International Journal of Management and Marketing Intelligence	*International Journal of Management and Marketing Intelligence, 1(4), 1-7.*	
	Volume: 1	http://ijmmi.com
	Issue: 4	ISSN:
	Received: September 11, 2024.	Accepted: December 8, 2024.
	Citation: Vasudevan, A. (2024). Cyber Security: A Customer Perspective on Emerging Technologies, International Journal of Management and Marketing Intelligence, 1(4), 1-7.	

Cyber Security: A Customer Perspective on Emerging Technologies

Asokan Vasudevan

Faculty of Business and Communications, INTI International University, 71800 Negeri Sembilan, Malaysia.

ARTICLE DETAILS

Article History
Published Online: December 2024

Keywords
Cyber Security
Emerging Technologies
Customer Perspective

JEL Codes:
D18, Q55, K22 & O33

Corresponding Author
Email: vasudevan@newinti.edu.my

ABSTRACT

Cybersecurity is important since it prevents both theft and damage to several types of information. This comprises delicate information, personally identifiable details, Personal Health Information (PHI), personal data, information related to property rights, and data management used by the government and industry. In the recent years, the cybersecurity has become significant trouble in business sectors worldwide that depend on digitization and faster transactions. Many devices are internet-connected, requiring security precautions to secure them from cyber-attacks. Moreover, the individuals who engage in digital transactions divulge a huge amount of financial and private knowledge that cybercriminals require. While offering or purchasing a product or service, both vendors and consumers must consider data privacy concerns. Many laws and rules, like the General Data Protection Regulation (GDPR) of the European Union, intend to regulate how businesses handle client information. Cybersecurity Perspectives is a worldwide platform combining industry standards and direct knowledge with cutting-edge research and advancement to boost Industrial Internet of Things (IoT) cybersecurity effectively. This research paper provides a cybersecurity framework for the customer perspective, which may ensure authorized and secure transactions to customers in business sectors.

1. INTRODUCTION

Cyber security has recently gained attention in the different areas like media, businesses, blogs, and social networks (Al Kurdi et al., 2024; Tariq et al., 2024). As a result, the internet is viewed as a wild cyberspace, a venue for commerce, consumption, business, and entertainment. However, the problem has grown more frequent in digital-related activities such as communications and banking (Alshurideh et al., 2024; Nuseir et al., 2024a). Despite determined rewards accompanying Information and Communication Technology (ICT), the concept of cyber security threat plays an important role in adopting and retaining the technology. Therefore, the growing knowledge of the idea (cyber threat) is regarded as a driver that could possibly moderate customers' awareness of the receipt and retaining of novel technology (Nuseir et al., 2023; Abuanzeh & Alshurideh, 2022). So the fundamental idea (cyber-threat) in the study issue emphasizes the consequences (bad effect) of ICT use, it also applies to the platform choice of the consumer. The financial sector, where the present study is relied, is noted to be characterized by the vulnerable institution (beneficiary) of this menace, particularly on internet banking schemes, due to the damaging influence on privacy, integrity, in addition to privacy of a bank and its customers (Abualoush et al., 2018).

The world is facing some reservations regarding new cyber-attacks with the integration of the emerging technologies. Cyber-attacks are deliberated as a threat to individuals, businesses, and governments (Alzoubi et al., 2024; Nuseir et al., 2024b). These attacks operate users in acquiring access to their information. Many cyber security challenges are connected to system applications, operational and communication systems, or magnetic devices. Cyber-attacks are offensive acts committed with a computer or linked networks or systems with the intent of disrupting and/or eliminating an adversary's vital cyber systems, resources, or operations. The intended consequences of a cyber-attack are not always restricted to the targeted computers systems or data; for example, computer-system attacks are meant to impair or destroy infrastructure capabilities. Cyberattacks may employ intermediary delivery systems such as peripherals, electronic transmitters, implanted malware, or human operators. The activation or impact of a cyber-attack may be both spatially and temporally separated from the delivery (Bapat et al., 2018).

The measurement of how cyber security attacks affect small firms is a vital problem that still requires more study. Only a few studies have studied the influence of cyber security protocols on the degree of loss or damage caused to small enterprises by cyber security attacks, despite the fact that that many research efforts have focused on cybersecurity awareness and education in small businesses (Abeshu and Chilamkurti, 2018). A cybersecurity system typically contains of two frameworks: Network Security (NS) as well as computer security (CS). CAs are managed using different technologies such as firewalls and encrypting. An IDS is more likely to avert remote attacks on CN. As a result, the IDS's primary goal is to classify or prevent various forms of harmful infrastructure projects. Traditional technologies, such as firewalls, are inadequate of carrying out the task efficiently. An Intrusion Detection System (IDS) monitors and evaluates network operations. It recognizes damaging cyber behaviors while detecting security risks or attacks (Ashik et al., 2020; Yuri et al., 2013).

Vulnerabilities can be mitigated by the use of various security measures, such as information security, physical security devices, software products, and software patching (Hasan et al., 2022). Since many industrial system control advances do not correspond to the security standards of a given instruction, cyber-attacks on their integrity, reliability, and secrecy can be carried out. A cyber threat to accessibility, for example, involves eliminating efficiency tools and leaving considerable control and advanced data unavailable at all moments (Amponsah, 2024; Zahra, 2024). Manipulating specific information on assets is a danger to authenticity, while monitoring more into essential data is a risk to confidentiality (Ud din Siddiqi & Ali, 2022; Von Solms and Van Niekerk, 2013).

Another problem with intrusion detection is a shortage of trained personnel competent of monitoring and reacting to intrusions by evaluating massive amounts of information in groups. In cyber security, ML techniques have been used efficiently to create efficient solutions. Since machine learning has a number of potential for detecting many types of cyber-attacks, malware protection, malware categorization and recognition, privacy preservation, and advanced threat, it is rapidly becoming a vital tool for attackers. As adversary techniques improve, major challenges become more complicated and complex. For example, most current security solutions may access to immediate threat disparities. As a result, self-learning solutions should be capable to address such concerns. In this context, machine learning techniques have arose as a vital tool for the whole security business (Gong and Navimipour, 2022).

Many cybersecurity research studies have been done to identify and avoid cyber-attacks or intrusions. Signature-based network attack detection is a well-known technique in the cyber sector. This technique, essentially takes use of a well-known signature, has lately achieved great recognition and personal wealth. For detecting covert or "zero-day attacks," however, the "anomaly-based method" has an benefit above the "signature-based method". This technique analyzes crucial security data to track NT and spot behavioural attack patterns. Many machine learning and data mining analyze this information these security event trends and provide useful conclusions. The major downside of the anomaly-based technique is that it may generate a lot of false reports since it might label previously unknown system behaviours as anomalies. Therefore, reducing an IDS's false favorable terms must be a top priority (Huda et al., 2018).

2. LITERATURE REVIEW

Many excellent works have already been done in cybersecurity utilizing different methods and customer perspectives, but these works have focused mainly on factors like e-banking and business. The authors explained the field of ICT, the concept of security has further been decomposed into three dimensions, known as CIA (confidentiality of information, the integrity of information, and availability of information). By extension, information confidentiality deals with securing a confidential identity without access to unauthorized parties. In the middle of the instability of innovation, it is worth noting that data is a valuable asset to any organization's development and growth, especially in banking industry, on which the research was based. Bank account records, private details, credit card numbers, corporate secrets, and government documents, for example, must be kept secret since preserving such vital information is a purpose of information security (Chen et al., 2021; Ozturk, 2024; Sukkari, 2024).

Integrity, however, refers to protecting information from being adapted or manipulated by an unsanctioned party. Consequently, information has value only when it is precise. So having this in mind, the possible users fo the innovative technology are sceptic about its utilization, which consequently disturbs the overall receiving and acceptance rate as probable in the business atmosphere. The availability of information also refers to ensuring that authorized parties can access the information when needed. For better understanding, data has value if the right people can assess it at the right times. So repudiating access to info by respective users has recently become an issue of importance to scholars and practitioners in the internet space (like e-banking) or social media (Lo and Campos, 2018; Setyowati et al., 2021; Al Kurdi, 2024; Alshurideh, 2024).

Due to the widespread production of software or hardware, it is essential to provide assurances in the supply chain process. The cyber domain varies qualitatively due of its scale. A bomb's range is extremely limited in extreme circumstances, but cyber-threats have a wide range of impacts, therefore the methods control real-world activities. Like many other area of knowledge, cyberspace operations are controlled by a small number of people. The software and hardware that users use can’t be modified or controlled by them. It is well recognized that only selected people have the ability to successfully control or direct cyberattacks (Lu and Cecil, 2015).

This term distorts the user's purpose of utilizing such technology towards its maximum potential. However, research on the subject have shown that identity theft may happen in any sector, including general industry, academic facilities, government and military groups, the health insurance industry, and banking, credit, and financial services. Similarly, identity fraud may ruin personal credit and might lead to very costly legal action that might take many years, if not decades, to properly correct or recover what has been lost. With this in mind, it is logically obvious that sceptics of e-banking would be hesitant to trade in or participate in a successful online trade due to the alleged identity theft connected with e-banking. At the same time, the users' trust, integrity, and privacy concerns about technology are at risk (Ghimire et al., 2020).

Technology experts believe that digital transformation is an inevitable necessity, and whoever lags behind will be out of the scene. Today, digital transformation is no longer a trend or an option of luxury, but it has become the most effective path that all countries of the world should take to ensure their survival and competition (Lezzi et al., 2018). It is axiomatic that particular organizations follow that path as others. It is also natural for to ask what is organization doing to keep pace with this digital world of rapid developments. The rapid increase in the digitization of the economy and social activity has led to an unprecedented expansion of data collection, use and transmission. Accordingly, the discussions of the ways can be used to improve cross-border data flows and overcome obstacles. The literture discussed the issue of cybersecurity with the aim of improving the resilience of global economic systems and dealing with the growing global challenges, given the size of the economic losses incurred from cyber-attacks (Culot et al., 2019).

Confronting cybersecurity threats to emerging challenges and opportunities of the technologies trigger the international conferences to be launched under several titles. The experts in this events stated the developed networks face many security challenges, and the network equipment security systems, which was developed according to vendor product security standards and life-cycle processes, provides a solid foundation for enabling network equipment to meet security requirements (Tawalbeh et al., 2020). The computer emergency response team of the organization organized the sidelines in recognition of the efforts in the field of cybersecurity. The experts also considerd the important testimony from the international teams of contributions to security innovations, as the company places cybersecurity at the top of its priorities (Nobles, 2018).

3. Proposed framework for cyber security

In the recent years, cybersecurity has emerged as a key disruptive technology all across the world. Cybersecurity is important for both customers and providers in a corporate world that relies on digitization and rapid transactions. Even if a vulnerability does not directly affect the device, these customers must consider cyber resilience while buying for services or products. Figure (1) emphasises the distinction, as well as the relationship between information security vs cybersecurity.

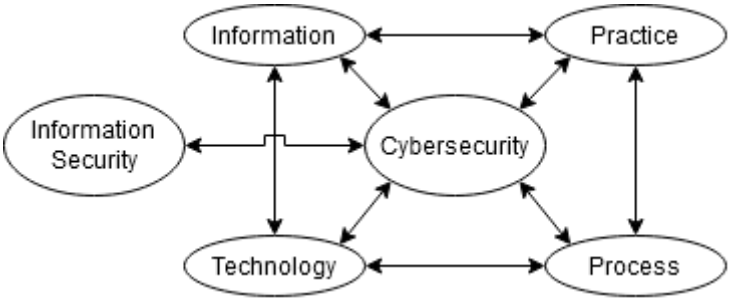

Figure (1): Cyber security framework

Figure 1 shows how cybersecurity involves many elements to secure a company. In contrast to information security, cybersecurity goes beyond internal control to include cyberspace protection as well. Although they are complimentary and equally vital, cyber and information security have a wide range of uses. Information Systems Security, Information Security, Data Security, and Cybersecurity all share the Confidentiality, Integrity, and Availability (CIA) triad's core principles and, taken as a whole, are reliant on the same factors, such as technology and information assets. Cybersecurity is a larger concept that includes safeguarding not only information assets and also related technologies, assets, processes, people, organisations, and procedures. Recent evidence indicates that the variety of assets protected by cybersecurity is continuing to grow.

4. PROBLEM STATEMENT AND RESEARCH CONTRIBUTION

Currently cybersecurity faces many problems in terms of data security. This study highlights different aspects of cyber security in terms of customer perspective on emerging technologis and provide efficient results to customer perspective in terms of business protection against cyberattacks and data breaches, data protection and networks, preclusion of unauthorized user access and better recovery time after a breach. There are many distinct types of

cyber security concerns, including ransomware, phishing, malware attacks, and much more. This research highlights critical analysis on cyber security in terms of customer perspective on emerging technologies and provides better results in terms of customers data security, data integration and authentication process.

The significance of this topic is associated with the potential danger and threats of cybersecurity that are increasing day by day with the rapid technological development, which calls for precaution and preparation to confront such threats that may have catastrophic effects on the economy, security and society if they occur, and this is what the government is fully aware about (Gunduz & Das, 2020). Especially with the presence of the cybersecurity reports documented about hundreds cases of cyberattacks. The reports also affirmed that information warfare is a feature of this era, in light of the development of communication technologies and digital communication tools, and the more information systems develop around the world, the more countries, organizations, institutions and people are active to penetrate those systems, pointing out the countries are exposed to increasing cyber-attacks, which vary in numbers and targets, indicating that these attacks focus on sovereign institutions, on financial and economic goals, and on individuals as well (Ghelani, 2022).

5. CRITICAL ANALYSIS

Reviewing the literature about the customers' perspectives, following analysis have been done.

5.1 ENFORCE PASSWORD RULES

One of the first line defense against intrusions is a strong password, and sometimes changing it can help to keep hackers away. But even when prompted, the majority of staff won't voluntarily change their passwords. Make it a requirement to update passwords often, and instruct users on how to develop and remember password protection (Li and Li, 2020).

5.2 UPDATE REGULARLY

Any internet access is susceptible, and hackers attempt to capitalize on its main characteristic. Maintain all relationships, software platforms, and applications with improvements and fixes. Updates to software and system safety are being implemented (Filipow et al., 2022).

5.3 IMPLEMENT VPNS FOR ALL CONNECTIONS

Networks that just use standard security protocols are more prone to penetration. Implement Virtual Private Networks (VPN) links between corporate locations, and make it explicit that mobile workers who join via public Wi-Fi networks must use them.

5.4 RETIRE ALL UNUSED SERVICES

Once limited-time goods expire, disassemble the related apps, logins, or user credentials. When you don't utilize every possible element of a UC installation, such as a video conferencing capability, switch off the feature to further prevent unwanted access to the enterprise.

5.5 LEVERAGE EXISTING SECURITY OPTIONS

Some programs provide security measures by default. While further precautions are always necessary, companies understand their respective products and commit substantial work to provide a safe client environment. Find out just what security features are available with your program and make full use of them in conjunction with any security measures you have in place. Limits potential vulnerability exposure as soon as possible (Zhu et al., 2019).

6. DISCUSSION

This study highlights the fact that, rather than focusing on individual hardware, software, and network layer flaws, the traditional approach has adopted packaged security protection techniques that shield everything within from perceived attacks. The vast majority of businesses use a defined security model to protect their network from any possible outside access. This research focuses on several ideas that include strengthening and building walls around essential internal IT resources, such as servers and operation data.

Due to the fact that the emerging economies and technologies are moving towards digital transformation in many sectors, and they seek to be among the ranks of the world in the digital economy by investing in technical sectors. The authority takes upon itself to protect the interests of users of communications, information technology and postal services, and because sustainability is the responsibility of everyone and part of the culture of the authority. The authority continuously seeks to achieve a positive impact on society and preserve the sustainability of the environment and to ensure the safety of users by launching initiatives that are in line with international best practices in cybersecurity. The interconnected network of information technology infrastructure, which includes the Internet, communication networks, computer systems and devices connected to the Internet, as well as processors and associated control devices.

A cutomer perspective, the authorities should issued regulatory frameworks for cybersecurity for service providers in the telecommunications, information technology and postal sectors, which contains a comprehensive set of cybersecurity requirements and controls. The targets providers of telecommunications, information technology and postal services, as the regulatory framework provides requirements for improving cybersecurity risk management through an approach consistent with global best practices and local cybersecurity frameworks. To contribute to regulating and enabling cybersecurity practices of telecommunications, information technology and postal service providers; this reflect in raising the level of confidence in the integrity of the service providers'

infrastructure, in addition to supporting the regulatory framework to adopt a risk management method to achieve cybersecurity requirements. And encourage the service providers to apply best practices to develop appropriate cybersecurity measures, and raising the level of service providers in resisting and responding to cyberattacks. In addition to ensure the confidentiality, integrity, and availability of the services provided to customers.

7. CONCLUSION

In this research, cyberspace has been extended and given powers further than the hyper-connectivity of the Internet itself thanks to the exceptional capabilities of these developing technologies. But these discoveries haven't only been incredibly helpful. The expanding network infrastructure and linked devices even those that don't first appear to be connected increase intrusion vulnerabilities. Additionally, the vast quantities of Internet-connected nodes' processing and data sharing make them more potential targets for exploitation and deception. The geopolitical conflict will be molded for years to come by state and non-state actors that want to create sophisticated methods of control and monitoring, particularly by using developing technology. It becomes more difficult for democratic nations to approach aimed and adapt to external threats when the information ecosystem becomes more contaminated, segregated, and strictly regulated. As a result, it is crucial to the alliance's effective operation in stability, crisis, and conflict to coordinate, synchronize, and carry out information and cyberspace activities that will intentionally generate counter effects that are like the original effects.

8. LIMITATIONS AND FUTURE DIRECTION

Today, cybersecurity offers many benefits over emerging technologies, including business protection against cyberattacks and data leaks, protection for data and networks, preventative measures of unauthorised access, accelerated breach recovery, protection for end users and endpoint devices, and regulatory compliance. However, it also has several drawbacks, such as vulnerabilities in software, ransomware attacks, IoT attacks, cloud attacks, phishing attacks, attacks on the blockchain and cryptocurrencies, and machine learning and AI risks. This study provided effective and safe data for the corporate sector and suggested a methodology for cyber security. Cybersecurity will be crucial in the future since it guards against theft and destruction to all types of data. This covers delicate information, personally identifiable information (PII), protected health information (PHI), personal data, data pertaining to property rights, and information systems used by the government and business.

References

Abeshu, A., & Chilamkurti, N. (2018). Deep learning: The frontier for distributed attack detection in fog-to-things computing. IEEE Communications Magazine, 56(2), 169-175.

Abualoush, S., Masa'deh, R., Bataineh, K., & Alrowwad, A., (2018). The role of knowledge management process and intellectual capital as intermediary variables between knowledge management infrastructure and organization performance. Interdisciplinary Journal of Information, Knowledge, and Management, 13, 279-309.

Abuanzeh, A. A., & Alshurideh, M. (2022, November). Cyberspace and Criminal Protection of Privacy in the Jordanian Legislation Under the Corona Pandemic: A Comparative Study. In International Conference on Advanced Intelligent Systems and Informatics (pp. 540-557). Cham: Springer International Publishing.

Al Kurdi, B. (2024). Social media addiction: Youths' perspectives. International Journal of Management and Marketing Intelligence, 1(1), 1-10.

Al Kurdi, B., Alquqa, E. K., Nuseir, M. T., Alzoubi, H. M., Alshurideh, M. T., & AlHamad, A. (2024). Impact of Cyber Security and Risk Management on Green Operations: Empirical Evidence from Security Companies in the UAE. In Cyber Security Impact on Digitalization and Business Intelligence: Big Cyber Security for Information Management: Opportunities and Challenges (pp. 151-167). Cham: Springer International Publishing.

Alshurideh, M. (2024). Utilize internet of things (IOTs) on customer relationship marketing (crm): An empirical study. International Journal of Management and Marketing Intelligence, 1(1), 11-19.

Alshurideh, M., Alquqa, E., Alzoubi, H., Kurdi, B., & Alhamad, A. (2023). The impact of cyber resilience and robustness on supply chain performance: Evidence from the UAE chemical industry. Uncertain Supply Chain Management, 11(1), 187-194.

Alzoubi, H. M., Alshurideh, M. T., & Ghazal, T. M. (Eds.). (2024). Cyber Security Impact on Digitalization and Business Intelligence: Big Cyber Security for Information Management: Opportunities and Challenges.

Amponsah, C. (2024). The Effects of Pros and Cons of Applying Big Data Analytics to Enhance Consumers' Responses. International Journal of Management and Marketing Intelligence, 1(3), 1-8.

Ashik, M. H., Maswood, M. M. S., & Alharbi, A. G. (2020, June). Designing a fog-cloud architecture using blockchain and analyzing security improvements. In 2020 international conference on electrical, communication, and computer engineering (ICECCE) (pp. 1-6). IEEE.

Bapat, R., Mandya, A., Liu, X., Abraham, B., Brown, D. E., Kang, H., & Veeraraghavan, M. (2018, April). Identifying malicious botnet traffic using logistic regression. In 2018 systems and information engineering design symposium (SIEDS) (pp. 266-271). IEEE.

Chen, J., Ramanathan, L., & Alazab, M. (2021). Holistic big data integrated artificial intelligent modeling to improve privacy and security in data management of smart cities. Microprocessors and Microsystems, 81, 1-10.

Culot, G., Fattori, F., Podrecca, M., & Sartor, M. (2019). Addressing industry 4.0 cybersecurity challenges. IEEE Engineering Management Review, 47(3), 79-86.

Filipow, N., Main, E., Sebire, N. J., Booth, J., Taylor, A. M., Davies, G., & Stanojevic, S. (2022). Implementation of prognostic machine learning algorithms in paediatric chronic respiratory conditions: a scoping review. BMJ Open Respiratory Research, 9(1), 1-11.

Ghelani, D. (2022). Cyber security, cyber threats, implications and future perspectives: A Review. American Journal of Science, Engineering and Technology, 3(6), 12-19.

Ghimire, A., Thapa, S., Jha, A. K., Adhikari, S., & Kumar, A. (2020, October). Accelerating business growth with big data and artificial intelligence. In 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) (pp. 441-448). IEEE.

Gong, J., & Navimipour, N. J. (2022). An in-depth and systematic literature review on the blockchain-based approaches for cloud computing. Cluster Computing, 25(1), 383-400.

Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. Computer networks, 169, 1-14.

Hasan, M. K., Ghazal, T. M., Saeed, R. A., Pandey, B., Gohel, H., Eshmawi, A. A., ... & Alkhassawneh, H. M. (2022). A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet‐of‐Medical‐Things. IET communications, 16(5), 421-432.

Huda, S., Yearwood, J., Hassan, M. M., & Almogren, A. (2018). Securing the operations in SCADA-IoT platform based industrial control system using ensemble of deep belief networks. Applied soft computing, 71, 66-77.

Lezzi, M., Lazoi, M., & Corallo, A. (2018). Cybersecurity for Industry 4.0 in the current literature: A reference framework. Computers in Industry, 103, 97-110.

Li, D., & Li, Q. (2020). Adversarial deep ensemble: Evasion attacks and defenses for malware detection. IEEE Transactions on Information Forensics and Security, 15, 3886-3900.

Lo, F. Y., & Campos, N. (2018). Blending Internet-of-Things (IoT) solutions into relationship marketing strategies. Technological Forecasting and Social Change, 137, 10-18.

Lu, Y., & Cecil, J. (2015). An internet of things (IoT) based cyber physical framework for advanced manufacturing. In On the Move to Meaningful Internet Systems: OTM 2015 Workshops: Confederated International Workshops: OTM Academy, OTM Industry Case Studies Program, EI2N, FBM, INBAST, ISDE, META4eS, and MSC 2015, Rhodes, Greece, October 26-30, 2015. Proceedings (pp. 66-74). Springer International Publishing.

Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. HOLISTICA–Journal of Business and Public Administration, 9(3), 71-88.

Nuseir, M. T., Alquqa, E. K., Al Shraah, A., Alshurideh, M. T., Al Kurdi, B., & Alzoubi, H. M. (2024a). Impact of Cyber Security Strategy and Integrated Strategy on E-Logistics Performance: An Empirical Evidence from the UAE Petroleum Industry. In Cyber Security Impact on Digitalization and Business Intelligence: Big Cyber Security for Information Management: Opportunities and Challenges (pp. 89-108). Cham: Springer International Publishing.

Nuseir, M. T., Alquqa, E. K., Alzoubi, H. M., Alshurideh, M. T., Al Kurdi, B., & AlHamad, A. (2024b). The Effect of Cyber Resilience Role in the Relationship of Intelligent Information System on the E-Supply Chain: An Empirical Evidence from the UAE Healthcare Industry. In Cyber Security Impact on Digitalization and Business Intelligence: Big Cyber Security for Information Management: Opportunities and Challenges (pp. 69-87). Cham: Springer International Publishing.

Nuseir, M. T., Refae, G. A. E., Alshurideh, M., Urabi, S., & Kurdi, B. A. (2023). The Influence of Sharing Fake News, Self-Regulation, Cyber Bullying on Social Media Fatigue During COVID-19 Work Technology Conflict as Mediator Role. In The Effect of Information Technology on Business and Marketing Intelligence Systems (pp. 131-145). Cham: Springer International Publishing.

Ozturk, I. (2024). Factors Influencing the Use of the Internet of Things (IoT) to Enhance Customer Relations and Customer Experience. International Journal of Management and Marketing Intelligence, 1(2), 1-9.

Setyowati, W., Widayanti, R., & Supriyanti, D. (2021). Implementation of e-business information system in indonesia: Prospects and challenges. International Journal of Cyber and IT Service Management, 1(2), 180-188.

Sukkari, L. (2024). The impact of big data analytics on customers' online buying. International Journal of Management and Marketing Intelligence, 1(2), 10-19.

Tariq, E., Akour, I., Al-Shanableh, N., Alquqa, E., Alzboun, N., Al-Hawary, S., & Alshurideh, M. (2024). How cybersecurity influences fraud prevention: An empirical study on Jordanian commercial banks. International Journal of Data and Network Science, 8(1), 69-76.

Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. Applied Sciences, 10(12), 1-17.

Ud din Siddiqi, A., & Ali, Z. (2022). The Sybil Attack Prevention Algorithm: Makes Blockchain Network More Secure. International Journal of Advanced Sciences and Computing, 1(1), 18-26.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97-102.

Yuri, D., Canh, N., & Peter, M. (2013). Architecture framework and components for the big data ecosystem. J. Syst. Netw. Eng, 1-31.

Zahra, A. (2024). Using Intelligent Information Systems to Enhance Customers' Knowledge. International Journal of Management and Marketing Intelligence, 1(3), 9-16.

Zhu, L., Wu, Y., Gai, K., & Choo, K. K. R. (2019). Controllable and trustworthy blockchain-based cloud data management. Future Generation Computer Systems, 91, 527-535.