Journal of Education for Pure Science- University of Thi-Qar
Vol.14, No. 4 (2024)
Website: jceps.utq.edu.iq Email: jceps@eps.utq.edu.iq

DOI: https://doi.org/10.32792/jeps.v14i4.420

Shared Cybersecurity Responsibilities in the Banking Sector :

A Case Study of the Republic of Iraq

Mohammed Fareed Mahdi
Ministry Of Higher Education And Scientific Research
University Of Thi_Qar
mfmsprof@utq.edu.iq

Received 6/6/2024, Accepted 22/7/2024, Published 1/12/2024

Abstract:

In order to protect data security, the study examined the relationship between online banks and their clients. Using a mixed-methods approach it was possible to identify a commitment to cybersecurity responsibilities and a common understanding between banking sector and their customers. The results showed that customers believe that banks' cybersecurity measures were effective and they had a strong sense of personal responsibility to follow security precautions when using online banking. The study also underlined how important cutting-edge technologies are to strengthening cybersecurity defenses. The study provides several recommendations to improve cybersecurity procedures and address cyber threats in the banking industry, including investi1ng in cybersecurity talent, collaborating with partners, integrating cutting-edge technologies, conducting frequent security assessments, and improving customer communication.

Keywords: Cybersecurity - Online Banks - Data Security - Customer Responsibility - Advanced Technologies.

1. Introduction:

In the banking sector, the use of digital platforms enhances the effective services to customers. However, cybersecurity threats pose significant dangers to both banks and their customers, ranging from data or identity theft to financial fraud. These risks rises questions about information security & trust between the bank and their customer . Online banks also face difficulties in facing cyber threats to protect their systems & sensitive data. Then, the responsibility for cyber security cannot fall only on banks, on the other hand customers also have a (Vital role)

The objectives of this research are to to analyze the cybersecurity risk assessment and methods in banking industry by identifying the processes followed by the organization starting from the types ,risks and threats. This research trying to identify how: cybersecurity can meet the needs of internal and external customers. By addressing best practices for managing cybersecurity risks in banking services and focused on transparent incident response plans and continuous monitoring systems as important elements of a cybersecurity strategy.

Furthermore, this research aims to provide recommendations about the data security in (Banking sector) by using new technologies such as: AI, IOT and ML. The new technologies will increase the efficiency of risk assessment and Sector Ability in facing future threats.

1.1 The research Questions:

1. What are the methodologies for assessing cybersecurity risks in banking services?

2. How can customers and the banking facility participate in protecting information security and activating cybersecurity tools (such as firewalls, encryption, multi-factor authentication, and intrusion detection systems)?

1.2 Research hypotheses:

- Human Factor represented as (Customers) who shares responsibility with the banking sector to protect data according to their awareness of the concept of cyber security and the threats they will face.
- Many technology tools are used to activate (Cybersecurity)in the banking sector.

2. Theoretical Framework:

- Cybersecurity

It's the process which prevents "Cyberattacks" & lowering the probability of falling victim into such a cybercrime (Alothaim et al., 2022). Technology is ever-evolving and has an impact on nearly every element of life. People may now connect globally more quickly and easily via digital communication technology. Digital technology has use in business, industries, corporations, and educational establishments. Technology has many advantages, but it also has many drawbacks including a number of risks and serious threats known as cybercrimes. Criminal conduct directed against digital technology such as (Mobile devices, computers & Networks) is known as cybercrime.

According to Pathan's study (2022) he stated that the term 'Digital' has various kinds of understandings, nonetheless, it could be best portrayed as electronic correspondence utilizing PCs and figuring gadgets and in accordance with that 'The internet' is the virtual climate made with the guide of data and correspondence advancements. Once more, security for (The internet) is spelt in two distinct ways: 'Network protection' and 'Network protection'. Both are tracked down in the writing in bounty, however they have a similar significance. One of the most reliable definitions for this would be “The assurance of programming, equipment and information assets” associated and put away on the Web or Web like climate is known as Network safety as a general rule this is about the security of the web-based climate and the items accessible in this climate (Pathan, A., 2022).

- Banking Sector:

The banking sector is the main driver of the front office staff of EDB branches as they are responsible for selling financial products and services and recruiting and retaining clients (Faria & Çipi, 2020).According to Семеняк, A. (2021), “The banking sector” is consisting of several national bank types functioning under one monetary system is essential to the viability of a nation's economy. (Семеняк, A., 2021)

- E- Banking:

"Electronic banking services" are type of banking services which the funds are transferred electronically in addition to traditional ways in exchanging cash, checks and paper documents. Furthermore, Iraqi government has followed the example of other countries in applying electronic banking services to provide its services to citizens (Mousa et al., 2021). E-banking utilizes new distribution channels such as mobile and Internet services to lower transaction costs that optimize service delivery and give clients anytime, anywhere access to services (Abdulla & Al-Hassani, 2022).

- Customer Behavior:

Customers control the market such as kings. The needs of the consumer have a big impact on banks, accordingly the needing for banking services has grown with the population. "Customer satisfaction and behaviors are influenced by many variables including effectiveness or competition and the service quality. The customer and the organization's overall performance are related. In addition to satisfying customers, it's important to develop strategies with plans to help the bank retain them and as customer behavior plays a significant role in determining the bank's acceptability and dependability. Banks will dependent on "the information technology" in the upcoming years so it will be critical to understand customer preferences for technological advancements in the banking industry. Customer perception provides a more thorough understanding of the client which is a necessity (Mishra, A., & Rajwani, P., 2020)

2.1 Banking Sector Cybersecurity Insights:

Depending on the importance of the data that related to the banking and financial sector, this sector has been a target of cyber attacks. Furthermore, the banking sector is dealing with more threats from cyber criminals as a result of its depending on technology and digital transformation. The banking industry is the foundation of the country's economy as it is linked to many other industries including mining, industry, health and petroleum, any major damage that could be caused to the banking industry could therefore extend to the entire economy. As a result, there was a need for protection from cyber threats and for risk management because it provides a framework for understanding the nature of cyber threats and how to address them, so that institutions are better able to assess their risks and create real strategies to Mitigate the risks with understanding the consequences of a "Cyber Attack" (Darem et al, 2023).

According to Darem study (2023) that aims to give a thorough examination of “cyberthreats” in the banking and financial industries, highlighting common threats as well as their characteristics and nature to aid in categorization. The paper makes a significant contribution by classifying cyber threats to the banking and financial sectors according to their technicality and severity. This categorization aids in determining the proper countermeasures needed to lessen the risks associated with each kind of threat. The study also examines organizational, non-technical, and technical countermeasures as well as legal and regulatory safeguards against cyberattacks that are used to safeguard financial transactions. Various research have been carried out to recognize and categorize cyber risks within the banking and financial sectors. In order to ensure the safety of the banking institution from cyberattacks in the digitalization, Shkodinsky (M. N. Dudin and S. V. Shkodinsky, 2022) carried out a critical analysis of the national and international academic papers and recommendations for future.

In addition to the many advantages that come with digitizing banking services—such as better access, convenience, and efficiency this sector is susceptible to cyberattacks. There are more opportunities for cybercriminals to take advantage of due to growing use of digital services like mobile and online banking (O. E. Akinbowale et al., 2020). Accordingly it's important to understand the characteristics and nature of these threats to create efficient defenses to face their effects (Alkhalil et al., 2021).Furthermore hackers have become more proficient and making it difficult for banks to avoid the cyber threats.

2.2 Online Banking Security Trends:

Cybercrimes are one of the biggest risks facing the financial sector, in order to safeguard itself and clients the banking must stay away of the threats as the cybercriminals who coming up with new ways to attack (Z. Barrigar, 2020).

The cyber threats categories as: Linsider threats, DDoS, Advanced Persistent Threats (APTs) and social engineering techniques) presented in Figure 1 (Alshamrani et al., 2019)

.

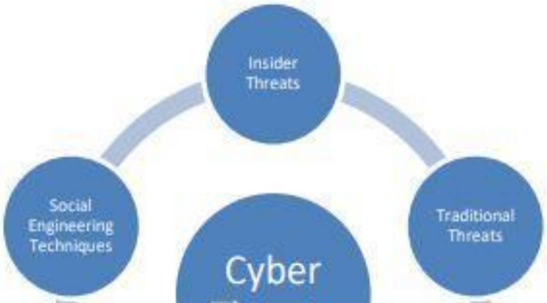

Figure 1Cyber Threats (Alshamrani et al.,2019)

Cybercrimes are now thought to be one of the biggest risks facing the financial industry because of how common they have become. Cyber attackers are always coming up with new ways to attack, and in order to safeguard both itself and its clients, the banking industry needs to stay on top of these continuously changing threats. The finance industry may be seriously affected by cyberattacks, which may result in lost profits, damage to one's reputation, and legalities. For instance, a recent study found that in 2020, the average cost of a data breach was USD 3.86 million (K. Haq, 2018). Nobles (2019) made clear how the financial sector is subject to human error, social engineering, intelligent cybersecurity threats, card fraud, & internet banking scams (C. Nobles, 2019).

According to Jakovljevic' (2022), the banking sector's most remarkable sources of cyber threats are mobile applications and Web portals.

The many security measures have been suggested in order to avoid or reduce these threats (N. Jakovljević, 2022).

The previous studies showed the importance of cybersecurity in the banking sector during digital transformation and highlighted the technological progress of cybercriminals and the financial and reputational risks of data breaches, in addition to human error and forms of fraud, the results showed the needing to invest in the field of cybersecurity to protect financial systems and Addressing various threats.

2.3 Case Studies in Cybersecurity Practices among banking:

Many researches have been conducted to identify and classify cyber attacks in the banking sector and to ensure that banking security is maintained from cyber threats. Dudin & Shkudinsky (2022) studied and analyzed national and international scientific literature and made recommendations for their application in the digital economy environment (M. N. Dudin and S. V. Shkodinsky, 2022). An advanced categorization of risks to bank information resources was presented by (S. Yevseiev et al., 2018). Popular cyberthreats aimed at the banking and finance industries were presented by (A. Tsvetanova and M. Stefanova, 2022) using data from cybersecurity firms and bank reports, Best et al. conducted a comparative study of the most prevalent threats facing the banking industry (M. Best, L. Krumov, and I. Bacivarov, 2019).Nobles focused on the financial sector's to human error, social engineering, cybersecurity threats, credit card fraud and online banking scam (C. Nobles, 2019). Mobile applications and web portals are sources of cyber threats according to Jakovlevy many countermeasures proposed to stop these threats (N. Jakovljević, 2022).

A combination of suggested factors was placed forward by Al-Alawi and Al-Bassam as factors pertaining to cybersecurity awareness in the banking industry (Al-Alawi and Al-Bassam, 2020). Cyber threats were defined in other literature as either internal or external (Chen, D., Zhao, H., Xu, J., Li, Z., & Wang, R. , 2020), or as targeted or non-targeted. Targeted attacks are usually carried out by skilled cybercriminals and are aimed at particular companies or people. Conversely, nontargeted attacks target any weak system and are typically performed by unpracticed attackers using widely available attack tools. Hackers who try to compromise the banking system's security are usually the source of external threats. Contrast, internal threats originate from partners, contractors, or staff members who have been accorded authorized to enter the system (A. Sood and R. Enbody, 2014).

Multiple scholarly works have defined cyber threats affecting the banking industry into multiple categories (F. Salahdine and N. Kaabouch, 2019), including distributed denial of service (DDoS), malware, phishing, and insider threats. One kind of malicious software that aims to compromise a system and cause disruptions is called malware (M. A. Kazi, S. Woodhead, and D. Gan, 2022). Sensitive data, including login details, bank account information, and personal information, can be stolen using malware. Phishing is a kind of attack where users are tricked into divulging sensitive information by sending spammers or by setting up totally fake websites. Social engineering is frequently used in phishing attacks to trick victims into disclosing information. These attacks can be extremely complex and challenging to identify (Z. Zahoor et al., 2016). As seen in figure 2, a few common cyberthreats in the financial industry are ransomware, phishing, data breaches, and DDoS attacks (Dawodu et al., 2023) .

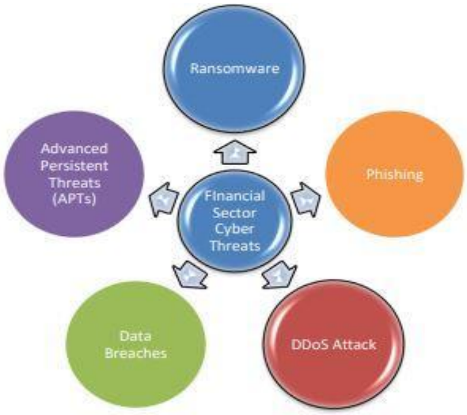
Ransomware
Advanced Persistent Threats (APTs)
Phishing
Financial Sector Cyber Threats
Data Breaches
DDoS Attack

Figure 2Financial Sector Cyber Threats
(Dawodu et al,2023)

"DDoS attacks" aim to interfere with a system's functionality by flooding with traffic. DDoS attacks can be nontargeted affecting any system that is vulnerable or they can be directed towards particular organizations or systems (U. Islam et al., 2022). Insider threats are when partners, contractors, or employees harm their access rights to steal or corrupt data. Essential strategic risks include- malware, trojans, SQL injections, temp folder inclusion, phishing, and cross-site coding (GuardRails, 2022).

As a result, the above mentioned studies indicate the increasing focus on technical security resilience and control and underline the essentiality for regulatory bodies to take a risk-based approach in order to improve banks' cyber-security frameworks. While brought as a whole, these studies explain the numerous components of cyber security in the banking industry and create a detailed view of its current state. And there are areas which need to be to closely examined, especially as it relates to threat classifications and countermeasures, that suggests lots of good opportunities with further research work.

3. The research methodology:

3.1 Methodology*:*

This study employs a mixed-methods approach, incorporating both qualitative and quantitative techniques to comprehensively explore the multifaceted aspects of cybersecurity risk assessment and methodologies within the banking sector.

3.2 Qualitative Component:

The qualitative aspect of the study involves a thorough review of previous studies and scholarly literature related to cybersecurity risk assessment in the banking industry. This review aims to identify key themes, challenges, and best practices documented in existing research.

3.3 Quantitative Component:

The quantitative approach of the study depending on a questionnaire for collecting data from three groups:

- Clients of Online Banking Services
- Cybersecurity and Data Protection Professionals in Banking sector.
- Technological Experts in Artificial Intelligence and Machine Learning

. The questionnaire was distributed to a sample of 150 participants between: 21 to 55 years. This sample includes An equal number of (males and females)followed by the educational level of the participants.

3.4 Data Analysis:

The qualitative data obtained from literature reviews and case studies will be analyzed thematically to identify recurring themes, patterns, and insights relevant to cybersecurity risk assessment in the banking sector.

Quantitative data collected from surveys will be subjected to statistical analysis using appropriate tools and techniques. Descriptive statistics will be employed to summarize survey responses, while inferential statistics may be utilized to identify correlations, trends, and associations between different variables. Statistical analyses will be unfold through SPSS ver.23.

3.5 Integration of Findings:

The qualitative and quantitative findings will be integrated to provide a comprehensive understanding of cybersecurity risk assessment methodologies in the banking sector. This integrated analysis will focus on the recommendations for enhancing cybersecurity practices and reducing the risks among the online banking environments.

Demographic information	Age (years)		
	21-30	31-40	41-55

Clients of Online Banking Services	25	15	10
Cybersecurity and Data Protection Professionals within Banks	25	10	15
Technological Experts in Artificial Intelligence and Machine Learning:	20	15	15
Total	150 participants		

3.6 Survey Questions:

The audience categories and study topics led to the division of the questionnaire into three sections. The questions followed the five Likert axes (Agree, Strongly Agree, Neutral, Disagree, Strongly Disagree):

To what extent do you agree with the following:

Axis 1: The Effectiveness of Cybersecurity Measures in the Banking Sector

1) The banking sector effectively implements cybersecurity measures to protect customer data.
2) I am confident in banks' ability to detect and respond to cyber threats promptly.
3) Continuous monitoring mechanisms in banks contribute significantly to enhancing cybersecurity effectiveness.
4) I am satisfied with the level of transparency banks provide regarding their cybersecurity measures and incident response plans.
5) Technological advancements like AI and machine learning have improved cybersecurity in the banking sector.

Axis 2: Responsibility for Adhering to Online Banking Security Measures

1) I feel responsible as a customer in adhering to online banking security measures to protect my personal and financial information.
2) Customers should actively participate in cybersecurity initiatives to enhance data security in online banking.

3) Banks educate their customers about online banking security measures and best practices adequately. 4) Banks should incentivize customers to adhere to online banking security measures. 5) I am satisfied with the level of support provided by banks in case I encounter security-related issues while using online banking services.
Axis 3: Customer Opinion on Cybersecurity Measures and Their Use
1) I am concerned about the security of my personal and financial information when using online banking services. 2) I frequently update my online banking passwords and other security credentials. 3) The use of advanced technologies like biometrics can enhance the security of online banking transactions. 4) I am satisfied with the overall cybersecurity measures implemented by my online banking provider. 5) I trust online banking platforms to adequately protect my personal and financial information from cyber threats.

4. Results and discussion

1. Percentage of audience responses based on degree of agreement and demographic differences:

The first axis: The effectiveness of cybersecurity measures in the banking sector.

➢ Age group: 21-30:

- This age group shows the highest rate (strongly agree + agree) at 75%. They expressed high level of confidence in cybersecurity measures in the banking sector.
- The neutral rate is low 15%, indicating that most participants in this age group had positive opinion about the effectiveness of cybersecurity.
- The rate of (disagree + strongly disagree) is the lowest at 10% indicating that minority of participants have doubts about the effectiveness of the measures.

- Age group: 31-40:

- The approval rate is high 70% that indicate to the strong belief of the effectiveness of cybersecurity measures.
- The neutral response rate is 15% indicated that this age group don’t have a strong two-way opinion.
- The rate of 15% compared to the 21-30 age group indicates a low level of uncertainty on participants.

- Age Group: 41-55:

- In this older age group the approval rate is 65% indicate a lower level of trust on effectiveness of cybersecurity measures compared to younger age groups.
- The neutral response rate 20% indicate higher level of “hesitation” among this age group.
- The difference rate for the 31-40 age group at 15% indicating a similar level of uncertainty.
- Overall, response rates indicate that younger age groups express higher levels of confidence in the effectiveness of cybersecurity measures in the banking sector than older age groups. However, a large percentage of participants across all age groups still agreed that cybersecurity measures were effective.

The following clustered columns showing the percentage of audience responses based on degree of agreement and demographic differences according to the first Axis (The effectiveness of cybersecurity measures in the banking sector).

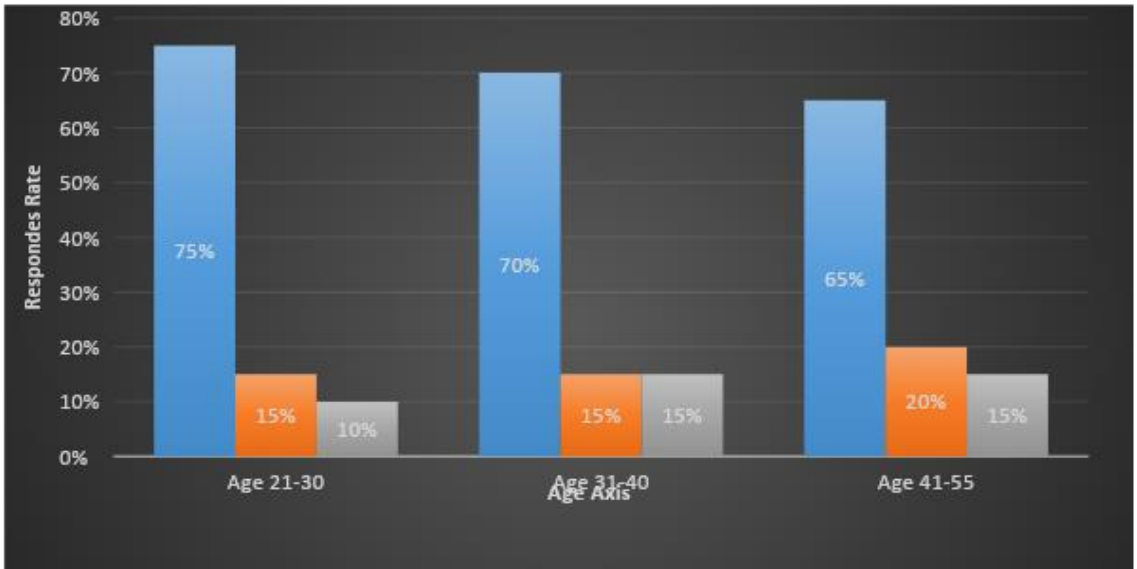

Figure 3: The effectiveness of cybersecurity measures in the banking sector

Axis 2: Responsibility for Adhering to Online Banking Security Measures

- Age group: 21-30 and 31-40:

▪ Those in the age groups of 21–30 and 31–40 exhibit high approval rates of 75%, suggesting a strong sense of accountability for following online banking security protocols.

▪ A 15% neutrality rate suggests that participants are not particularly biased.

▪ The comparatively low variation rate of 10% suggests that a minority lacks a sense of accountability.

- Age group: 41-55:

▪ Compared to the younger age groups, the older group's combined agreement rate is slightly lower at 65%, suggesting a lower level of agreement with a sense of responsibility.

▪ There was a 25% increase in the neutrality rate suggesting that participants were unsure.

▪ At 10%, the joint disagreement rate is still comparable to the younger groups.

Both younger and older age groups express a strong sense of responsibility towards adhering to online banking security measures, according to the response rates. Furthermore, compared to younger age groups there is less agreement among older age groups.

The following clustered columns showing the percentage of audience responses based on degree of agreement and demographic differences according to the second Axis :(Responsibility for Adhering to Online Banking Security Measures)

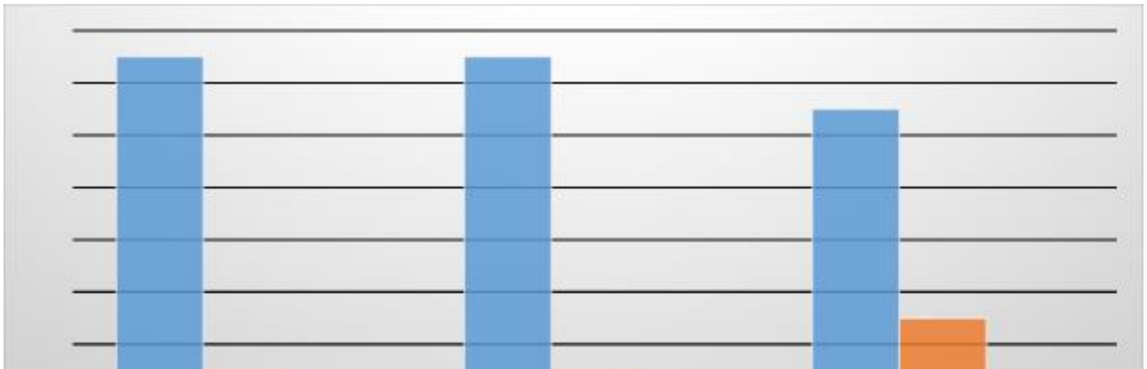

Figure 4: Responsibility for Adhering to Online Banking Security Measures

Third axis: Customer opinion on cybersecurity procedures and their use

- Age group: 21-30 and 31-40:

- The combined high agreement rates of 70% suggest that people have a favorable opinion of the cybersecurity precautions taken in online banking.
- The 20% neutral rate is in line with their unwillingness to respond or ignorance of these procedures.
- A minority expressed disagreement with cybersecurity measures, as indicated by the comparatively low 10% disagreement rate.

- Age range: 41–55:

- Compared to younger age groups, a lower approval rate of 62% signifies a lack of agreement with cybersecurity measures.
- There was a 25% increase in the neutral rate, suggesting a higher degree of uncertainty.
- At 13%, the disagreement rate is comparable to younger age groups.

The majority of the response rates showed both younger and older age groups have positive opinions about cybersecurity precautions among the applications in online banking. However, there is a lower level of agreement among older age groups than younger age.

The following clustered columns showing the percentage of audience responses based on degree of agreement and demographic differences according to the second Axis :(Responsibility for Adhering to Online Banking Security Measures) .

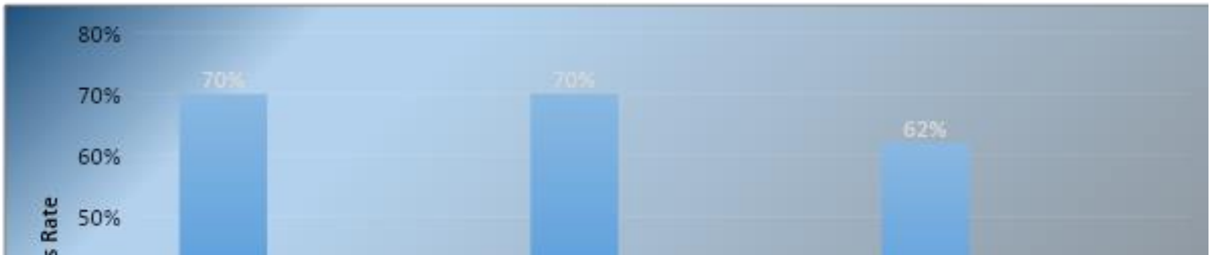

Figure 5: :(Responsibility for Adhering to Online Banking Security Measures)

Table 2: Percentages of audience responses based on the degree of agreement with the questionnaire's axes

Axis	*Percentage of audience responses %*				
	Strongly Agree:	*Agree*	*Neutral*	*Disagree*	*Strongly Disagree*
1.The Effectiveness of Cybersecurity Measures in the Banking Sector	*35*	*40*	*15*	*8*	*2*
2.Responsibility for Adhering to Online Banking Security Measures	*30*	*45*	*15*	*7*	*3*

3.Customer Opinion on Cybersecurity Measures and Their Use	*32*	*38*	*20*	*7*	*3*

4.1 Discussing the research hypothesis:

H 1: The majority of survey participants from all age groups expressed their confidence in the effectiveness of cybersecurity measures in the banking sector.

- The combined approval rate ranged between 65% to 75% and indicated to the understanding of the importance of data protection.
- There are a large percentage of participants who agree that they feel responsible for adhering to the security measures for online banking services. The percentage of agreement was between 70% and 75% and this indicates a feeling of personal responsibility for protecting data.
- *In the first hypothesis we find that these response rates were consistent with the hypothesis: that customers understand their role in cybersecurity and see it as a shared responsibility with the banking sector.

H2: The majority of participants expressed approving opinions regarding cybersecurity procedures and their use in online banking services.

- The approval rates were 70% that indicated to awareness of the importance of technology tools in enhancing security, on the other hand, small percentage of participants showed doubts about the effectiveness of cybersecurity measures with rates between 10% to 13%
- The positive rates indicated that technology tools, such as firewalls, encryption, multi-factor authentication, and intrusion detection systems, play a crucial role in protecting data in the banking sector by preventing unauthorized access, securing sensitive information, and monitoring for potential threats.
- These response rates confirm the hypothesis that technology tools, including software and systems designed to protect data, are essential for implementing effective cybersecurity measures in the banking sector.

Overall the response rates confirm the validity of the two research hypotheses indicating the shared responsibility between customers and the banking sector in protecting data and the important role of technology tools in enhancing cybersecurity.

4.2 Conclusion:

This research explored various cybersecurity risks in the banking industry, drawing insights from case studies on different types of risks and threats. Through this analysis, we developed a thorough understanding of the cybersecurity landscape. The objective was to address the needs of external customers, business owners, and internal stakeholders in the banking sector. The study concludes with recommendations for implementing effective cybersecurity strategies tailored to meet the requirements of all stakeholders, ensuring enhanced protection against cyber threats.

4.3 Recommendations:

- Release campaigns to notify staff as well as the clients about cyber threats. Communication and collaboration for both authorities banks sharing of knowledge.
- Going to invest in data security measures through employing skilled to check up on possible attacks.
- Reported greater security audits to discover the weaknesses in defenses.
- Keeping customers informed on updates of the cybersecurity practices.

5. References

A. Sood and R. Enbody. (2014). *Targeted Cyber Attacks: Multi-Staged Attacks Driven by Exploits and Malware*. Rockland, MA, USA: Syngress Media.

Al-Alawi and Al-Bassam. (2020). *‘‘The significance of cybersecurity system in helping managing risk in banking and financial sector* (Vol. 14). J. Xidian Univ.

A. Tsvetanova and M. Stefanova. (2022). *Key cybersecurity threats* (Vols. 5, no. 1, pp. 32–38). Math.,Comput. Sci. Educ.

Abdulla & Al-Hassani. (2022). *Consumer use of E-Banking in Iraq: security breaches and offered solution*. Iraqi Journal of Science. doi:https://doi.org/10.24996/ijs.2022.63.8.40

Alkhalil et al. (2021). *Phishing attacks: A recent comprehensive study and a new anatomy* (Vols. 3, Art. no. 563060). Frontiers Comput. Sci.

Alothaim et al. (2022). *Analysis of Cybersecurities within Industrial Control Systems Using Interval-Valued Complex Spherical Fuzzy Information*. Computational Intelligence and Neuroscience, 2022, 1–28. doi:https://doi.org/10.1155/2022/3304333

Alshamrani et al. (2019). *A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities* (Vols. 21(2), 1851-1877.). IEEE Communications Surveys & Tutorials.

C. Nobles. (2019). *Disrupting the U.S. national security through financial cyber crimes* (Vols. 3, no. 1). Int. J. Hyperconnectivity Internet Things.

Chen, D., Zhao, H., Xu, J., Li, Z., & Wang, R. . (2020). *Security and privacy issues in cloud-based government services: A survey*. Computers & Security, 96, 101993. doi: https://doi.org/10.1016/j.cose.2020.101993

Darem et al. (2023). *Cyber Threats Classifications and Countermeasures in Banking and Financial Sector*. IEEE Access. doi:https://doi.org/10.1109/ACCESS.2023.3327016

Dawodu et al. (2023). *CYBERSECURITY RISK ASSESSMENT IN BANKING: METHODOLOGIES AND BEST PRACTICES*. Computer Science & IT Research Journal. doi:https://doi.org/10.51594/csitrj.v4i3.659.

F. Salahdine and N. Kaabouch. (2019). *Social engineering attacks: A survey* (Vols. 11, no. 4). Future Internet.

Faria & Çipi. (2020). *A CONSTRUCTIVIST MODEL OF BANK BRANCH FRONT-OFFICE EMPLOYEE EVALUATION: AN FCM-SD-BASED APPROACH*. Technological and Economic Development of Economy. doi:https://doi.org/10.3846/tede.2020.11883

GuardRails. (2022). *The Top 10 Cybersecurity Threats to Digital*. Banking and how to Guard Against Them. Retrieved from https://www.guardrails.io/blog/the-top-ten-cyber-security-threats-to-digital-banking-and-how-to-guard-against-them/

K. Haq. (2018). *What is Cybersecurity? New York, NY, USA: Rosen Education Service*. Britannica Educational Publishing.

M. A. Kazi, S. Woodhead, and D. Gan. (2022). *An investigation to detect banking malware network communication traffic using machine learn ing techniques* (Vols. 3, no. 1). J. Cybersecurity Privacy.

M. Best, L. Krumov, and I. Bacivarov. (2019). *Cyber security in banking sector* (Vols. 8, no. 2). Int. J. Inf. Secur. Cybercrime.

M. N. Dudin and S. V. Shkodinsky. (2022). *Challenges and threats of the digital economy to the sustainability of the national banking system* (Vols. 26, no. 6, pp. 52–71). Theory Pract.

Mishra, A., & Rajwani, P. (2020). *A Study Of Bank Customer Experience In Relation To Technology Innovation In Banking.* Journal of Cryptology. doi:https://doi.org/10.51767/JOC1203

Mousa et al. (2021). *Determinants of customer acceptance of e-banking in Iraq using technology acceptance model.* (Vol. 2). Telkomnika, 19. doi:https://doi.org/10.12928/telkomnika.v19i2.16068

N. Jakovljević. (2022). *Analysis of cyber threats as a risk factor in the banking sector* (Vols. 51, nos. 3–4). Bankarstvo.

O. E. Akinbowale et al. (2020). *Analysis of cyber-crime effects on the banking sector using the balanced score card A survey of literature* (Vols. 27, no. 3, pp. 945–958). J. Financial Crime.

Pathan, A. (2022). *On the scale of Cyberspace and Cybersecurity.* International Journal of Computers and Applications.

S. Yevseiev et al. (2018). *Classification of cyber cruise of informational resources of automated banking systems* (Vols. 2, no. 2). Cybersecurity, Educ., Sci.Technique.

Schlesinger Rudolf B. (1957). , *Research on the General Principles of Law Recognized by Civilized Nations 51 A.J.I.L.*

U. Islam et al. (2022). *Detection of distributed denial of service (DDoS) attacks in IoT based monitoring system of banking sector using machine learning models* (Vols. 14, no. 14). Sustainability.

Z. Barrigar. (2020). *Examining the current threat of cybercrime in mobile banking and what can be done to combat it.* Utica, NY, USA: '' Ph.D. dissertation, Dept Cybersecurity, Utica College, Utica Univ.

Z. Zahoor et al. (2016). *Challenges in privacy and security in banking sector and related countermeasures* (Vols. 144, no. 3, pp. 24–35). Int. J. Comput.Appl.

Семеняк, А. (2021). *Проблемы устойчивого функционирования банковского сектора РТ.* Landscape Journal. doi:https://doi.org/10.18411/LJ-02-2021-95