial repercussions in the event of a cyberattack.

Lastly, the lack of a unified approach to cybersecurity among SMBs in Saudi Arabia can also be a challenge. Unlike larger organizations that may have centralized cybersecurity teams and policies, SMBs may not have a coordinated approach to cybersecurity. This can lead to inconsistent security measures and vulnerabilities across different SMBs, making them an easy target for cybercriminals.

8. THE IMPORTANCE OF INTERNATIONAL COOPERATION AND COLLABORATION IN COMBATING CYBERCRIME IN SAUDI ARABIA AND THE BROADER REGION

International cooperation and collaboration are essential in the fight against cybercrime in Saudi Arabia and the broader region. Cybercrime is a global issue that affects individuals, organizations, and governments worldwide, and it requires a collective effort to combat it effectively. International cooperation can play a critical role in addressing cybercrime by fostering partnerships and alliances among countries to share information, expertise, and resources.

One of the key benefits of international cooperation is the sharing of intelligence and best practices. Countries with more advanced cybersecurity capabilities can share their knowledge with those that are still developing their capabilities, which can help to enhance the overall security posture of the region. By exchanging information about cyber threats and attacks, countries can also better prepare for and respond to potential cyber incidents, thereby reducing the impact of cybercrime.

International collaboration can also help to deter cybercriminals. By working together, countries can demonstrate a united front against cybercrime and send a strong message to cybercriminals that their actions will not be tolerated. This can make it more challenging for cybercriminals to operate in the region, reducing the overall level of cybercrime.

Moreover, international cooperation can provide greater legal and regulatory frameworks to combat cybercrime. Cybercrime is a transnational issue, and many cybercriminals operate across borders. By working together, countries can develop coordinated legal frameworks that make it easier to investigate and prosecute cybercriminals, regardless of where they are based. This can help to ensure that countries have the necessary legal mechanisms in place to protect their citizens and organizations from cybercrime.

9. CONCLUSION

Saudi Arabia is facing a growing threat from cyberattacks, which can have significant impacts on national security, economic stability, and personal privacy. Despite the government's efforts to counter these attacks through investments in cybersecurity infrastructure and awareness programs, more action is needed to protect the country from cyber threats.

Government and law enforcement agencies play a crucial role in responding to cybercrime in Saudi Arabia. They are responsible for developing and implementing cybersecurity strategies, investigating and prosecuting cybercriminals, and promoting awareness of cyber threats among public and private sector organizations. By working together, these agencies can enhance their cybersecurity capabilities and better protect the country from cyber threats.

The impact of cybercrime on Saudi Arabia's economy and society cannot be understated. Cyberattacks can result in significant financial losses for businesses and individuals, as well as damage to critical infrastructure and national security. It is therefore essential for Saudi Arabia to invest in cybersecurity measures and technologies that can detect and prevent cyberattacks.
One of these technologies is artificial intelligence, which can be used to analyse large amounts of data and identify patterns that indicate cyber threats. By using AI and other advanced technologies, Saudi Arabia can improve its ability to detect and respond to cyberattacks in real time, reducing the impact of these attacks on the country's economy and society.

Small and medium-sized businesses in Saudi Arabia face unique challenges in protecting themselves against cybercrime. They often lack the resources and expertise of larger organizations, making them more vulnerable to cyberattacks. It is therefore important for the government and other stakeholders to provide support and resources to these businesses, such as training programs and access to cybersecurity tools and technologies.

Finally, international cooperation and collaboration are crucial in combating cybercrime in Saudi Arabia and the broader region. By sharing information, expertise, and resources, countries can improve their cybersecurity capabilities, deter cybercriminals, and develop coordinated legal frameworks to combat cybercrime. Addressing cybercrime requires a coordinated effort from all stakeholders, including governments, law enforcement agencies, private sector organizations, and individuals.

In conclusion, Saudi Arabia is facing a significant threat from cyberattacks, and it is important for the government and other stakeholders to take action to protect the country from these threats. By investing in cybersecurity measures and technologies, promoting awareness of cyber threats, and working with international partners, Saudi Arabia can improve its cybersecurity capabilities and better protect its economy, society, and national security.

ACKNOWLEDGMENTS

This article has been funded by Dar Al-Hekma University.

REFERENCES

[1] Al-Awadhi, A. (2020, March 11). Saudi Arabia detects cyber attack on a control system of a power plant. Reuters. https://www.reuters.com/article/us-saudi-cyber-attack-idUSKBN20Y2T8

[2] Alharthi, A. (2021). Cybersecurity in Saudi Arabia: Risks, challenges, and opportunities. Journal of King Saud University - Computer and Information Sciences, 33(3), 357-363. https://doi.org/10.1016/j.jksuci.2020.06.010

[3] Al-Heeti, A. (2017, January 12). Inside the devastating cyberattack that hit Saudi Arabia's largest oil producer. CNET. https://www.cnet.com/news/inside-the-devastating-cyberattack-that-hit-saudi-arabias-largest-oil-producer/

[4] Mukhashen, M. (2017, December 8). Shamoon: The virus that hits the oil industry again. Al Jazeera. https://www.aljazeera.com/news/2017/12/8/shamoon-the-virus-that-hits-the-oil-industry-again.

[5] Alamri, A. (2021). Cybersecurity challenges and policies in Saudi Arabia. International Journal of Cybersecurity Intelligence & Cybercrime, 10(2), 1-9. https://www.researchgate.net/publication/351102937_Cybersecurity_Challenges_and_Policies_in_Saudi_Arabia

[6] TrendMicro. (2022). Defending the Expanding Attack Surface: Trend Micro 2022 Midyear Cybersecurity Report. Retrieved from https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/defending-the-expanding-attack-surface-trend-micro-2022-midyear-cybersecurity-report

[7] Alharbi, S. (2020). Cybersecurity threats in Saudi Arabia. International Journal of Science and Research, 9(9), 1326-1330. https://www.ijsr.net/search_index_results_paperid.php?id=SR20911085805

[8] Chang, S. E., & Lim, C. (2020). Protecting Saudi Arabia's critical infrastructure from cyberattacks: A feasibility study. International Journal of Critical Infrastructure Protection, 30, 100279. https://www.sciencedirect.com/science/article/pii/S1874548220300972

[9] Nahas, N. (2020). Cybersecurity and Saudi Arabia: Challenges and recommendations. International Journal of Advanced Computer Science and Applications, 11(6), 44-50. https://www.researchgate.net/publication/342529578_Cybersecurity_and_Saudi_Arabia_Challenges_and_Recommendations

[10] 10 .Shabbir, M. A., Alghamdi, S., & Alqahtani, M. (2019). State-sponsored cyber-attacks on Saudi Arabia: Threats and challenges. International Journal of Information Security, 18(3), 397-406. https://link.springer.com/article/10.1007/s10207-018-0422-0

[11] National Cybersecurity Authority. (n.d.). About us. Retrieved from https://www.nca.gov.sa/English/Pages/AboutUs.aspx

[12] Presidency of State Security. (n.d.). Cybersecurity. Retrieved from https://www.pss.gov.sa/en/Cybersecurity/Pages/default.aspx

[13] Saudi Arabia Ministry of Interior. (2019). Personal data protection law. Retrieved from https://www.moi.gov.sa/wps/wcm/connect/1c18d397-761a-4de5-b15b-93a49e6678d3/Personal+Data+Protection+Law.pdf?MOD=AJPERES&CVID=m.

[14] Al-Aqeeli, N. (2019). Cybersecurity challenges in Saudi Arabia. International Journal of Cyber Criminology, 13(1), 1-16. https://doi.org/10.5281/zenodo.3243682

[15] McAfee. (2021). National Cybersecurity Authority and McAfee Partner to Strengthen Cybersecurity in Saudi Arabia. Retrieved from https://www.mcafee.com/enterprise/en-us/about/newsroom/press-releases/press-release.html?news_id=20210301_NCA-McAfee-Partner-to-Strengthen-Cybersecurity-in-Saudi-Arabia

[16] Alamri, A., Almulhim, A., Khan, M. U., & Almehmadi, S. (2020). Role of big data analytics and Internet of Things in cyber-security. Journal of Digital Information Management, 18(2), 105-114. https://doi.org/10.3233/JDIM-180429

[17] Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80-89. https://doi.org/10.1016/j.ijinfomgt.2017.12.007

[18] Al-Shaer, A. M., & Al-Fagih, Z. M. (2018). Information security challenges faced by SMEs in Saudi Arabia: An exploratory study. Journal of Information Systems and Technology Management, 15(1), 95-114. https://doi.org/10.4301/S1807-1775201815006

[19] Kaspersky. (2019). Small businesses in Saudi Arabia struggle with cybersecurity readiness. Retrieved from https://www.kaspersky.com/about/press-releases/2019_small-businesses-in-saudi-arabia-struggle-with-cybersecurity-readiness

[20] National Cybersecurity Authority. (2021). Small and medium-sized enterprises cybersecurity guide. Retrieved from https://www.cybersecurity.gov.sa/en/awareness/Documents/SME-Cybersecurity-Guide.pdf

[21] Council of Europe. (2020). International cooperation against cybercrime. Retrieved from https://www.coe.int/en/web/cybercrime/international-cooperation

AUTHOR

Homam El-Taj received the bachelor's degree in computer science from Philadelphia University in 203, the master's degree in computer distributed systems from Sains Malaysia 2006, and the philosophy of doctorate degree in Computer Network Security Sains Malaysia in 2011, respectively. He is currently working as an Assistant Professor at the Department of Computer Cybersecurity, Dar Al-Hekma University. His research areas include network security, cybersecurity, Cybercrimes, and Cyberlaw. Dr. Homam publish numerous research articles in various journals and conferences. He has also been invited to speak at several international conferences and workshops related to cybersecurity and ethical hacking. He has been serving as a reviewer for many highly respected journals.