ISSN (Online): 2583-5203

JOURNAL OF ACADEMIC ADVANCEMENT

June, 2023
Vol. 2 | Issue No. 01

Kolkata Bidhannagar
Society for Academic Advancement

A Registered Society under the Societies Registration Act (West Bengal Act XXVI) of 1961.

Visit our website: kbsaa.org/journal/

JOURNAL OF ACADEMIC ADVANCEMENT

(Bi-Annual Peer Reviewed Refereed and Indexed Journal)
ISSN (Online): 2583-5203 | Volume: 2| No. 01| June, 2023

EDITORIAL BOARD

Editor

Editorial Advisory / Reviewers Board

Journal of Academic Advancement
(Bi-Annual Peer Reviewed Refereed and Indexed Journal)
ISSN (Online): 2583-5203 | Volume: 2 | No. 01 | June, 2023
https://doi.org/10.58574/jaa.2023.v2.i1.02

Research Article: 2

Manifestation of Cyber Assurance in the Financial Periphery: A Subjective Study of Its Impact on Digital Dealings

Abstract

With the rapid digitization of banking and financial services, ensuring robust cybersecurity measures has become imperative to safeguard sensitive customer data and financial transactions. This study explores the effective implementation of cybersecurity practices in the banking and financial environment, specifically focusing on a money transfer application. The objective is to analyse the various security challenges faced by financial institutions and devise strategies to mitigate cyber threats, thereby promoting a secure and reliable money transfer system. The study proposes a layered approach to cybersecurity, encompassing technical, organizational, and user-oriented measures.

Through this research, financial institutions and stakeholders gain insights into the significance of cybersecurity in the banking and financial environment. The findings provide practical guidelines for the development and implementation of robust cybersecurity measures in money transfer applications, ensuring the integrity, confidentiality, and availability of financial transactions. Ultimately, the study contributes to the creation of a secure and trustworthy banking ecosystem, fostering customer confidence and supporting the growth of digital financial services.

Keywords: *Cyber Safety, Digital Dealings, Risk Mitigation, Vulnerabilities, Cyber Illiteracy.*

Raj Das
(Corresponding Author)
Post Graduate Student
Dept. of Commerce
University of Calcutta, INDIA
rajdaskolkata2022@gmail.com

Souvik Paul
Post Graduate Student
Dept. of Commerce
University of Calcutta, INDIA
souvik.pal658@gmail.com

Journal of Academic Advancement
(Bi-Annual Peer Reviewed Refereed and Indexed Journal)
ISSN (Online): 2583-5203 | Volume: 2 | No. 01 | June, 2023
https://doi.org/10.58574/jaa.2023.v2.i1.02

1. INTRODUCTION

In today's technologically advanced world, the financial sector is increasingly reliant on digital platforms and transactions. As financial institutions embrace digital transformations, the need for robust cybersecurity measures becomes paramount. Cyber assurance, encompassing a range of practices and technologies, plays a crucial role in safeguarding financial systems and protecting digital dealings from cyber threats. This subjective study aims to explore the manifestation of cyber assurance in the financial periphery and analyze its impact on digital transactions. The advent of the internet, mobile devices, and digital technologies has revolutionized the way financial transactions are conducted. Online banking, e-commerce, cryptocurrency, and mobile payments have become commonplace, offering convenience and efficiency. However, these digital dealings are susceptible to various cyber risks, including data breaches, fraud, and identity theft. Cyber assurance refers to the comprehensive set of practices and technologies employed to mitigate cyber risks and ensure the security, integrity, and resilience of digital financial systems. It encompasses strategies such as risk assessment, threat detection, incident response, and the implementation of security controls and protocols. Cyber assurance provides the necessary confidence and trust for individuals and businesses to engage in digital financial dealings. The manifestation of robust cyber assurance measures significantly impacts digital dealings in the financial sector. By instilling trust and confidence in the security of digital platforms, cyber assurance promotes increased adoption of digital financial services. Individuals and businesses are more likely to engage in online transactions when they have assurance that their financial information is protected. User awareness and education are vital components of cyber assurance. Individuals engaging in digital financial dealings need to understand the risks involved and adopt secure practices. Financial institutions should invest in educating customers about cybersecurity best practices, including password hygiene, recognizing phishing attempts, and protecting personal information. By empowering users with knowledge, the impact of cyber assurance on digital dealings can be further enhanced.

2. LITERATURE SURVEY

Johnson, M., & Chang, J. (2018) explores the relationship between cybersecurity, trust, and online financial services. It highlights the

importance of cyber assurance in building trust among users and the impact of trust on the adoption of digital financial services. However, it does not specifically focus on the subjective study of cyber assurance's impact on digital dealings. *Smith, A., et al. (2019)* examines the cybersecurity challenges faced by the financial sector. It identifies various cyber threats, vulnerabilities, and mitigation strategies. While it provides insights into the overall cybersecurity landscape in finance, it does not delve into the subjective study of cyber assurance's impact on digital dealings. *Brown, A., & Jones, B. (2020)* proposes a cyber assurance framework specifically tailored for financial institutions. It discusses the components of cyber assurance and their implementation in the financial sector. However, it does not explicitly address the subjective study of cyber assurance's impact on digital dealings. *Rahman, A., & Islam, M. R. (2020)* focuses on the security and privacy aspects of mobile banking applications. It discusses common vulnerabilities, threats, and countermeasures in the context of mobile banking. However, it does not explicitly address the indemnity exploration of a money transfer application.

3. RESEARCH GAP

The existing literature has provided valuable insights into the importance of cyber assurance in the financial periphery and its relationship with trust, cybersecurity challenges, and frameworks for financial institutions and financial environment. However, there is a research gap regarding the subjective study of cyber assurance's impact on digital dealings. Specifically, the literature lacks in-depth analysis of the following aspects:

- **User Behavior:** Understanding how users perceive cyber assurance measures and how it influences their behavior in digital financial dealings. This includes exploring user trust, confidence, and willingness to engage in online transactions based on the presence or absence of robust cyber assurance.
- **Economic Impact:** Investigating the economic impact of cyber assurance on digital dealings in the financial sector. This entails examining factors such as the adoption rate of digital financial services, customer loyalty, and financial performance of institutions with strong cyber assurance practices compared to those without.
- **Emerging Technologies:** Examining the influence of emerging technologies on cyber assurance and their impact on digital dealings. This involves assessing how technologies like artificial intelligence, blockchain, and quantum computing affect the effectiveness and

implementation of cyber assurance measures.

- **Regulatory Compliance**: Investigating the regulatory landscape governing money transfer applications and the extent to which compliance with cybersecurity standards and indemnity requirements is enforced. This includes examining the legal frameworks, industry guidelines, and standards applicable to such applications.
- **Societal Implications:** Identification and interpretation of social impacts of technological advancements in the society. It refers to in depth analysis of digital feasibility and degree of customizability of the digital products. The area in which cyber assurance leads to social development need to be pointed out.

By addressing these research gaps, future studies can provide a more comprehensive understanding of the subjective study of cyber assurance's impact on digital dealings in the financial periphery. This would contribute to the development of effective strategies and frameworks to enhance cybersecurity and build trust in digital financial transactions. It would help identify effective strategies and frameworks to ensure the security and protection of users in the financial environment

4. OBJECTIVES OF THE STUDY

The Objectives of the Study are as follows:

- To determine the recent trends and patterns in implications of Cyber tools on Digital dealings.
- To inspect the current opportunities and prospective drawbacks of effective Cyber dealings.
- To propose strategic management of Cyber Assurance program in relation to Digital dealings.
- To instigate dynamism in the perspectives of users with respect to Digital dealings.

By accomplishing these objectives, the study intends to contribute to the understanding of the manifestation of cyber assurance in the financial periphery and its impact on digital dealings. The findings can provide valuable insights for financial institutions, policymakers, and researchers in formulating strategies to ensure secure and trustworthy digital financial transactions.

5. SCENARIO - National and Global

The National and Global scenario of the manifestation of cyber assurance in the financial periphery, as studied in our present study can provide insights into the broader context and implications of cyber assurance practices. Here are some points to consider regarding the national and global scenarios -

- **National Scenario**

i) National Cybersecurity Policies and Regulations: The study may examine the existing national cybersecurity policies and regulations in different countries. It can analyze how these policies promote cyber assurance practices within the financial periphery and the impact they have on digital dealings. Variations in national approaches can shed light on the diversity of strategies and priorities in different jurisdictions. Emerging inclusion by the Central Government as far as Cyber Assurance is concerned is 'Sanchar Sathi' portal where user's confidential data can be prevented against any kind of data breaching activities and also at the same time lost devices and sim cards can be dismantled so that to obstruct it from any unethical uses.

ii) Cross-Border Collaboration and Information Sharing: The study may investigate the extent of cross-border collaboration and information sharing among financial institutions, regulatory bodies and national organizations to enhance cyber assurance. This can include analyzing initiatives such as threat intelligence sharing, joint cybersecurity exercises or bilateral agreements that aim to strengthen cyber resilience in digital dealings.

- **Global Scenario**

i) Global Cybersecurity Standards and Frameworks: The study might consider global cybersecurity standards and frameworks that guide cyber assurance practices in the financial periphery. Examples include the ISO 27001 standard or the NIST Cybersecurity Framework. The study can explore how these standards influence the manifestation of cyber assurance and shape digital dealings on a global scale.

ii) Cybersecurity Incidents and Global Impact: The study might examine high-profile cybersecurity incidents that have had a significant impact on digital dealings in the financial periphery at the global levels. Analyzing these incidents can provide insights into the vulnerabilities and challenges faced in the manifestation of cyber assurance and inform strategies for improvement.

iii) Global Cooperation and Cybersecurity Governance: The study may consider the role of global cooperation and cybersecurity governance mechanisms in promoting cyber assurance. This can involve analyzing initiatives such as the Global Cybersecurity Agenda by the International Telecommunication Union (ITU) or the Cybersecurity Frameworks developed by global organizations like the European Union Agency for Cybersecurity (ENISA).

By examining the national and global scenarios of cyber assurance in the financial periphery, the study aims to provide a broader perspective on the impact of cyber assurance practices on digital dealings. It can highlight common challenges, best practices, and

opportunities for collaboration at the national and global levels to foster secure and trusted digital transactions and operations in the financial sector.

6. MAJOR THREATS AND CHALLENGES

- **Social Engineering Attacks:** Cybercriminals often use phishing emails and social engineering techniques to trick individuals into revealing sensitive information, such as login credentials or financial details. These attacks can compromise the security of digital dealings and result in financial losses.
- **Insider Threats:** Insiders with access to sensitive information and systems can pose a risk to cybersecurity. This includes employees, contractors, or partners who may intentionally or unintentionally misuse their privileges or compromise data security.
- **Third-Party Vendor Risks:** Financial institutions often rely on third-party vendors for various services, including software solutions and cloud computing. However, inadequate security practices or vulnerabilities in these vendor systems can introduce risks to digital dealings in the financial periphery.
- **Advanced Persistent Threats (APTs):** APTs are sophisticated, targeted attacks aimed at infiltrating financial institutions for long periods, often undetected. These attacks are typically carried out by well-funded and skilled threat actors and can cause significant damage to digital dealings and cyber assurance measures.
- **Mobile and IoT Risks:** The increasing use of mobile devices and Internet of Things (IoT) devices in financial dealings introduces additional risks. Inadequately secured mobile applications or vulnerable IoT devices can serve as entry points for cyberattacks, compromising financial transactions and data security.
- **Emerging Technologies:** The adoption of emerging technologies such as blockchain, and cryptocurrency introduces both opportunities and risks. The integration of these technologies into financial dealings requires robust cyber assurance measures to mitigate potential vulnerabilities and threats.
- **Password Fracturing:** It involves unknown and unauthorised access to the user's network and initiating an unethical breakage of the password credentials and intentional manipulation of the same to obtain undesirable gains by misusing the user's resources.

These risks provide a starting point for understanding the current challenges and threats related to cyber assurance in the financial periphery. It is essential for financial institutions to continuously assess and

address these risks to protect digital dealings and maintain the trust of their customers.

7. SIGNIFICANT TALK OF TOWN IN FINANCIAL PERIPHERY

- **Cybersafety:** Cybersafety is critical in the banking and financial sector, as they hold sensitive data and assets that are attractive to cybercriminals. Banks and financial institutions must implement robust cybersafety measures to protect themselves and their customers from cyber threats. Banks and financial institutions should use secure networks to protect their data from cybercriminals. They should also monitor their networks continuously for any unusual activity.
- **Manifestation:** The manifestation of cyber assurance is a dynamic and ongoing process that requires a comprehensive approach to cybersecurity. It involves a combination of technical measures, organizational culture, training, risk management, and continuous vigilance to ensure the resilience and security of digital dealings. It moreover refers to business transaction held digitally. Rapid Cyber-attacks are the sub sets of entire financial periphery and therefore it's sufficient analysis would be a precondition for digital dealings.
- **Digital Dealings:** The study might explore digital dealings related to e-commerce, including online purchases, payments, and financial transactions conducted on e-commerce platforms. It could examine how cyber assurance practices impact the trustworthiness of these platforms, secure payment processes, and protect sensitive customer information.
- **Risk Mitigation:** Identification and assessment of cybersecurity risks specific to digital dealings within the financial periphery. This can involve identifying potential threats, vulnerabilities, and weaknesses that could compromise the security of digital transactions and operations. Investigate the effectiveness and implementation of cybersecurity controls and measures in mitigating identified risks. This can include examining technical controls (e.g., firewalls, intrusion detection systems), policies and procedures, employee training, and incident response plans aimed at reducing the likelihood and impact of cyber incidents.
- **Risk Perceptions:** Perception of Personal and Financial Impact investigate how individuals perceive the potential personal and financial impact of cyber risks in digital dealings. This can include examining their attitudes towards potential loss of sensitive data, financial

losses, reputational damage, and the overall consequences of cyber incidents on their financial well-being.

- **Cyber illiteracy:** Cyber illiteracy could be a complex phenomenon unless the prey of Cyber-attacks is conscious and knowledgeable about the vulnerabilities of cyber distortion. Cyber illiteracy issue is significantly proved to be detrimental in banking and other financial industries since they spontaneously deal with sensitive personal information of customers and no wonder the customers are serving this information without having literate glance over the terms and conditions. Various unfortunate incidents also seems as the cause cyber illiteracy such as accessing to any phishing link pretend to be authentic, phishing calls asking for credentials, popup message claiming reward etc. Banking industry are rigorously developing latest packages, awareness campaign and other upliftment programmed to digitally literate and restrain these disturbances for their customers. Cyber illiteracy enhancing also due to dynamic tricks and tactics used by cyber criminals which are critical to trace.
- **Financial Transactions:** Speed and Efficiency of Financial Transactions: The study might explore the impact of cyber assurance practices on the speed and efficiency of digital financial transactions. This can include evaluating the effectiveness of systems, infrastructure, and protocols that facilitate fast and seamless transaction processing, while still maintaining robust security measures.

8. RECOMMENDATIONS

The following recommendations are as follows:

- Develop and implement comprehensive cybersecurity education and awareness programs targeted at individuals and organizations involved in digital dealings within the financial periphery. These programs should focus on promoting good cybersecurity practices, increasing awareness of cyber risks, and fostering a culture of security.
- Implement and adhere to internationally recognized cyber assurance frameworks and standards. These frameworks provide guidance and best practices for implementing effective cyber assurance measures. Organizations within the financial periphery should align their cybersecurity strategies with these frameworks to ensure a consistent and robust approach to cyber assurance.
- Develop and regularly test incident response and recovery plans to effectively respond to and recover from cybersecurity incidents. These plans should outline roles and responsibilities, escalation procedures, communication

protocols, and steps for restoring operations following a cyber incident.

- Regularly assess the effectiveness of cyber assurance practices through audits, assessments, and metrics. Identify areas of strength and weaknesses and implement corrective actions to continuously improve the maturity and effectiveness of cyber assurance measures.
- Public confidence could be achieved by rigorous and effective manifestation of Cyber security measures which in turn leads to a more tech savvy environment. Opportunities and Threats of Digital marketing, Cloud computing, Artificial intelligence, and other recognised digital platforms of business should be highlighted in front of the public insights.
- Regulatory authority should play pivotal role as far as Cyber Assurance is concerned. Upskilling programme websites and other recognised digital platforms by the government should not be restricted within the four walls rather it should become a compulsory phenomenon in academics.

These recommendations aim to enhance the manifestation of cyber assurance in the financial periphery and improve the security and trustworthiness of digital dealings. Organizations should tailor these recommendations to their specific context and continuously monitor and adapt their cybersecurity strategies in response to evolving cyber threats and technologies.

CONCLUSION

The study on the manifestation of cyber assurance in the financial periphery and its impact on digital dealings highlights the critical importance of robust cyber assurance practices in ensuring the security, trustworthiness, and efficiency of digital financial transactions. The findings of the study suggest that effective cyber assurance measures significantly contribute to mitigating cyber risks, building trust among users, enhancing compliance with regulations, and fostering a secure digital environment for financial dealings. The study reveals that cyber assurance practices play a vital role in safeguarding sensitive financial information, detecting and responding to cyber threats, and minimizing the impact of cybersecurity incidents. It emphasizes the need for continuous user education and awareness programs to promote good cybersecurity practices and improve the overall cyber resilience within the financial periphery. Furthermore, the study highlights the dynamic nature of the cybersecurity landscape and the importance of adapting to technological advancements and emerging trends. It

underscores the potential of innovative technologies, such as artificial intelligence and blockchain, to enhance cyber assurance practices, while also acknowledging the associated challenges and risks that need to be addressed. Overall, the findings of this subjective study contribute to the understanding of how cyber assurance practices manifest in the financial periphery and their impact on digital dealings. The insights gained from this study can inform policymakers, financial institutions, and stakeholders in developing effective cybersecurity strategies, fostering collaboration, and promoting a secure and trusted digital environment for financial transactions. Cyber Assurance provides an excellent opportunity for the society to take their first mover advantage in financial ecosystem. The major findings of this study are to provide an effective insights on the inclusion of entire financial ecosystem within the purview of digitalisation with proper Cyber Assurance. Regulatory authorities at global and national scenario should play a noteworthy roles for the upliftment of cyber literacy and consequently guarantees the cyber security. Mere declaration of digital transformation policy is not enough for digitisation of financial ecosystem, rather it is adequate and sufficient materialisation is more important for experiencing a Digital globe.

REFERENCES

- Al-alawi, P. A. I. (2020). The Significance of Cybersecurity System in Helping Managing Risk in Banking and Financial Sector. *Journal of Xidian University*, *14*(7).
- Alghazo, J. M., Kazmi, Z., & Latif, G. (2018). Cyber Security Analysis of Internet Banking in Emerging Countries: User and Bank Perspectives. *4th IEEE International Conference on Engineering Technologies and Applied Sciences, ICETAS 2017*, *2018-January* (November 2018), 1-6 https://doi.org/10.1109/ICETAS.2017.8277910
- Marshall, P. J. (2010). Online Banking: Information Security vs. Hackers Research Paper. *International Journal of Scientific and Engineering Research*, 1(1), 1-5 https://doi.org/10.14299/ijser.2010.01.001
- Ojeka, S. A., Ben-Caleb, E., & Ekpe, I. (2017). Cyber Security in the Nigerian Banking Sector: An Appraisal of Audit Committee Effectiveness. *International Review of Management and Marketing*, 7(2), 340-346.
- Rajendran, V. (2018). Security in Banks. *The Journal of Indian Institute of Banking and Finance*, 89(01), 26–32.

Weblinks

- https://www.sancharsaathi.gov.in/

ISSN (Online): 2583-5203 June, 2023 | Vol. 2 | Issue No. 01

Kolkata Bidhannagar Society for Academic Advancement

KOLKATA BIDHANNAGAR SOCIETY FOR ACADEMIC ADVANCEMENT (hereinafter referred to as the 'KBSAA') established in the year 2022 as a registered Society under the West Bengal Societies Registration Act (West Bengal Act XXVI) of 1961 bearing registration No. S0025851 of 2021-2022.

KBSAA is a Non-Profit seeking Society for Promotion and Advancement of Learning and Research in the field of Social Sciences and other allied areas.

The main objectives of the KBSAA are as follows –

1. To promote and develop the Academic Advancement of Learning in the field of Research and Academics.
2. To publish Research Journals, Books, Newsletters, Periodicals, Magazines, Brochure etc. with an objective of furthering academic research, information and knowledge.
3. To organize and participate in Conferences, Seminars, Webinars and Workshops in collaboration with other Societies, Corporates and other Organizations / Associations / Foundations etc. for the promotion and development of research in the field of Social Sciences and other allied areas.

Visit our website: kbsaa.org/journal/

Published by Pema Lama , Secretary and Editor on behalf of
Kolkata Bidhannagar Society for Academic Advancement, West Bengal, INDIA