INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 14, Issue 6, (2024) E-ISSN: 2222-6990

Cyber Security and Cyber Threats in the Jordan Business Context

Alanoud Amer Saleem Alrkeebat
Charisma University

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v14-i6/21991 DOI:10.6007/IJARBSS/v14-i6/21991

Published Date: 29 June 2024

Abstract

In today's digital world, cyber security has become a top priority for companies, particularly in Jordan. Owing to the fast assimilation of technology and the growing dependence on digital platforms, enterprises in Jordan encounter an extensive array of cyber hazards that have the potential to jeopardize their information, functions, and standing. The purpose of this article is to present a thorough study of the common cyber threats and cyber security strategies in the context of Jordanian company. This research outlines the main cyber threats that Jordanian firms face, including malware, phishing attacks, distributed denial-of-service (DDoS) assaults, and advanced persistent threats (APTs), through a thorough analysis of the literature that has already been published and industry reports. Because these risks have the potential to cause data breaches, financial losses, and operational interruptions, it is crucial that businesses put strong cyber security measures. The paper delves deeper into the cyber security tactics and best practices that Jordanian companies have used to lessen these risks. Implementing intrusion detection and prevention systems, firewalls, encrypting critical data, carrying out frequent vulnerability assessments, and raising employee understanding of cybersecurity through training and educational initiatives are some of these precautions. Through an analysis of the consequences of cyberattacks and the efficacy of different cyber security strategies, this research offers important information that Jordanian companies may use to improve their cyber resilience. It also emphasizes how crucial it is for the public and commercial sectors to work together with cybersecurity specialists to create a thorough cybersecurity framework that protects the country's digital infrastructure and promotes a safe business climate.

Keywords: Cyber Threats, Jordan, Business Security, Cyber Security, Digital Resilience, Risk Mitigation

Introduction

In the digital age, cyber security has become a critical issue for companies, especially in Jordan. Organizations are more susceptible to a variety of cyberthreats that might jeopardize their operations, data integrity, and reputation as a result of their growing reliance on

information and communication technology (ICT) to spur efficiency, innovation, and growth (Darwazeh et al., 2015). Strong cyber security protocols are more important than ever in the context of Jordanian company. Cybersecurity is the collective application of plans, strategies, tactics, engagements, training, best practices, assurance, and expertise to safeguard information systems, organizations, and related assets from cyber-attacks, according to the International Telecommunication Union (ITU, 2008). According to Al-Sayyed et al (2019), the swift integration of ICT in Jordan has created new prospects for enterprises, allowing them to improve cooperation, optimize workflows, and broaden their market penetration. A proactive strategy to cybersecurity is now necessary, though, as this digital revolution has also exposed firms to previously unheard-of cyber hazards.

The motivation for this study stems from the critical need to address the growing cybersecurity challenges faced by Jordanian businesses in an increasingly digital landscape. As cyber threats continue to evolve in sophistication and frequency, there is an urgent requirement for a comprehensive understanding of both the threat landscape and effective countermeasures specific to the Jordanian business context. This research contributes to the existing body of knowledge by providing an up-to-date analysis of cyber threats tailored to Jordan's unique business environment, along with practical, actionable strategies for enhancing cyber resilience. By bridging the gap between theoretical cybersecurity concepts and their practical application in Jordanian enterprises, this study aims to equip business leaders, IT professionals, and policymakers with the insights needed to strengthen the country's overall cybersecurity posture.

Businesses in Jordan are subject to a wide variety of cyberthreats, such as advanced persistent threats (APTs), malware, phishing attempts, and distributed denial-of-service (DDoS) attacks (Alghusin, & Al-Ajlouni, 2020). According to Al-Khateeb et al (2022), these dangers have the potential to cause disastrous outcomes, including financial losses, operational interruptions, data breaches, and reputational harm. Strong security measures are required since organizations engage with partners and stakeholders more often and share networks and data, which increases the danger of cyberattacks (Al-Khateeb and Al-Nuemat, 2018). Furthermore, the emergence of cloud computing has caused organizational network borders to become less distinct, posing new cybersecurity dangers and difficulties (Al-Sayed et al., 2019). Businesses in Jordan must negotiate this challenging environment to safeguard their digital assets, preserve business continuity, and promote innovation (Al-Khateeb et al., 2021).

Businesses in Jordan must implement a thorough cybersecurity plan that includes risk assessment, incident response planning, security awareness training, and the use of cutting-edge security technologies in order to lessen these cyberthreats (Alghusin, & Al-Ajlouni, 2020). Establishing a strong cybersecurity framework that protects the country’s digital infrastructure and promotes a secure business environment requires cooperation between the private sector, governmental organizations, and cybersecurity specialists (Al-Khateeb and Al-Nuemat, 2018).

The purpose of this study is to give a thorough analysis of the most common cyberthreats and cybersecurity countermeasures in the context of Jordanian company. This study looks at the effects of cyberthreats and the efficacy of different cybersecurity tactics in an effort to provide insightful analysis and helpful suggestions for Jordanian companies looking to improve their cyber resilience and prosper in the digital era.

Cyber Threats

Businesses in Jordan are exposed to a great deal of risk from cyber-attacks, which may seriously harm operations, reputation, and data integrity (Alghusin, & Al-Ajlouni, 2020). Cybercrime and cyberwarfare are the two primary categories into which these threats may be generally divided. The use of computer technology to obstruct a state, organization, or vital infrastructure in order to achieve military or strategic objectives is known as cyberwarfare (Al-Khateeb et al., 2021). When it comes to enterprises, cyberwarfare can refer to deliberate assaults by nation-states or persistent and sophisticated threats (APTs) with the intention of stealing confidential information or interfering with daily operations (Al-Sayyed et al., 2019).

However, a broad variety of illicit acts involving the use of computers, networked devices, or networks are included in cybercrime (Darwazeh, Al-Qassas, & AlDosari, 2015). According to Al-Khateeb and Al-Nuemat (2018), these actions could involve financial fraud, data breaches, theft of intellectual property, and the dissemination of malware or unlawful material. Businesses in Jordan must contend with a range of cyberthreats, such as advanced persistent threats (APTs), malware infections, phishing scams, and distributed denial-of-service (DDoS) assaults (Alghusin, & Al-Ajlouni, 2020). Malware, which includes Trojan horses, worms, and viruses, may seriously harm networks and computer systems, resulting in lost data, system outages, and monetary losses (Erbschloe, 2004). Businesses in Jordan frequently face the possibility of phishing attacks, which entail deceiving customers into disclosing confidential information or downloading malicious software (AlSobeh et al., 2023). Businesses may face serious repercussions from these cyberthreats, such as interrupted operations, monetary losses, harm to their reputation, and legal ramifications (Kala, 2023). Therefore, in order to reduce these risks, it is imperative that Jordanian enterprises develop a strong cybersecurity culture and put in place strong cybersecurity procedures.

Cyber Security

According to Verma & Shri (2022), cyber security is the process of preventing malevolent cyberattacks and illegal access to computers, servers, mobile devices, networks, and data. As businesses depend more and more on digital systems and data to power their operations and competitiveness, cyber security has become essential in the Jordanian business environment (Amer & Al-Omar, 2023).

Using a variety of remedies to lessen cyber risks is essential for effective cyber security in Jordanian organizations (Alghusin, & Al-Ajlouni, 2020). The implementation of advanced security technologies like firewalls, intrusion detection/prevention systems, and encryption, as well as regular software patching and vulnerability management, are some examples of these countermeasures (Jimmy, 2024). Employee training on cybersecurity policies, access controls, and authentication mechanisms are also possible.

In addition, it is imperative that companies develop a strong cybersecurity culture where workers comprehend and apply security best practices in order to improve cyber resilience in the Jordanian business environment (Kanaan et al., 2024). By putting strong cyber security measures in place and encouraging a security-aware mentality, Jordanian companies can better safeguard their digital assets and lessen the risks associated with cyber threats.

Objective and Purpose of the Paper

Given the growing dependence on digital technology and the constantly changing cyber threat environment, the purpose of this paper is to present a thorough examination of the

most common cyber risks and cybersecurity countermeasures in the context of Jordanian business. The paper's main goal is to identify and investigate the main cyber threats that Jordanian enterprises must deal with, along with their characteristics, origins, and possible repercussions.

Literature Review

Businesses are undergoing a digital revolution that has brought with it previously unheard-of opportunities and difficulties, especially in the area of cyber security. Organizations in Jordan are becoming more susceptible to a variety of cyber threats as they utilize technologies including cloud computing, the Internet of Things (IoT), and mobile apps (Obaidat et al., 2020). This study of the literature looks at the important discoveries and gaps in the body of knowledge about cybersecurity measures and cyber threats in the context of Jordanian business.

Cyber Threats in the Jordanian Business Context

Businesses in Jordan confront a wide range of constantly changing cyberthreats. In research on cybersecurity in Jordan's banking industry, Alghusin, & Al-Ajlouni, (2020) identified a number of dangers, including phishing assaults, malware infections, and advanced persistent threats (APTs). They discovered that these risks pose serious dangers to the banking sector since they can result in large-scale financial losses, data breaches, and operational disruptions.

Al-ma'aitah, (2022) investigated the idea of a cybersecurity culture in Jordan, stressing the value of staff involvement and knowledge in reducing cyber threats. According to their analysis, insider threats—such as negligent or hostile workers—pose a serious risk to Jordanian companies because they have the potential to purposefully or unintentionally compromise confidential data or assist cyberattacks.

The influence of cloud computing usage on cybersecurity in Jordanian enterprises was examined by (Al-Sayyed et al., 2019). They discovered a number of risks associated with the cloud, such as data breaches, denial-of-service (DDoS) assaults, and the possibility of illegal access to private information kept on cloud servers. Their conclusions made clear that strong governance structures and security precautions were required to guarantee Jordan's safe cloud computing adoption.

Cybersecurity Measures and Strategies

Various cybersecurity tactics and procedures have been introduced by Jordanian organizations in response to the increasing cyber threats. A safe cloud computing paradigm based on data categorization was presented by Lacuška & Peráček (2021) with the goal of improving data security and privacy in cloud environments. Their solution uses data anonymization, access restrictions, and encryption to reduce the hazards related to cloud computing.

Field research on cybersecurity risk management in information systems was carried out by (Mokhor et al., 2020). The deployment of firewalls, intrusion detection/prevention systems, frequent software patching, and staff education on cybersecurity best practices are just a few of the crucial tactics they mentioned. The significance of a comprehensive strategy for cybersecurity that incorporates organizational regulations, technical controls, and human aspects was underscored by their findings.

The study conducted by Amer & Al-Omar (2023) investigated the impact of cybersecurity awareness and training initiatives on improving the cybersecurity posture of enterprises in Jordan. Their research showed that since human mistake and ignorance may seriously compromise cybersecurity efforts, it is imperative that companies foster a culture of security consciousness and provide ongoing staff education.

Impact of Cyber Threats and Cybersecurity Measures

Previous studies have examined the effects of cyberthreats and the efficacy of cybersecurity protocols on enterprises in Jordan. In the smart city of Amman et al (2022) carried out a case study on Internet of Things (IoT) cybersecurity. They noted a number of possible dangers connected to Internet of Things devices, including the possibility of cyber-physical assaults, illegal access, and data breaches. The significance of strong security protocols and incident response systems in reducing the dangers associated with IoT installations in smart cities was underscored by their findings.

The financial effects of cybersecurity events on Jordanian organizations were examined by (Al-ma'aitah, 2022). According to their research, cyberattacks may cause large financial losses in the form of both direct (such as cleanup expenses and legal fees) and indirect (such as reputational harm and a decline in consumer trust) costs. They emphasized the necessity for businesses to invest in cybersecurity first and to manage cybersecurity risk using a risk-based strategy.

Methodology

The primary research approach used in this study was the application of quantitative research methodologies. Secondary data that was taken from other related research that had already been published online was used in this study. The studies were selected for retrieval based on their pertinence to the subject matter, and their contents were subjected to thematic analysis.

Discussion and Findings

This study included a number of prior research papers on the subject that had been published in various publications with information on countermeasures and cyber security risks from various organizations, including the government and other major corporations. The following is a discussion of the findings:

Cyber Threats

Businesses in Jordan are becoming more and more digitally savvy, which has opened them up to a variety of cyberthreats that might jeopardize the availability, confidentiality, and integrity of their information systems and information (Aswathy, Tyagi, & Kumari, 2021). Any successful cyberattack has the potential to have serious repercussions, such as revenue loss, reputational harm, and the disclosure of private, proprietary, or economic information (Alghusin & Al-Ajlouni, 2020). Some of the major cyberthreats that Jordanian firms have to deal with are as follows:

Insider Threats

Businesses in Jordan are at serious danger from insider threats, which occur when staff members intentionally misuse or target company computer assets for personal gain, retaliation, or other motives (Schoenherr et al., 2022). System administrators are examples

of privileged users who can abuse their high-level access to launch attacks on the organization's systems, get illegal access, or misuse the rights of other users (Sindiren & Ciylan, 2018).

PBX/VoIP Fraud

When outside parties breach a company's VoIP (Voice over Internet Protocol) or PBX (Private Branch Exchange) phone system and make unlawful calls on the company's account, it is known as PBX/VoIP fraud (Naaman et al., 2022). According to Jørgensen (2022), hackers may be able to access the phone system and use it to make false calls to premium rate lines, leaving the organization responsible for paying for them.

Social Media Threats

According to Obeidat at al (2018), social media platforms have become a haven for cyber threats in Jordan. These threats often take the shape of phony offers intended to deceive users into disclosing their login credentials or installing dangerous software. According to Diwan (2021), hackers may also distribute phony plugins or extensions that, whenever installed, infect the consumer's computer and steal confidential data.

Distributed Denial-of-Service: Attacks

DDoS assaults, which try to prevent legitimate users from accessing websites, servers, and IT infrastructures, are a frequent danger faced by organizations in Jordan (Owen et al., 2021). These assaults, which take advantage of holes in applications and network communication protocols, might come from hacked systems at hosting service providers or sites outside the jurisdiction of international authorities (Alghusin & Al-Ajlouni, 2020).

Botnet Attacks

Botnets are networks of hacked devices that are dispersed throughout the internet and are the source of botnet assaults (Owen et al., 2021). The possibility for botnets to proliferate increases as more devices in Jordan are linked to the internet. This gives cybercriminals the ability to attack targets including government organizations and financial institutions with the intention of committing fraud, causing disruption, or stealing data (Al-Sayyed et al., 2019).

Cyber Espionage

Theft of secret or private data kept digitally on information technology (IT) and networks is known as cyber espionage (Alghusin & Al-Ajlouni, 2020). Driven by economic, political, or competitive objectives, state-sponsored or well-funded groups use sophisticated tactics to gain access to networks and steal information covertly (Ahmad et al., 2019). Jordan's cyber threat landscape is ever-changing due to the advancement of technology and the sophistication of hackers. To lessen these threats and safeguard their digital assets, business operations, and reputation, companies in Jordan need to continue being watchful and aggressive in their cybersecurity endeavors.

Technical controls, organizational rules, employee awareness, and training are all necessary components of a multi-layered strategy for effective cyber threat management (Naseer, 2020). Safeguarding against external dangers requires putting strong security measures in place, like firewalls, intrusion prevention/detection systems, the use of encryption, and accessibility restrictions (Saxena et al., 2020). But enterprises also need to

deal with insider threats by monitoring employees, enforcing strict access restrictions, and developing a robust cybersecurity culture (Cappelli et al., 2012).

Furthermore, international cooperation and public-private sector collaboration are critical for thwarting cyberthreats that cut across national borders (Ikitemur, 2014). Jordan's total cyber resilience may be improved by putting in place efficient cybersecurity oversight frameworks, information sharing channels, and incident response procedures (Mohebbi et al., 2020). Businesses in Jordan may better safeguard their digital assets, stakeholders, and operations by being aware of the most common cyber risks and putting in place the necessary countermeasures. This will help to create a safe and resilient corporate environment in the digital age.

Countermeasures Related to Cyber Security

To effectively neutralize the wide spectrum of cyber risks that firms in Jordan confront, a comprehensive approach combining many countermeasures is necessary. These countermeasures fall into three categories: technological, organizational, and human-centric. Each of these three types of countermeasures is essential to improving the overall cyber resilience of a company.

Countermeasures Related to Insider Threats

Because insider threats involve individuals who may purposefully or inadvertently compromise organizational cyber assets, they represent a serious danger to Jordanian organizations (Cappelli et al., 2012). Organizations should use the following steps to lessen these threats:

Security awareness training: Consistent training initiatives should be carried out to teach staff members how to spot and react to social engineering schemes, phishing scams, and other malicious activity vectors.

Strong access controls: According to Cappelli et al (2012), putting in place measures like role-based access restrictions and two-factor authentication can help thwart unwanted access and reduce the possibility of power abuse.

Monitoring and auditing: Regularly reviewing system logs and keeping an eye on user activity can help identify insider threats and take fast action against them.

Security culture: A key element in reducing insider threats is cultivating a strong security culture within the company, where staff members are aware of and supportive of cybersecurity best practices.

PBX/VoIP Fraud Countermeasures

The following countermeasures should be taken into consideration by Jordanian enterprises in order to counteract PBX/VoIP fraud, which occurs when outside parties obtain illegal access to an organization's phone system:

Segregated traffic: Voice traffic sniffing by internal hackers can be avoided by implementing virtual LANs (VLANs) to separate voice and data traffic.

QoS, or quality of service, Reliable voice communication may be ensured by implementing QoS should take precedence voice traffic over data traffic.

Traffic monitoring: It might be helpful to spot and look into any fraud attempts to continuously monitor voice traffic and spot odd increases.

Call restrictions: You may detect and stop unwanted call patterns by limiting international calls to certain phone numbers and keeping an eye on call detail records (CDRs) (Alghusin & Al-Ajlouni, 2020).

Social Media Threats Countermeasures

In order to reduce the risks associated with social media, including malware dissemination and phishing attempts, Jordanian enterprises have to use a dual strategy:

Employee awareness: Regularly educating staff members about social media hazards, including phishing attempts and social engineering techniques, through awareness training (Aldawood & Skinner, 2019).

Okpa et al (203) defines policy enforcement as the process of putting into place and upholding corporate policies that specify how social media should be used and how cases of phishing and social engineering should be handled.

Distributed Denial-of-Service Attacks Countermeasures

DDoS attacks seek to prevent legitimate users from accessing websites, services, or entire infrastructures by flooding them with traffic from compromised systems. In order to counteract these attacks, Jordanian businesses should think about the following measures:

Network segmentation: dividing up internal and external networks, especially those that house critical systems, to reduce the attack surface alongside potential impact.

Vulnerability management: implementing automated scanning along with patching of potential distributed denial of service risk factors in internet-facing services to lower the risk of exploitation.

DDoS protection services include working with Internet service providers (ISPs) to put DDoS protection agreements into practice. These agreements may include traffic filtering, IP blocking, or black-holing, among other tactics (Alghusin, & Al-Ajlouni, 2020).

Countermeasures for Botnet Attacks

Botnet assaults: These are online attacks carried out by cybercriminals using hacked machines, or “botnets,” that are dispersed over the internet. Businesses in Jordan should think about implementing the following countermeasures:

Traditional defenses: locating and taking down the botnets’ central command and control infrastructure, frequently working with ISPs and law enforcement.

Strategies for mitigation: putting in place technological controls to limit the bandwidth that botnets may use, so slowing them down and lessening their influence.

Manipulation techniques: Making use of holes in botnets’ command interfaces to send orders that impair or destroy the botnets’ ability to function.

Vulnerability management is the process of routinely patching and upgrading systems to fix flaws that hackers could use to build new botnets.

Cyber Espionage Countermeasures

A multifaceted strategy is needed to counter cyber espionage, which entails the stealing of private or sensitive data:

Protecting sensitive information from illegal access or exfiltration requires putting strong data encryption, access restrictions, and data loss prevention mechanisms in place.

Threat intelligence: Recognizing and countering ongoing cyberespionage operations by utilizing cutting-edge threat analysis techniques and threat intelligence services (Imam et al., 2023).

Creating and testing incident response plans on a regular basis will guarantee a timely and efficient reaction to any possible data breaches or cyber espionage situations.

International cooperation: exchanging threat intelligence and coordinating countermeasures to cyber espionage operations with law enforcement, government agencies, and international organizations (Alghusin & Al-Ajlouni, 2020).

Conclusion

Due to the digital transformation process, Jordanian firms now face a complicated and dynamic array of cyber threats. Organizations confront a variety of hazards, ranging from sophisticated cyber espionage operations to insider threats and social engineering assaults. As such, a holistic strategy to cybersecurity is necessary. Insider threats, social media threats, distributed denial-of-service (DDoS) assaults, botnet attacks, online and mobile banking fraud, PBX/VoIP fraud, mobile money fraud, and cyber espionage are just a few of the common cyber risks that Jordanian organizations have to deal with, as this study has brought to light. In order to properly manage resources and prioritize cybersecurity activities, companies must have a thorough understanding of the nature and possible impact of these threats.

The research has also looked at a number of cybersecurity remedies that Jordanian companies might implement to reduce cyber risks and improve their overall cyber resilience. Technical controls, organizational regulations, staff understanding and training, and cooperation with outside parties like law enforcement and Internet service providers (ISPs) are all included in these countermeasures. The successful adoption and long-term efficacy of these countermeasures depend on companies cultivating a strong cybersecurity culture where staff members comprehend and embrace security best practices. Furthermore, international cooperation and public-private sector coordination are critical for thwarting cyber threats that cut across state borders.

Jordanian organizations may enhance the security of their digital assets, operations, and stakeholders in the digital age by implementing the advice and conclusions presented in this study. This will help to create a resilient and secure corporate environment. Organizations must adopt cybersecurity best practices, manage risks proactively, and maintain constant watchfulness in order to prosper in the face of changing cyber threats.

References

Ahmad, A., Webb, J., Desouza, K. C., & Boorman, J. (2019). Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack. *Computers & Security*, *86*, 402-418.

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future internet*, *11*(3), 73.

Alghusin, N., & Al-Ajlouni, M. I. (2020). Transformational leadership as an antecedent for organisational commitment and job performance in the banking sector of Jordan. *International Journal of Productivity and Quality Management*, *30*(2), 186-213.

Al-ma'aitah, M. A. (2022). Investigating the drivers of cybersecurity enhancement in public organizations: The case of Jordan. *The Electronic Journal of Information Systems in Developing Countries*, *88*(5), e12223.

Al-ma'aitah, M. A. (2022). Investigating the drivers of cybersecurity enhancement in public organizations: The case of Jordan. *The Electronic Journal of Information Systems in Developing Countries*, *88*(5), e12223.

AlSobeh, A. M. R., AlAzzam, I., Shatnawi, A. M. J., & Khasawneh, I. (2023). Cybersecurity awareness factors among adolescents in Jordan: Mediation effect of cyber scale and personal factors. *Online Journal of Communication and Media Technologies*, *13*(2), e202312.

Altulaihan, E., Almaiah, M. A., & Aljughaiman, A. (2022). Cybersecurity threats, countermeasures and mitigation techniques on the IoT: Future research directions. *Electronics*, *11*(20), 3330.

Amer, T. B., & Al-Omar, M. I. A. (2023). The Impact of Cyber Security on Preventing and Mitigating Electronic Crimes in the Jordanian Banking Sector. *International Journal of Advanced Computer Science and Applications*, *14*(8).

Amer, T. B., & Al-Omar, M. I. A. (2023). The Impact of Cyber Security on Preventing and Mitigating Electronic Crimes in the Jordanian Banking Sector. *International Journal of Advanced Computer Science and Applications*, *14*(8).

Aswathy, S. U., Tyagi, A. K., & Kumari, S. (2021). The Future of Edge Computing with Blockchain Technology: Possibility of Threats, Opportunities, and Challenges. *Recent Trends in Blockchain for Information Systems Security and Privacy*, 261-292.

Cappelli, D. M., Moore, A. P., & Trzeciak, R. F. (2012). *The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes (Theft, Sabotage, Fraud)*. Addison-Wesley.

Darwazeh, N. S., Al-Qassas, R. S., & AlDosari, F. (2015). A secure cloud computing model based on data classification. *Procedia Computer Science*, *52*, 1153-1158.

Diwan, T. D. (2021). An investigation and analysis of cyber security information systems: latest trends and future suggestion. *Information Technology in Industry*, *9*(2), 477-492.

Erbschloe, M. (2004). *Trojans, worms, and spyware: a computer security professional's guide to malicious code*. Elsevier.

Ikitemur, G. (2014). *Enhancing cyber security in Turkey through effective public and private cooperation*. The University of Texas at Dallas.

Imam, M., Wajid, M. A., Bhushan, B., Hameed, A. A., & Jamil, A. (2023, September). Cyber Threat Analysis and Mitigation in Emerging Information Technology (IT) Trends. In *International Conference on Emerging Trends and Applications in Artificial Intelligence* (pp. 570-588). Cham: Springer Nature Switzerland.

Jimmy, F. N. U. (2024). Cyber security Vulnerabilities and Remediation Through Cloud Security Tools. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 129-171.

Jørgensen, N. (2022). Contentious expertise: Hacking mobile phones, changing mobile technology. *First Monday*, *27*(3).

Kala, E. M. (2023). The impact of cyber security on business: how to protect your business. *Open Journal of Safety Science and Technology*, *13*(2), 51-65.

Kanaan, A., AL-Hawamleh, A., Aloun, M., Alorfi, A., & Abdalwahab Alrawashdeh, M. (2024). Fortifying Organizational Cyber Resilience: An Integrated Framework for Business Continuity and Growth amidst Escalating Threat Landscapes. *International Journal of Computing and Digital Systems*, *16*(1), 1-13.

Lacuška, M., & Peráček, T. (2021). Trends in global telecommunication fraud and its impact on business. *Developments in Information & Knowledge Management for Business Applications: Volume 1*, 459-485.

Mohebbi, S., Zhang, Q., Wells, E. C., Zhao, T., Nguyen, H., Li, M., ... & Ou, X. (2020). Cyber-physical-social interdependencies and organizational resilience: A review of water, transportation, and cyber infrastructure systems and processes. *Sustainable Cities and Society*, *62*, 102327.

Mokhor, V., Honchar, S., & Onyskova, A. (2020, October). Cybersecurity Risk Assessment of Information Systems of Critical Infrastructure Objects. In *2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T)* (pp. 19-22). IEEE.

Naaman, D. W., Rasheed, B. H., Ahmed, B. T., Salih, A. Y., & Mustafa, S. H. (2022). Design a Real-time Communication System using 3CX Software-based Private Branch Exchange Phone System on Raspberry Pi Device. *Asian Journal of Research in Computer Science*, *13*(4), 34-45.

Naseer, I. (2020). Cyber Defense for Data Protection and Enhancing Cyber Security Networks for Military and Government Organizations. *MZ Computing Journal*, *1*(1).

Obaidat, M. A., Obeidat, S., Holst, J., Al Hayajneh, A., & Brown, J. (2020). A comprehensive and systematic survey on the internet of things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures. *Computers*, *9*(2), 44.

Obeidat, Z. M., Xiao, S. H., al Qasem, Z., & Obeidat, A. (2018). Social media revenge: A typology of online consumer revenge. *Journal of Retailing and Consumer Services*, *45*, 239-255.

Okpa, J. T., Ajah, B. O., Nzeakor, O. F., Eshiotse, E., & Abang, T. A. (2023). Business e-mail compromise scam, cyber victimization, and economic sustainability of corporate organizations in Nigeria. *Security Journal*, *36*(2), 350-372.

Owen, H., Zarrin, J., & Pour, S. M. (2022). A survey on botnets, issues, threats, methods, detection and prevention. *Journal of Cybersecurity and Privacy*, *2*(1), 74-88.

Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K. K. R., & Burnap, P. (2020). Impact and key challenges of insider threats on organizations and critical businesses. *Electronics*, *9*(9), 1460.

Schoenherr, J. R., Lilja-Lolax, K., & Gioe, D. (2022). Multiple Approach Paths to Insider Threat (MAP-IT): Intentional, Ambivalent and Unintentional Insider Threats. *Counter-Insider Threat Research and Practice*, *1*(1).

Sindiren, E., & Ciylan, B. (2018). Privileged account management approach for preventing insider attacks. *International Journal of Computer Science and Network Security*, *18*(1), 33-42.

Verma, A., & Shri, C. (2022). Cyber security: A review of cyber crimes, security challenges and measures to control. *Vision*, 09722629221074760.