INTERNATIONAL JOURNAL OF MANAGEMENT AND ORGANIZATIONAL RESEARCH

Cyber Resilience and its Impact on Improving the Quality of Digital Financial Services: An Applied Study at the Jordanian National Cyber Security Center

Dr. Ali Zaidan Fenjan
College of Basic Education, University of Kufa, Iraq

* Corresponding Author: **Dr. Ali Zaidan Fenjan**

Article Info

ISSN (online): 2583-6641
Volume: 04
Issue: 01
January-February 2025
Received: 20-10-2024
Accepted: 22-11-2024
Page No: 143-150

Abstract
This examine explores the critical courting between cyber resilience and the enhancement of digital monetary services fine. With the increasing reliance on virtual systems, economic establishments face escalating cyber threats that demand sturdy techniques to ensure provider continuity, protection, and trustworthiness. By focusing on the Jordanian National Cyber Security Center, this study examines how enforcing cyber resilience measures—which includes hazard intelligence, incident reaction, and continuous machine tracking—contributes to improving provider reliability, client pleasure, and operational performance.
The study employs a carried-out method, integrating each qualitative and quantitative tactics to assess the middle's strategies and their outcomes. Findings reveal that proactive cyber resilience frameworks substantially mitigate risks and bolster self-belief in digital financial transactions. The studies conclude with recommendations for strengthening public-non-public collaborations, improving staff abilities, and making an investment in superior technologies to preserve and enhance the satisfactory of virtual financial offerings in Jordan.

DOI: https://doi.org/10.54660/IJMOR.2025.4.1.143-150

Keywords: Cyber Resilience, Financial Services Quality, Jordanian National Cybersecurity Center

1. Introduction

In a more and more interconnected digital international, the rapid improvement of economic generation has revolutionized the way people and establishments interact with monetary offerings. However, the benefits of virtual transformation include full-size challenges, mainly in phrases of cybersecurity threats. These demanding situations require the adoption of strong cyber resilience strategies to defend sensitive statistics, make certain provider continuity, and beautify accept as true with among users of digital economic offerings. Cyber resilience, a comprehensive method to handling and mitigating cyber risks, is going beyond conventional cybersecurity measures through emphasizing the capacity to anticipate, withstand, recover from, and adapt to adverse cyber events. In the context of digital financial services, this resilience will become a vital factor in protecting transactions, safeguarding person information, and making sure the stableness of financial platforms (Björck, 2015:22) [7].
This observe specializes in the role of cyber resilience in improving the exceptional of virtual financial services, with a specific application to the Jordanian National Cyber Security Center. As a pivotal institution inside the cybersecurity framework in Jordan, the National Cyber Security Center plays a key position in establishing and retaining cyber resilience mechanisms that directly affect the u . S .'s digital financial ecological and economic device.
Drawing upon an implemented approach, this observes pursuits to explore the strategies utilized by the National Cyber Security Center to enhance cyber resilience, analyze their effect at the pleasant and reliability of virtual economic services, and offer actionable guidelines for stakeholders. This investigation will make a contribution to a deeper information of the way powerful cyber resilience practices enhance consider, safety, and performance in digital finance.

1.1 Problem of the Study

In the swiftly evolving digital financial device, ensuring the safety and reliability of economic offerings has end up a urgent challenge. Cyber resilience, which includes the capability to assume, respond to, get over, and adapt to cyber threats, performs a vital position in preserving and enhancing the fine of virtual monetary offerings.

Despite its importance, there is a loss of comprehensive implemented studies that explores the direct effect of cyber resilience techniques on the quality of digital monetary services in institutional frameworks. Specifically, the position of the Jordanian National Cyber Security Center in enhancing cyber resilience and its impact on improving provider satisfactory in the virtual monetary region stays unexplored. This studies seeks to fill this gap by means of investigating the realistic implications of cyber resilience on enhancing provider great. Therefore, the trouble of the take a look at is summarized in elevating the following questions:

- What is cyber resilience, and why is it vital for virtual economic offerings*?*
- How does the National Cybersecurity Authority contribute to enhancing cyber resilience within the virtual monetary sector in Jordan*?*
- What lessons can be discovered from the National Cybersecurity Authority's revel in to inform the improvement of cyber resilience frameworks in other countries?

1.2 Aims of the Study

The have a look at targets to discover the concept of cyber resilience and its importance in improving the exceptional of digital economic services. By analyzing the practices and strategies carried out with the aid of the National Cyber Security Center in Jordan, we will delve into the precise ways wherein cyber resilience may be applied to enhance the safety and reliability of digital economic structures*.*

1.3 Significance of the Study

The significance of the observe is as follows*:*

- With the increasing reliance on virtual monetary services, the chance of cyber threats has increased drastically. This look at explores how cyber resilience can act as a pivotal aspect in mitigating those risks and is consistent with the global want to beautify cybersecurity measures, specially in critical sectors together with finance*.*
- The recognition on improving the fine of digital monetary services highlights the direct blessings of robust cybersecurity practices, with an emphasis on higher consumer experience, consider, and operational performance*.*
- Three. By analyzing the Jordanian National Cybersecurity Center, the have a look at offers insights into how a countrywide-degree organisation can enforce cyber resilience techniques. It can serve as a version for other countries and companies looking for to enhance their virtual protection frameworks*.*
- The implemented nature of the observe ensures that the findings are actionable and applicable to enterprise practitioners, financial institutions, and policymakers. The examine also contributes to the existing literature with the aid of immediately linking cyber resilience to service first-class inside the monetary zone, imparting a completely unique angle on the interrelationship among security and service improvement.

1.4 Hypothesis of the Study

The study hypothesis is a possible solution to the study problem and the main study hypothesis states: "Cyber resilience significantly affects the quality of digital financial services at the Jordanian National Cyber Security Center."

2. Theoretical Background

2.1 Theoretical framework of the independent variable cyber resilience

2.1.1 The concept of cyber resilience

Cyber risks have evolved over the past 25 years from minor annoyances to potentially disastrous occurrences that might jeopardize the survival of businesses that rely on technology. Cyber hazards are considered a "source of systemic risk to the financial system" by the European Systemic Risk Board, which oversees the European Union's financial system (ESRB 2020). This is due to worries that a cybersecurity attack would get worse and trigger a liquidity crisis, which would erode financial actors' confidence and cause the system to become unstable. Although such catastrophic scenarios may appear exaggerated, an International Monetary Fund research from 2018 projected that the annual losses from cyberattacks on 7,947 banks worldwide totaled $97 billion (9% of net revenue) using data from the Operational Risk Data Sharing Association, ranging from $147 billion to $201 billion (14% to 19% of net income), with the value at risk (VaR) changing over time. Under the worst circumstances, the most pessimistic models predict annual losses of up to 51% (Bouveret, 2018: 20-21) [11].

One of the best examples of how cyber threats may create such devastating shocks to the essential infrastructures on which we depend is the well-known Danish shipping business APM-Maersk. What is noteworthy is how devastating such incidents can be for even the largest and most established organizations, and how victims are adopting a cyber resilience model instead of their traditional cybersecurity risk management model. The identity of the attackers and the attack's implications for the current state of cyber conflict (Arquilla and Ronfeldt, 2007; Rid, 2012; Rid and Buchanan, 2015) [1, 22, 23] are not particularly noteworthy.

One of the best examples of how cyber threats may create such devastating shocks to the essential infrastructures on which we depend is the well-known Danish shipping business APM-Maersk. What is noteworthy is how devastating such incidents can be for even the largest and most established organizations, and how victims are adopting a cyber resilience model instead of their traditional cybersecurity risk management model. "The identity of the attackers and the attack's implications for the current state of cyber conflict" (Arquilla and Ronfeldt, 2007; Rid, 2012; Rid and Buchanan, 2015) [1, 22, 23] are not particularly noteworthy. While Maersk was infected in less than seven minutes, it took almost two hours to bring the company's entire global network offline in a fruitless attempt to thwart the attack (Greenberg, 2019: 152) [15].

Maersk's management provided a clear and helpful explanation of how it dealt with the aftermath of the attack: Adam Banks, the company's chief information and technology officer, gave a sobering assessment of the damage: 49,000 PCs and printers, 83% of the 1,200 apps needed to run the business, and 56% of the 6,200 servers were instantly rendered unusable; mobile phones were down because all contacts using Microsoft Outlook for synchronization had been erased; and fixed telephone lines that were needed to coordinate the response were unavailable due to their reliance on the computer network (Ritchie 2019) [24]. Additionally, encrypted data backups were not recoverable because all domain controller servers had to be

rebuilt on a map of the compromised network (Greenberg, 2019: 194) [15].

One of Maersk's first decisions was to abandon its existing crisis management protocol, which had never included plans for such a comprehensive level of destruction, and instead rebuild its network from scratch, with the help of a consulting firm that had been given a blank check. The company had a lucky break when it discovered that the power outage in Nigeria had spared a single server that could be used to rebuild the entire network. Starting with that single machine, Maersk reinstalled 2,000 laptops within 10 days and within a month had issued nearly 50,000 clean devices to employees. Even though the shock cost the company between $200 and $250 million, it managed to survive, and its willingness to share lessons learned along the way improved its reputation. Maersk began with that one machine, reinstalling 2,000 laptops in 10 days, and within a month, it had distributed nearly 50,000 clean devices to staff members. The firm survived the shock, and its openness to share lessons gained along the road improved its image, despite the massive losses it sustained (between US$200 and US$250 million). In the meantime, employees who had went back to pen and paper and received orders via personal Gmail and WhatsApp accounts were able to maintain 80% of container traffic (Crozier, 2018) [12]. According to the company's CEO, his new goal was to leverage the incident to eventually make [Maersk's] cybersecurity management skills a competitive advantage (Crozier, 2018) [12].

An excellent illustration of cyber resilience in action is the Maersk experiment or experience, wherein the company was completely overwhelmed by its current cybersecurity measures despite what was thought to be a sufficient level of readiness. An unexpected threat led to a situation that had never been encountered or even imagined. Although luck was a factor in overcoming this obstacle, it would not have been sufficient if staff members from different areas of the company had not banded together and come up with creative ways to keep things going. External resources were also necessary since, without the consulting firm's experience, Maersk might not have been able to reconstruct its network so quickly.

When the local supply of USB drives ran out, Maersk was allowed to use its own IT networks for fresh installations, demonstrating the confidence and goodwill it had developed among its peers (Ritchie, 2019) [24]. The organization was able to showcase its new cybersecurity knowledge at the World Economic Forum a year later, thanks to the successful adaption process that resulted from this significant shock (Olenick, 2018) [19]. Despite instances like these, a lengthy history of application in materials science, ecology, and psychology, and its recent broad adoption as a strategy for managing Anthropocene concerns, the idea of resilience remains marginal in the literature on cyber risk (Boin and van Eeten, 2013) [9]. When the local supply of USB drives ran out, Maersk was allowed to use its own IT networks for fresh installations, demonstrating the confidence and goodwill it had developed among its peers (Ritchie, 2019) [24]. The organization was able to showcase its new cybersecurity knowledge at the World Economic Forum a year later, thanks to the successful adaption process that resulted from this significant shock (Olenick, 2018) [19]. Despite instances like these, a lengthy history of application in materials science, ecology, and psychology, and its recent broad adoption as a strategy for managing Anthropocene concerns, the idea of resilience remains marginal in the literature on cyber risk (Boin and van Eeten, 2013) [9].

The ability to accomplish a desired result in the face of ongoing negative cyber occurrences is known as cyber resilience (Björk *et al*., 2015: 312). This notion sets cyber resilience apart from cybersecurity, which focuses on anticipating and averting negative outcomes. The ability of an organization to anticipate, respond to, and recover from cyber incidents while preserving essential operations is often referred to as cyber resilience. In the context of financial services, and particularly within organizations such as the Jordanian National Cyber Security Center, enhancing cyber resilience is critical due to the increasing frequency and sophistication of cyber attacks targeting this sector (Annarelli, & Palombi, 2021: 14) [2].

2.1.2 The importance of cyber resilience

The importance of cyber resilience in financial services is as follows: Cyber attacks can cause major operational interruptions and financial losses, and the banking sector is especially sensitive to them. A strong cyber resilience strategy that emphasizes not just prevention but also recovery and adaptability is necessary due to the growing sophistication of these attacks. By guaranteeing that institutions can continue to provide services even in the event of cyberattacks, this dual focus contributes to the improvement of the quality of digital financial services (Petrenko, 2022: 159) [21].

2.2 Theoretical framework for the dependent variable: financial services quality

2.2.1 Concept of digital financial services quality

Accessibility and financial inclusion have altered as a result of digital financial services. Particularly in underserved locations, the effectiveness of meeting customers' requirements depends on the caliber of these services. Good digital financial services can lower transaction costs, increase consumer satisfaction, and facilitate access to official financial accounts (Sharma & Díaz Andrade, 2023: 586) [25]. For underprivileged groups, digital financial services have greatly increased access to financial resources. For underserved populations, these services improve financial stability and alleviate poverty by making official accounts easier to use and lowering remittance fees. This impact underscores the importance of maintaining high-quality services to ensure that the benefits of digital finance are widely distributed (Ozili, 2018: 349) [20]. The efficacy, efficiency, and user convincement of digital financial services are all considered aspects of its quality. Excellent digital financial services satisfy clients, guarantee dependability, and add value for both people and companies (Luo *et al*., 2022: 18) [17]. The effectiveness and efficiency of financial services delivered via digital channels in satisfying client demands and expectations is another aspect of digital financial services quality. The quality of digital services is a key factor in achieving the success of any financial institution in the labor market due to technological growth (FinTech). (Bapat, 2022: 305) [3].

2.2.2 Dimensions of financial services quality

Digital financial services include a wide range of financial products and services offered through digital channels. The quality of these services is critical to ensuring customer satisfaction and promoting financial inclusion. The following

are the main dimensions of quality in digital financial services: (Bankuoru Egala, *et al*, 2021: 148) [4].

1. Access and customer support: This component describes how customers, particularly underserved groups, can access digital financial services. It takes into account things like the services' geographic reach and the state of the technology infrastructure. Promoting economic inclusion and allowing customers to take benefit of digital financial services require extensive get admission to. This size also consists of the efficacy and accessibility of customer service offerings, like as help desks and online guide. Maintaining patron delight and right away resolving troubles depend on having high-quality customer service.
2. Usage: This measurement measures the frequency and effectiveness of customers' interplay with virtual financial services. It displays the real adoption and use of those services with the aid of consumers. High utilization prices suggest that the services meet customers' desires and integrate into their economic behaviors.
3. Data Quality: The precision, comprehensiveness, and dependability of the statistics utilized in virtual financial offerings are the principle issues of this dimension. It is important for danger management and sound choice-making. Customer believe in economic services can be broken with the aid of bad records fine, which also can bring about extreme operational concerns. Aspects of provider delivery consisting of dependability, protection, and consumer enjoy are all protected in high-quality. It additionally covers how fast the provider responds to questions and issues from customers. High-great offerings sell person believe and pride, that is crucial for lengthy-time period engagement and loyalty.

2.2.3 The Impact of Cyber Resilience on Digital Financial Services

The quality of digital financial services is influenced by several factors, including data integrity, customer experience, and their role in promoting financial inclusion. As the digital financial landscape continues to evolve, focusing on these aspects will be critical to maximizing the benefits of these services for all users (Yadav, 2023: 57) [28]. Implementing effective cyber resilience measures can lead to several positive outcomes for digital financial services: Dupont, 2019: 34) [13].

1. By demonstrating a commitment to cybersecurity, financial institutions can build trust with customers, which is essential for the adoption of digital services.
2. Cyber resilience strategies ensure that essential services remain operational during and after a cyber-incident, thereby minimizing disruptions.
3. As cybersecurity regulations tighten globally, having a robust cyber resilience framework helps institutions comply with legal requirements, reducing the risk of penalties.
4. Focusing on resilience enables institutions to better understand and manage their cyber risks, leading to more informed decision-making and resource allocation.

3. The practical side of the Study

3.1 A rapid glance at the research center

The National Cyber Security Center is a government agency that aims to plan, develop, and implement an effective cyber security system at the national level in order to protect the Kingdom from cyber threats and successfully combat them in a way that maintains national security, the sustainability of work, and the safety of people, property, and information.

The centre aims to train, qualify, raise awareness, and educate employees in the public and private sectors as well as all societal segments in order to create a safe and dependable Jordanian cyber space. It also aims to make Jordan a regional and global hub for innovation and excellence in this field by equipping them with the knowledge and skills they need to reduce risks and threats in accordance with best practices in the field of cyber security and in a way that ensures the highest level of efficiency.

Critical infrastructure is a collection of electronic systems and networks, physical and intangible assets, or cyber assets and systems whose continued functioning is required to ensure the security of the state, its economy, and the safety of society, according to Cybersecurity Law No. 16 of 2019. Since the law has defined critical infrastructure using the definition above and stated that critical infrastructure is essentially networks and information systems that are closely linked to the security of the state, the economy, and the safety of society, Article 6 of that law states that the Center will be in charge of identifying critical infrastructure networks and their sustainability requirements in order to achieve its goals, the following basic criteria have been adopted, and it is sufficient for one of them to apply to the sector in order for it to be considered a critical infrastructure sector:

- State Security.
- Economy.
- Community Safety.

In light of the above, the following sectors were considered critical infrastructure sectors: (Official website of the National Cyber Security Center)

1. Government services sector
2. Industry and trade sector
3. Financial and banking sector
4. Communications and information technology sector
5. Energy sector
6. Health sector
7. Agriculture, water and environment sector
8. Transportation sector
9. Education sector
10. Defense and security sector

3.2 Main services provided by the center

Through its various services, the center develops scientific research capabilities in all aspects of cybersecurity and works to create an integrated awareness system among individuals and institutions in order to accomplish its goals. These services include the following: (National Cybersecurity Center's official website):

1. Responding to national and federal cybersecurity incidents, offering advice, and publishing relevant findings.
2. Keeping an eye on government networks, examining data and movement records, and alerting the appropriate authorities to hacking cases that could compromise government websites, systems, or institution networks.
3. Analyzing digital evidence, detecting malware, and determining the cause and mechanism of hacking.
4. Getting reports and grievances about cybersecurity

events.

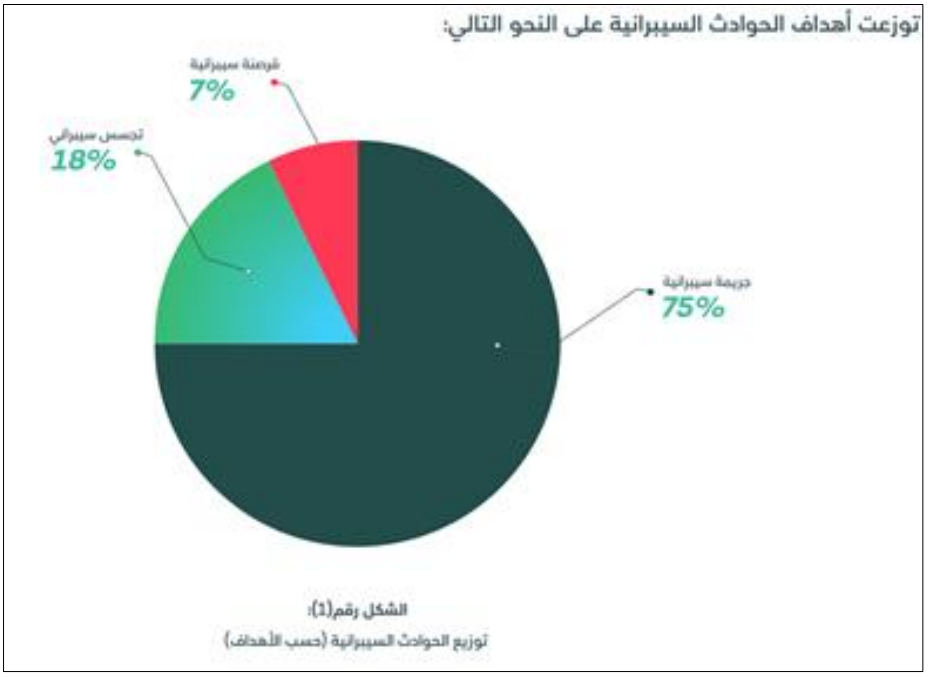
5. Creating national legislative frameworks for cybersecurity risk management and governance.
6. Creating and putting into effect cybersecurity rules.
7. Cybersecurity workshops for many societal groups, including individuals and institutions.
8. Institutional and individual training programs.
9. Cybersecurity and information contests for college and university students. 10. Information security guidelines and security alerts for individuals.

3.3 Statistics of incidents that affect government and national networks

The center handled 3582 cyber attacks in 2024, which targeted several government agencies and ministries in addition to several critical institutions.

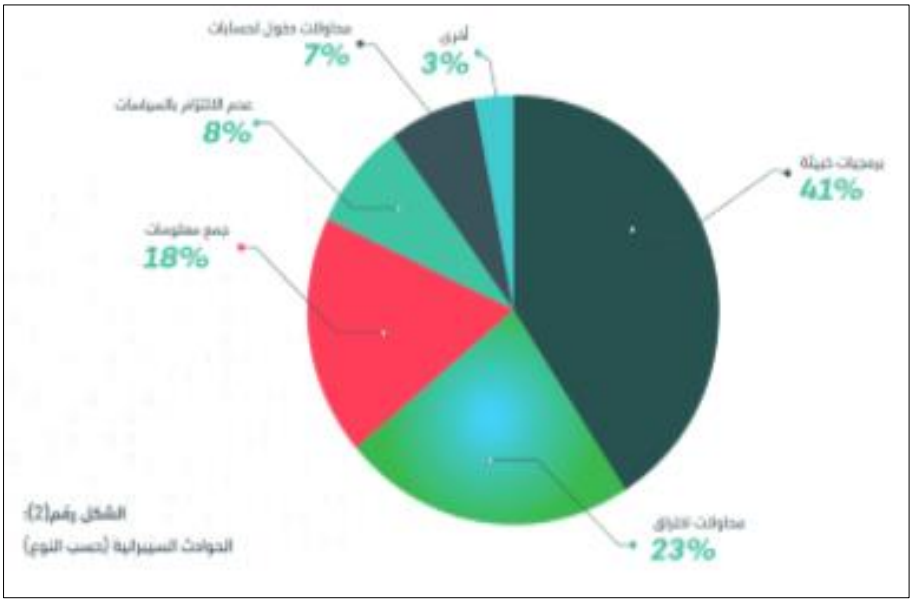
Due to institutions' greater commitment to putting security policies and measures in place, it was observed that the number of detected cyber incidents fell by 23% from 2023 to 2024. However, even though the number of incidents decreased in 2024, the overall trend of incidents is still high when compared to prior years.

Cybercrime is the word for unlawful activities carried out through computers or the Internet, including data theft, money demands, the installation of malicious software, and general device hacking.



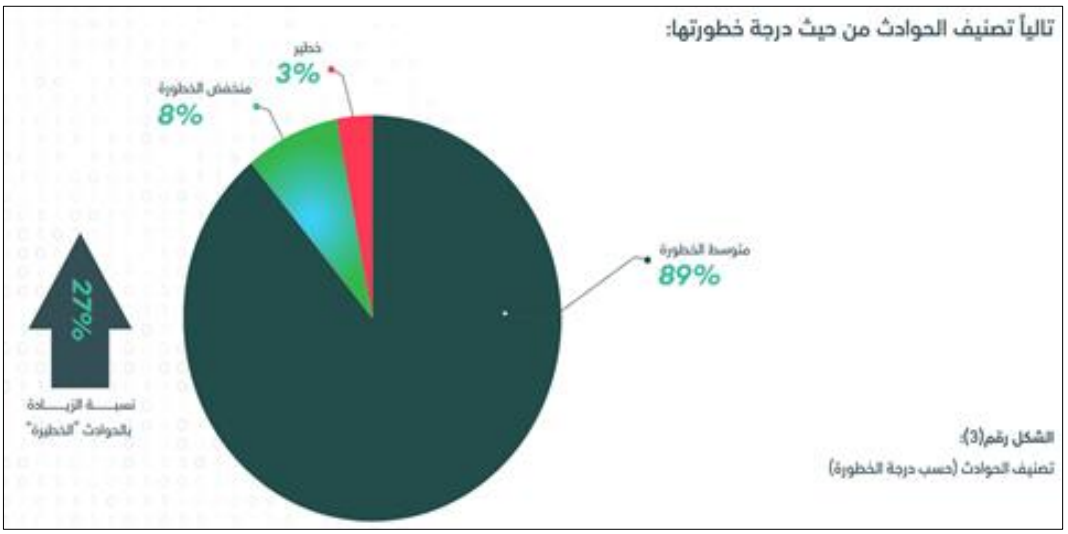
Source: National Cyber Security Center Reports 2024

Fig 1:

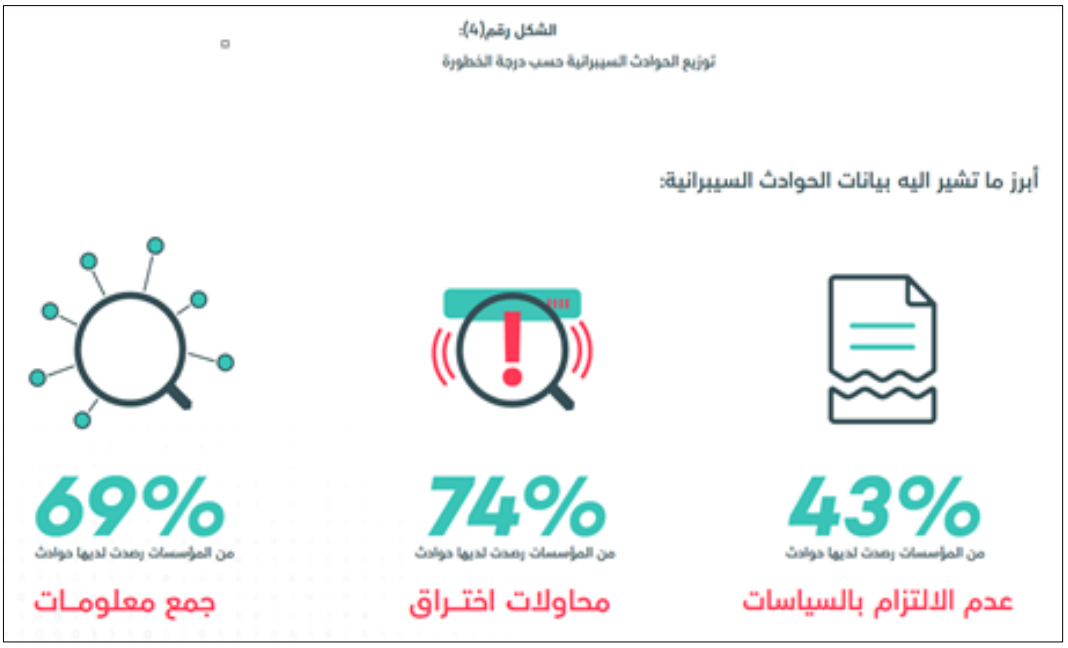


Source: National Cyber Security Center Reports 2024

Fig 2:



Source: National Cyber Security Center Reports 2024



Source: National Cyber Security Center Reports 2024

3.3 Influence relationships

The main effect hypothesis states that there is a significant effect relationship between cyber resilience and achieving the quality of financial services. The results of testing this hypothesis showed Table (1) Analysis of variance between variables on indicators indicating the relationship.

Table 1: Analysis of variance (ANOVA) for the relationship between cyber resilience and the quality of financial services

Model	Sum of squares	DF	Mean Squares	F	P-Value
Reg.	16.356	1	16.356	432.862	0.000
Res.	3.457	***40***	0.22		
Tot.	19.813	***41***			

Prepared by the researcher based on the outputs of the computer.

Table (2) shows the model coefficients.

Table 2: The model coefficients

Model	Unstandardized Coefficients		Standardized Coefficients		P-Value
	B	Std. Err.	B.	T	
Constant	0.603	0.126		3.329	0.000
X	0.812	0.042	0.882	24.765	0.000

Prepared by the researcher based on the outputs of the computer.

Table 3: Summary of analytical indicators of the impact of cyber resilience on the dimensions of financial services quality

Significance level	cyber resilience	Indicators	Dimensions of digital financial services quality
0.05	206.67	F	الوصول ودعم الزبائن
	0.000	P value	
	0.540	R2	
	0.735	B	
0.05	103.65	F	الاستخدام
	0.000	P value	
	0.401	R2	
	0.634	B	
0.05	231.19	F	جودة البيانات
	0.000	P value	
	0.646	R2	
	0.804	B	
0.01	264.98	F	ابعاد جودة الخدمات المالية الرقمية مجتمعة
	0.000	P value	
	0.777	R2	
	0.882	B	

Prepared by the researcher based on the outputs of the computer.

Table (3) above, which summarizes the analysis indicators at the level of hypothetical dimensions, reveals the following results:

1. As the calculated value of (F) was (206.67), greater than the tabular value at the level of (P <=0.05), and the value of (B) reached (0.735), access and customer support had a significant impact on the quality of financial services. The independent variable (access and customer support) explains 54.0% of the dependent variable (quality of financial services), according to the coefficient of determination value (0.540 R2=).
2. The calculated value of (F) was 103.65, which is higher than the tabular value at the level of P <=0.05. The value of (B) reached 0.634%. The independent variable (use) accounts for 40.1% of the dependent variable (quality of financial services), as indicated by the coefficient of determination value of 0.401 = R2. Use had a significant impact on the quality of financial services.
3. The calculated value of (F) was (231.19), which is greater than the tabular value at the level of (P <=0.05). The value of (B) was (0.804), and the independent variable (data quality) explains 64.6% of the dependent variable (quality of financial services), as indicated by the coefficient of determination value of (0.646 R2 =). These results demonstrate that data quality had a significant impact on the quality of financial services.
4. Since the independent variable of cyber resilience explains 77.7% of the changes in the dependent variable (quality of financial services), as indicated by the coefficient of determination value of 0.777, the combined effect of cyber resilience had a significant impact on the dimensions of financial services quality. The calculated value of (F) was (164.98), which is greater than the tabular value at the level of (P <=0.01), and the value of (B) was (0.882). In light of the analytical indicators in Table (7) above, it is clear that all dimensions of cyber resilience had a significant impact on the quality of financial services.

This indicates the acceptance of the second main hypothesis and the hypotheses arising from it, despite the difference in the strength of the impact between these dimensions.

4. Conclusions and Recommendations

4.1 Conclusions

This study aimed to investigate the relationship between cyber resilience and the quality of digital financial services, with a focus on the Jordanian National Cyber Security Center. The study findings highlight several key conclusions as follows:

1. Cyber resilience is a crucial element of turning in terrific virtual monetary services. A sturdy cyber resilience framework permits financial institutions to withstand cyber-attacks, limit disruptions, and maintain the integrity and availability of their offerings.
2. The National Cyber Security Center is a key player in promoting cyber resilience inside the Jordanian monetary zone. Its efforts in developing and implementing cybersecurity requirements, conducting chance checks, and offering incident reaction offerings make contributions notably to the general cyber resilience posture of economic institutions.
3. Three. Strong leadership and governance are crucial: Effective leadership and robust governance practices are important to constructing and sustaining cyber resilience. Clear cybersecurity policies, risk management frameworks, and regular security checks are vital to keeping a excessive level of protection.
4. Educating personnel approximately cyber threats, high-quality practices, and incident reaction strategies is important. A well-skilled body of workers is the first line of protection in opposition to cyber assaults .
5. Collaboration between monetary institutions, the National Cyber Security Center, and other applicable stakeholders is essential to proportion danger facts, excellent practices, and instructions found out. Sharing information allows companies to proactively cope with emerging threats and vulnerabilities.

4.2 Recommendations

Based at the findings, numerous hints may be made to enhance cyber resilience and the satisfactory of virtual financial services:

1. Financial establishments ought to spend money on superior cybersecurity technology that can locate and mitigate threats in real time. This includes implementing AI and gadget studying answers to enhance chance

detection capabilities.
2. Creating a established framework for cyber resilience can assist groups systematically address vulnerabilities. This framework ought to include threat evaluation, incident response planning, and healing strategies.
3. Three. Regular worker training and cognizance applications are critical. These programs need to awareness on spotting phishing tries, know-how facts protection regulations, and promoting a cybersecurity subculture.
4. Financial establishments must collaborate with cybersecurity professionals and organizations to stay updated on the contemporary threats and great practices. This collaboration could also encompass sharing threat intelligence to beautify collective protection.
5. Five. Continuous testing of cybersecurity measures through simulations and penetration checking out can assist pick out vulnerabilities. Organizations should additionally frequently replace their security protocols to evolve to evolving threats.

7. References

1. Arquilla J, Ronfeldt D. Cyberwar is coming! Comp Strategy 1993;12(2):141-65.
2. Annarelli A, Palombi G. Digitalization capabilities for sustainable cyber resilience: a conceptual framework. Sustainability 2021;13(23):13065.
3. Bapat D. Exploring the relationship between lifestyle, digital financial element and digital financial services experience. Int J Bank Mark 2022;40(2):297-320.
4. Bankuoru Egala S, Boateng D, Aboagye Mensah S. To leave or retain? An interplay between quality digital banking services and customer satisfaction. Int J Bank Mark 2021;39(7):1420-45.
5. Bastien DT, Hostager TJ. Jazz as a process of organizational innovation. Commun Res 1988;15(5):582-602.
6. Bilge L, Dumitraş T. Before we knew it: an empirical study of zero-day attacks in the real world. In: Proceedings of the 2012 ACM conference on Computer and communications security; 2012. p. 833-44.
7. Björck F, Henkel M, Stirna J, Zdravkovic J. Cyber resilience–fundamentals for a definition. In: New Contributions in Information Systems and Technologies: Volume 1. Springer; 2015. p. 311-6.
8. Bodeau D, Graubart R, Picciotto J, McQuaid R. Cyber resiliency engineering framework. MTR110237, MITRE Corporation; 2011.
9. Boin A, Van Eeten MJ. The resilient organization. Public Manag Rev 2013;15(3):429-45.
10. Bossong R, Wagner B. A typology of cybersecurity and public-private partnerships in the context of the EU. Crime Law Soc Change 2017;67:265-88.
11. Bouveret A. Cyber risk for the financial sector: A framework for quantitative assessment. International Monetary Fund; 2018.
12. Crozier R. Maersk Had to Reinstall All IT Systems after NotPetya Infection. itNews 2018.
13. Dupont B. The cyber-resilience of financial institutions: significance and applicability. J Cybersecur 2019;5(1):tyz013.
14. European Systemic Risk Board. The General Board of the European Systemic Risk Board held its 36th regular meeting on 19 December 2019 [Internet]. 2020 [cited 2024 Jul 19]. Available from: https://www.esrb.europa.eu/news/pr/date/2020/html/esrb.pr200107~29129d5701.en.html
15. Greenberg A. Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers. Anchor; 2019.
16. Linkov I, Eisenberg DA, Bates ME, *et al*. Measurable resilience for actionable policy. Environ Sci Technol 2013;47(18):10108-10.
17. Luo D, Luo M, Lv J. Can digital finance contribute to the promotion of financial sustainability? A financial efficiency perspective. Sustainability 2022;14(7):3979.
18. National Cyber Security Centre. Russian military 'almost certainly' responsible for destructive 2017 cyber attack [Internet]. 2018 [cited 2024 Jul 19]. Available from: https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack
19. Olenick D. NotPetya Attack Totally Destroyed Maersk's Computer Network: Chairman. SC Media 2018.
20. Ozili PK. Impact of digital finance on financial inclusion and stability. Borsa Istanb Rev 2018;18(4):329-40.
21. Petrenko S. Cyber resilience. River Publishers; 2022.
22. Rid T. Cyber war will not take place. J Strateg Stud 2012;35(1):5-32.
23. Rid T, Buchanan B. Attributing cyber-attacks. J Strateg Stud 2015;38(1-2):4-37.
24. Ritchie R. Maersk: Springing back from a catastrophic cyber-attack. I-Global Intelligence for Digital Leaders 2019.
25. Sharma H, Díaz Andrade A. Digital financial services and human development: current landscape and research prospects. Inf Technol Dev 2023;29(4):582-606.
26. National Academies of Sciences, Engineering, and Medicine. Disaster resilience: A national imperative. Washington, DC: The National Academies Press; 2012.
27. Van Eeten M, Nieuwenhuijs A, Luiijf E, Klaver M, Cruz E. The state and the threat of cascading failure across critical infrastructures: the implications of empirical evidence from media incident reports. Public Adm 2011;89(2):381-400.
28. Yadav D. A Framework for Implementing Data Integrity Program Enabling Mid-Size Financial Institutions to Meet United States Federal Reserve Data Quality Requirements for Model Risk Management [dissertation]. University of Arkansas at Little Rock; 2023.