Journal Homepage: - www.journalijar.com
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)
Article DOI: 10.21474/ IJAR01/ 21307
DOI URL: http://dx.doi.org/10.21474/ IJAR01/ 21307
ISSN NO. 2320-5407

RESEARCH ARTICLE

The National Conference on Innovative Trends in Modern Business Environment (ITMBE 2025) , DPG Institute of Technology and Management (DPGITM) Guru gram

IMPACT OF CYBERSECURITY ON SUPPLY CHAIN: BANKING SECTOR CASE STUDY

Dr Bharti Bisht[1], Himanshu Gaur[2] and Dr. Sonika[2]
1. Assistant Professor, Department of Computer Science, DPGITM, Guru gram
2.Assistant Professor, Department of Management Studies, DPGITM, Guru gram

Manuscript Info

Keyword: -
Cyberspace, Supply Chain, Risk mitigation, Cyber security practices, Security level, Quality.

Abstract

With the world's economy taking on a digital character, it is important now more than ever to integrate cyber-security in supply chain operations, especially in banking, where aspects of the data, such as confidentiality, integrity and availability are very critical. The study examined the effect of cyber-security actions on the banking industry's supply chain in its ability to recover, sustain and manage risk. This work used a questionnaire that targeted managers and clients and involved 30 managers and 260 digital banking clients. Out of the data collected, 200 were legitimate for analysis using PLS-SEM V4 and IBM SPSS V26. In our survey, we also discarded 30 responses as they did not provide valid responses to the survey including having a standard deviation of zero and identified as outliers using Cook's distance. The research explored current approaches in risk mitigation through a variety of mechanisms such as zero-trust architecture,incident response frameworks, and vendor risk assessments. The results showed that well-established, knowledgeable managers were aware of and taking cyber-security actions. This makes it clear that stakeholders need to regularly evaluate cyber security practice training and talks.However , clients providing banks a passing mark to collaboratively educate clients regarding cyber-security risks better given they were satisfied with the level of security in their accounts.

Introduction:-

In this digital age, cyber security is important for every industry because we are becoming more and more dependent on technology, which makes us more vulnerable to online threats and attacks. Cyber attacks on physical, technical, and administrative security have gotten smarter and more relentless.

systems. Cyber attacks come in many forms, such as phishing schemes, viruses, worms, Trojan horses, ransom ware, and denial-of-service attacks. These attacks can be very bad, causing people to lose money, have their reputations hurt, and have private information stolen [1]. The International Telecommunication Union (ITU) provides the following definition of cyber security: it

refers to all the tools, policies and practices that protect the business, users, and the cyber environment (ITU, 2023). At the same time, the ITU also has a mandate to protect the safety and security of the digital landscape.

Cyber security practices protect sensitive data and systems, ensure businesses stay out of trouble with the law, and ultimately maintain the trust of customers and employees. The practice of cyber security has been adopted by many businesses with a focus on fortifying security to protect the business but also to build customer's trust.

Cyber security practices are new and futuristic, and recent studies show how important they are in the fields of data science, network science, and business research. Cyber security steps are important because they can improve security and deal with cyber threats. Cyber security can give businesses a competitive edge, but there are also risks that can make the supply chain less flexible and make customers unhappy with the quality of a product or service. These techniques are being used by or moving toward being used by top companies around the world. Because they risk a lot of money, any problems with hacking can be very bad for manufacturing companies. The manufacturing sector is very important, but so are cyber security policies in the digital service sector.

The banking sector experiences fresh opportunities and challenges that come with additional risks due to digital banking. The literature shows that money-related dealings by way of digital banking could experience cyber security breaches that can carry financial loss, reputational damage to a bank, and litigation. The impact from these breaches can be worse in the banking industry [2]. For example, [3] put forth that digital banking expands the attack surface related to new ransom ware and phishing attacks emanating from the lack of weak authentication protocols, insider threats, and encryption disadvantages. To illustrate, the Capital One data breach of 2019 compromised the personal data of approximately 6 million citizen accounts were vulnerable due to firewalls misconfiguration that allowed unauthorized access of its cloud-based servers [4]. Despite these risks around cyber security breaches - not much documentation is available exploring how banks in developing economies manage these attacks or what impacts they may have on supply chain efficiencies.

The shift towards digital banking offers banks new opportunities and risks. Despite recent advances in digital banking, the implications of digital banking have not received enough attention. The banking industry has a multitude of cyber exposures, particularly in developing countries, and needs more research on the implications of cyber security practices. Research into the science of cyber security does not

have a hundred years of development, and the body of evidence is mostly theoretical work for some of the strategic perspectives of cyber security practices. For example, very rarely will there be a practical study in a banking supply chain which considers the role cyber security practices are contributing to the supply chain performance? This leads to the primary research question that we address in this study: what are the implications of cyber security practices on supply chain performance in the Jordanian banking industry? This knowledge gap can pose a serious risk exposure for banks who are interested in adopting cyber security practices and want to understand the implications that these practices have on supply chain performance. We conduct research into cyber security practices, supply chain performance in Jordanian banking industry setting, and its key characteristics, levels and interactions.

LITERATURE SURVEY

Cyber security, as the word suggests, is the protection of cyberspace, which is a system that is linked to the Internet. Technology is always changing, and this has been a big part of turning boring business jobs into very creative and effective ones. According to [5], cyber-physical systems share information by combining real parts, network systems, embedded computers, software, and sensors. For tech companies, data breaches and hacking are a big risk. This is why information security is an important part of national security in many places. Governments are putting in place broad rules to make sure cyber security, and these rules are meant to find and stop hacks. With the proper protections in place [6], your IT equipment, software, and data that you store, or access can be protected against theft and/or other harm. Yip (2015) discussed internet supply chain security for securing supply chain networks. In this case the physical infrastructure addressed putting up firewalls to prevent hackers and extract private information, as well as dealing with malware, cyber terrorism, impersistent threats and data theft. Cyber security is required for every business as a part of its business and design and strategy. In fully implementing Industry 4.0, this means safety is a large factor in creating a competitive business [7].

Cyber safety means keeping digital data and the system that supports it safe. Researchers in [8], who wrote not long ago, pointing out that while technological progress has been good for the banking business, cyber attacks are a major threat to the same group. The report offers computer safety checks, teaching about electronic safety, cyber protection checks, and making security stronger. The study [9] put out a risk-based systems method and suggestions for how financial institutions can deal with the risk of cyber attacks. The methodology focused on six sections: cyber defence threat mitigation system, technological resilience assessment, cyber security functional resilience, cyber security intelligence, and metrics, surveillance, and reports. The work [10] highlighted that digital safety is part of the answer when a crime happens. Cyber attacks, the spread of viruses and logic bombs, and denial of Cybercrime comes in many forms, such as denial of service attacks, hacking, jacking, and more. It mentioned that the world's cyber skills gap is getting worse and that 86% of information security managers asked thought there weren't enough experienced cyber

security workers. Cyber warfare is suggested to stop cybercrime, and software tools are made and used. The connection surveillance systems are a type of computer programs that look at how the system works to find strange safety violations and tell the difference between hostile and legal network users. Effectiveness of the supply chain and cyber security have been salient issues to managers as well as academia. Both dimensions have been linked in several studies [11], [12]. There are relatively few studies on each measure independently [13], [14]; however, there are substantial studies approaching all the measures transcending those two dimensions [15],[16].

According to [17], data and digital technologies can be used to improve a service chain's performance quality. Prioritizing cyber security across the service supply chain is critical if a service provider wants to provide a high level of service quality. Cyber security is about implementing security measures that include securing sensitive information and assets, protections to ensure systems and networks remain uncompromised, and ensuring authorized users can access and consume services. They continued with a point about consistently and reliably delivering service to achieve service quality. Achieving high levels of cyber security and service quality means it takes technical knowledge and expertise, process control, and effective communication and collaboration across the service supply chain. Customer satisfaction (CS) focuses on customers' perceptions, which is when expected performance can be compared to what the customer expects from the service. In study [18] researchers stated that customer satisfaction is essential for marketing success, since marketing success and customer satisfaction depend on its competitiveness. Service innovation is important because businesses use service innovation to develop services, which can be described as creating services for customers. To that end, business food service companies ought to solicit customers' opinions about their satisfaction level with the services they provide using periodic surveys. Customer satisfaction in a service supply chain can be regarded as how satisfied consumers are with a business' service offerings and that business' supply chain operations.

Ensuring confidentiality, integrity, and availability are essential components of cyber security, which in turn must adhere to certain protocols outlined below. Most research has focused on the service industry, however, there has been some study in banks and the financial industry[19]. Particularly in the wake of the global crises, numerous research has focused on the efficiency of supply chains. To improve supply chain effectiveness, we must understand what factors companies worldwide should consider. Improving the efficiency of supply chains is an important consideration for businesses worldwide [20][21]. The current global financial crisis, the conflict in Ukraine, and the conclusion of the COVID-19 pandemic make this point even more poignant.Cybersecurity risk management and assessing national cyber security in crisis

avoidance [22][23] represent two of the multitude of studies that have examined aspects affecting supply chain performance from various perspectives. The study [24] investigates cyber security trends in the banking sector and the work [25] explores cyber supply chain security and the impact on performance in lean and agile supply chains.

METHODOLOGY:-

Design

This study employs both quantitative and descriptive methods to get the information it needs and figure out how cyber security procedures affect the performance of the supply chain in banking sector. The quantitative method checks the study's hypotheses and answers its questions by looking at past research and using an analytical method on the data gathered from a questionnaire sent to bank management and customers. This study looks at how cyber security measures affect the performance of the supply chain for electronic services in banking sector by using a cross-sectional method, which is a sort of snapshot data.

Study Group and Sample

Figuring out the study's population is important for making the study's variables and goals clear. The people in this study are all the private banks, together with their managers and clients. Study is based on200 people, so two samples were selected to get results that were accurate and not biased. The study set the sample of managers apart by adding a special section for them to fill out to find out how they felt about cyber security policy. Only managers knew about this.

Table 1 shows the demographic information for clients, while Table 2 shows the demographic information for managers. Table 1 shows that most of the consumers who were questioned (60.56%) are between the ages of 25 and 35. Fifteen percent are between the ages of 36 and 45, 6.2 percent are under 25, and 6.34 percent are beyond 45. The researchers think that these results show that the sample is representative because the biggest age group uses electronic banking services. So, the data we get will provide us a true picture of reality.

TABLE I
CLIENT RESPONDENT'S PROFILE SAMPLE

Criteria	Total Count	Percentage
Criteria 1: Age Group		
<25 years	18	6.2%
25-35 years	110	60.56%
36-45 years	20	15.23%

> 45 years	15	6.34%
Criteria 2: Gender Basis		
Male	98	45.8%
Female	100	50.9%
Criteria 3: Educational Background		
High Schooling	1	0.5%
Diploma	8	3.8$
Graduation	127	59.12%
Post Graduation	65	30.18%

TABLE II
MANAGER RESPONDENT'S PROFILE SAMPLE

Criteria	Total Count	Percentage
Criteria 1: Job Profile		
Department Head	5	15.5%
Assistant Head	2	5.2%
Manager	18	49.15%
Assistant (Director)	4	14.34%
Operational Head	1	1.78%
Administrator	1	4.65%
Account Manager	1	1.82%
Criteria 2: Experience Count		
5-10 years	9	21.54%
11-15 years	19	62.3%
> 15 years	1	4.92%

Evaluation Indicators

The current study looked at three important aspects of cyber security practices: availability, trustworthiness, and privacy. Based on past study in the field, these dimensions were picked. The CIA triad is made up of three things: access, honesty, and privacy. It was used as an independent variable in this study. To keep data safe in ICT systems, only allowed users can get to it. This can be done with user IDs, passwords, policy-based security, and access control lists (ACLs). Integrity makes sure that data stays in its original form while it's not being used and that only allowed people can change it. To make sure that data or information systems are safe, things like data encryption, hashing methods, and private computing can be used. To stop people from changing or tampering with information, businesses should use digital signatures, regular tracking, and audits. Making sure that systems, information, and services are always available can be helped by cloud computing, software updates, predictive analytics, and hardware repair. The three-rank scale was used to figure out the deviations from the mean levels for the whole sample. This lets us figure out how much each dimension is present in our goal context.

Data Screening

The goal of this study is to find out how customers and managers in the Jordanian banking field feel about things. Over 30 responses were gathered from the manager dataset. Most of the responses were at the agree or highly agree level, with only a few at the neutral level. Because the sample size was small, statistical tools like Cook's distance were not used to get rid of the few outliers. In SPSS, 200 answers from the customer sample were coded. After coding, a few blank items were found, which added up to a missing ratio of 0.12%.When data was missing for Liker scale items, the median of nearby

Points was used to fill in the blanks.Then, regular trends in assessments were looked at using standard deviation. Lastly, Cook's distance was used to look for outliers. Any data above the 0.1 level was considered an outlier and taken out of the regression model. Using Cook's distance, five observations were found to be outliers and taken out of the group. After the data screening process for the sample of customers was done, 200 valid answers were looked at.SPSS [v.27] was used for coding and screening data, evaluating model fit, and doing descriptive analysis. PLS-SEM was used to test the measurement and structure models for the whole sample, checking how strong the relationships were between the model variables.

Study Design and Working Hypothesis

The adoption of information and communication technology is not to propagate risks that prohibit business and need to be represented in the literature. This study focuses on electronic services provided by commercial banks and seeks to address cyber

security practices (confidentiality, integrity, and availability) that enable flexibility, and service quality, and how that relates to customer satisfaction. Consequently, the following model (Figure 1), which aims to help outline and describe the relationship between cyber security practices as the independent variable and supply chain performance as the dependent variable.

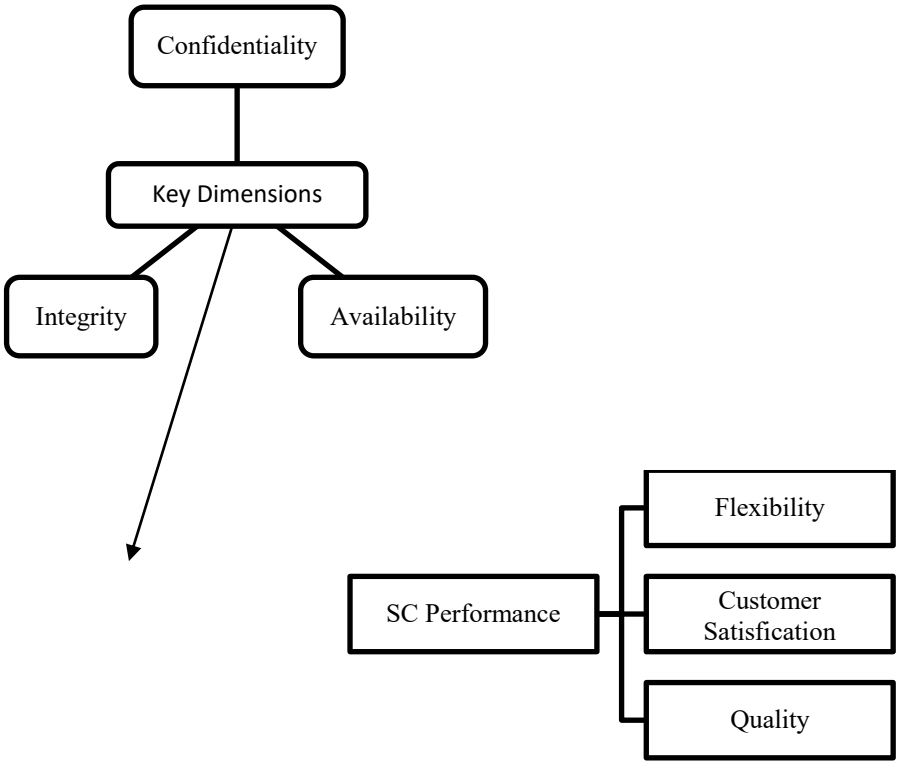

Figure 1. Research model

The conclusions significantly impacted our comprehension of cyber security and its impact on financial institutions. The study to improve performance by identifying cyber security threats and attacks in a globalized supply chain (SC) based on the information flow upstream and downstream across the SC. This study found that the cyber security program significantly impacted the proper use of cloud accounting, cyber security governance requirements, cyber risk assessment and management, and cyber security information management. The findings demonstrated that the banks' security procedures would be ineffective without knowledge and training. As a result, the hypothesis for this work is:

H1. Cyber security practices have a significant impact on the SCP of the commercial banking sector.
The following sub-hypotheses can be made based on this hypothesis and how cyber security is used:

H1.1: Confidentiality has a big effect on the SCP of the commercial banking sector.
Confidentiality protects information from being seen or accessed by anyone who is not authorized or trusted. Certain kinds of data can't be stored or used in certain ways because of confidentiality. There is a link between secrecy and information security, and confidentiality is a strong predictor of how safe people think their information is. One study [25] found that keeping information private is important for making internet banking systems safer.

H1.2: Integrity has a big effect on the SCP of the commercial banking sector
Integrity means the data is valid and precise and data can't be changed, lost, or disposed of unless permission is granted. The safe data handling, sharing, storage, and transfer keep data's integrity well. The study [3] found that honesty is very important for online banking platforms. The study used a paired sample T-test and structural equation modelling (SEM) to show that honest results are good for information security in a measurable way. In their work on the link between integrity and how customers see information security, Alaskan and Adjei-Quaye also discovered that integrity has a good effect on information security. Referential integrity in a database is not the same as data integrity, which says that changes can't be made without permission.

H1.3: Availability has a big effect on the SCP of the commercial banking sector.
It permits a person who has the rights to access the assets and information that related to it when needed."Availability" means that people are allowed to subject can get to data resources as many times as they need to or can just start up their own operations again after something unexpected happens. It is investigated what customers think about information protection and availability. Customers' sense of
how safe the information they send and receive over the Web is affected by how easily accessible the information is.

RESULTS AND DISCUSSION:-

Different cyber security-related data from the two samples was collected in the personal information area. Table 3 shows how customers responded to information about cyber security in the banking sector.

TABLE IIII
CUSTOMER RESPONSE ABOUT CYBER SECURITY

Criteria	Total Count	Percentage
Criteria 1: Electronic services		
Yes	200	91.5%
No	5	1.2%
Not sure	3	1.15%
No response	1	0.34%
Criteria 2: Cyber security risks		
Yes	11	4.39%
No	172	82.31%
Not sure	1	4.92%
Criteria 3: Cyber security practices Level		
Low priority	10	4.56%
Moderate priority	99	42.32%
High Priority	78	38.23%
Very High priority	14	6.7%

91.5% of those surveyed had used electronic services like Internet banking. Digital wallets and bank apps, which shows that the sample is good for this study. Only 1.2% didn't use electronic services, and 1.15% weren't sure. Overall, 82.31% of customers did not experience any cyber threat, risk, or problem, 4.39% did, and 4.92% were not sure. In total, 44.4% of respondents said that cyber security practices were moderately important. 38.23% said it was high priority, 6.7% said it was very high priority, and 4.56% said it was low priority. Overall, 82.8% of users had never talked to their bank about cyber security, 8.9% had, and 1.3% were not sure. Overall, 59.2% of customers said they had not experienced a security event due to an abusive or careless employee, 2.6% said they had, and 19.2% were not sure. Customers said that bank employees knew a lot about security risks (22.1%), some knew a lot (49.5%), and some didn't know or weren't sure (12.5%).
Table 4 shows a summary ratio and statistical analysis of the mean and standard deviation for the two groups' ideas about the amount of cyber security practices.

TABLE IVI
CUSTOMER RESPONSE ABOUT CYBER SECURITY

Construct	Mean Value	Std. value
Policy related to cyber security	4.25	0.35
Confidentiality principle	4.51	0.43
Integrity principle	4.27	0.47
Availability principle	4.25	0.37

With an average score of 3.37, the cyber security policies in banks got high marks. The mean scores for all practices were high, ranging from 4.51 to 4.27.The standard deviation values were between 0.43 and 0.37, which shows that the answers were mostly close to the mean value. This suggests that the assessment levels were all the same. The overall mean value for the cyber security

strategy was 3.54, which means that banks have a high level of implementation. With mean scores between 3.50 and 3.68, all things in this construct got high marks. The item that got the lowest score was "The bank is committed to cyber security rules and regulations set by the Central Bank." The item that got the highest score was "The bank defines the objectives, responsibilities, and work procedures related to the cyber security policy." The standard variation made it clear that the tests were all the same. The overall mean number for the confidentiality dimension was 3.40, which means that all of the items got high marks. The item with the best mean score, "My bank checks the customer's identity before any physical or electronic action," got 3.70 out of 5. The item that got the lowest mean score, "My bank teaches customers how to verify the company's identity on the Internet and mobile apps while using them," got a score of 4.13.The standard deviation numbers were less than 1, which means that the tests were all the same.

Hypothesis testing results indicated what the main results of this study were. The structural model was tested using path analysis, then we used the measure of variance, R2, to indicate how it can change over time. The hypothesis choice used the path coefficient and value of the t-statistic. The main hypothesis H1 indicated that cyber security practices have a very high evaluated influence on the dependent measure SCP. The effects given by cyber security practices' accounted for a lot of variance at 60.4% (Figure 2), the main hypothesis H1 indicated that cyber security practices had a high effect on the dependent variable SCP.

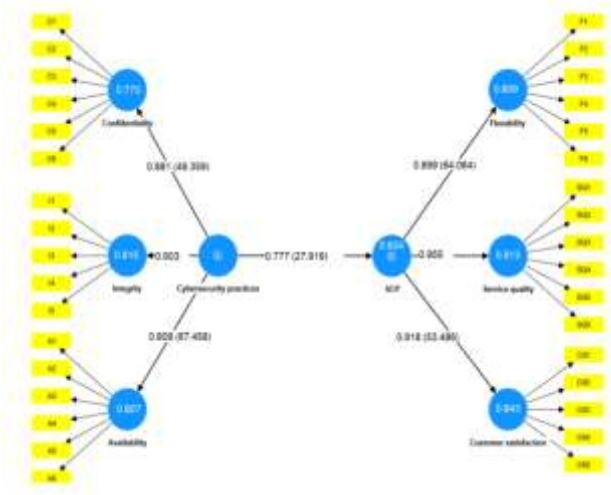

Figure 2. Structural model

This study looks at how cyber security practices affect the performance of supply lines in the banking sector in the northern part of Jordan. A custom-made questionnaire and the analytical/descriptive method were used to gather information. Statistics were used to look at the data, which led to several results that helped answer the study questions. Customers had good things to say about the level of cyber security measures. This is because most of the group was made up of people who use electronic services offered by banks, which meant they were good candidates for the study. Moreover, a lot of people said they worked with had no security problems in the banks they dealt with. However, bad things happened because customers thought banks should have started a conversation with them to clear up things linked to cyber security. Most of the customers in the sample said that employees didn't know much about cyber security. This showed that more courses and conferences need to be held on these topics, and there needs to be a way for clients and employees to talk to each other about cyber security to make everyone more aware of it.

CONCLUSION AND FUTURE SCOPE

The research emphasizes that hacking is a necessity for ensuring a reliable a transparent banking supply chain. Given increasing reliance on third-party integrations and digital interactions, banks expose themselves to cyber threats that can impact operations, steal confidential information, and diminish customer trust. The case study demonstrates that cybercriminals can impact an organization - and its third-party risk supply chain - through low cyber security practices. The negative impacts can unit an organization, but ultimately the effects can extend to the organization's operations as a whole. As shown in the case study, proper frameworks and solutions need to be in place in terms of cyber security that include vendor risk assessments, real-time threat assessments, and adherence to common policies including GDPR, RBI guidelines, and ISO 27001. It is evident that banks should move toward a proactive and collective action in an organization's approach to cyber security. Banks should leverage secure digital supply chain practices, seek out ongoing training for all stakeholders, and invest in new digital technologies (e.g., block chain, zero-trust architectures, and AI driven threat detection) committed to secure practices.

Not only do the findings of this study contribute to the overall understanding of cyber security practices and supply chain efficiency, but they also offer opportunities for future research and growing understanding of the potential impacts of cyber security on banking. Future research needs to hone in on those cyber security practices that have a greater influence on supply chain efficiency. Understanding the impact of continued, regular cyber security training and investments, and their long-term benefits for organizational resilience and consumer trust would similarly be of benefit. Additionally, comparisons between countries or industries may indicate promising practice and areas for improvement. Future studies can leverage the number of sampled institutions in Southern branch and beyond, especially if prioritized targeting managers from all bank branches, enabling further generalizations of the findings. Future research concerned with supply chain performance with customer satisfaction acting as a mediating variable, one that examined the influences of cyber security practices on employee performance in public banks would also be promising.

REFERENCES:-

[1] AbuAlKhair, D. M. H. M. I. (2023). The impact of internal audit quality in reducing cyber risks in order to support financial stability in electronic banks (a field study). Scientific Journal of Financial and Administrative Studies and Research, 15(1), 1–71.

[2] Al-Alawi, A. I., Mehrotra, A. A., & Al-Balsam, S. A. (2020). Cybersecurity: Cybercrime prevention in higher learning institutions. InImplementing Computational Intelligence Techniques for Security Systems Design (pp. 255–274). IGI Global.

[3] Alhassan, M. M., & Adjei-Quaye, A. (2017). Information security in an organization. International Journal of Computer (IJC), 24(1),100–116.Availableonline: https://ijcjournal.org/index.php/InternationalJournalOfComputer/article/view/820 (accessed on1 September 2024).

[4] Ali, N., Ahmed, A., Anum, L., Ghazal, T. M., Abbas, S., Khan, M. A., Alzoubi, H. M., & Ahmad, M. (2021). Modelling supply chain information collaboration empowered with machine learning techniques. Intelligent Automation and Soft Computing, 30(1), 243–257.

[5] Alkhatib, S. F. S. (2024). An advanced fuzzy approach for assessing supply chain resilience in developing economies. International Journal of Operational Research, 50(4), 401–425.

[6] Almufleh, N. M., & Alkhatib, S. F. (2023). The impact of supply chain management practices on the operational performance of 5-starhotels operating in Jordan. Jordan Journal of Business Administration, 19(1).

[7] Alnadi, M., & Altahat, S. (2024). Artificial intelligence applications for enhancing organizational excellence: Modifying role of supplychain agility. Problems and Perspectives in Management, 22(2), 339–351.

[8] Alotaibi, F., Furnell, S., Stengel, I., & Papadakos, M. (2016). A review of using gaming technology for cyber-security awareness. International Journal for Information Security Research (IJISR), 6(2), 660–666.

[9] Al-Sarhan, H. A.-M. S., & Al-Mashaqbeh, M. N. M. H. (2020). The impact of applying cyber security policy on the quality of accounting

[10] information in Jordanian commercial banks [Unpublished master's thesis]. Al al-Bayt University.

[11] Alzoubi, H., Alshurideh, M., Kurdi, B., Akour, I., & Aziz, R. (2022). Does BLE technology contribute towards improving marketing strategies, customers' satisfaction and loyalty? The role of open innovation. International Journal of Data and Network Science, 6(2),449–460.

[12] Arabyat, Y. A., Alarabeyyat, A., & Abuaddous, M. (2023, December 18–19). Overview of cyber security trends in Jordan's financial sector. International Conference of Reliable Information and Communication Technology (pp. 285–292), Johor Bahru, Malaysia. Available online: https://link.springer.com/chapter/10.1007/978-3-031-59707-7_25.

[13] Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? arXivarXiv:1901.02672.

[14] Baltacioglu, T., Ada, E., Kaplan, M. D., Yurt, A. O., & Cem Kaplan, Y. (2007). A new framework for service supply chains. The Service Industries Journal, 27(2), 105–124. Available online: https://www.tandfonline.com/doi/abs/10.1080/0264206060112262

[15] Baltacioglu, T., Ada, E., Kaplan, M. D., Yurt, A. O., & Cem Kaplan,Y. (2007). A new framework for service supply chains. The Service Industries Journal, 27(2), 105–124. Available online: https://www.tandfonline.com/doi/abs/10.1080/02642060601122629

[16] Beamon, B. M., & Balcik, B. (2008). Performance measurement in humanitarian relief chains. International Journal of Public Sector Management, 21(1), 4–25. Available online: https://www.emerald.com/insight/content/doi/10.1108/09513550810846087/full/ html.

[17] Byrne, B. M. (2016). Structural equation modelling with AMOS: Basic concepts, applications, and programming. Rutledge. Availableonline:https://www.taylorfrancis.com/books/mono/10.4324/9781315757421/structural-equation-modeling-amos-barbara-byrne.

[18] Cele, N. N., & Kwenda, S. (2024). Do cyber security threats and risks have an impact on the adoption of digital banking? A systematic literature review. Journal of Financial Crime, ahead-of-print.

[19] Cinnamon, J., Sjödin, D. R., & Parida, V. (2017). Adopting a platform approach in servitization: Leveraging the value of digitalization. International Journal of Production Economics, 192, 54–65.

[20] Chang, H. H., Wong, K. H., & Chiu, W. S. (2019). The effects of business systems leveraging on supply chain performance: Process innovation and uncertainty as moderators. Information & Management, 56(6), 103140.

[21] Chowdhury, M. M. H., Quad's, M., & Agawam, R. (2019). Supply chain resilience for performance: Role of relational practices and network complexities. Supply Chain Management: An International Journal, 24(5), 659–676.

[22] Craigie, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cyber security. Technology Innovation Management Review, 4(10), 13–21.

[23] Dam, S. M., & Dam,T. C. (2021). Relationships between service quality, brand image, customer satisfaction, and customer loyalty. The Journal of Asian Finance, Economics and Business, 8(3), 585–593.

[24] Daud, N. M., Mamud, N. I., & Aziz, S. A. (2011). Customer's perception towards information security in Internet banking system in Malaysia. Australian Journal of Basic and Applied Sciences, 5(9), 101–112. Available online: https://www.atlantis-press.com/article/125925996.pdf.

[25] Del Giorgio Solfa, F. (2022). Impacts of cyber security and supply chain risk on digital operations. Available online: https://www.aacademica.org/del.giorgio.solfa/495 (accessed on 1 September 2024).