Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume: 1 Issue: 2
February 2026
Impact Factor: 11.9
Subject: Management

EVALUATING CYBERSECURITY RISK AND ITS IMPLICATIONS FOR RISK MANAGEMENT IN MODERN BANKING SYSTEMS

Sukumarn Nair. B
Research Scholar,
Sanskriti University &
Dr. Pradeep Meghwal
Assistant Professor
Sanskriti University

ABSTRACT

The fast digitalization of banking services has made becoming vulnerable to cybersecurity threats a serious issue, and efficient risk management is now the priority of the new banking system. The paper will assess the assessment of key cybersecurity threats, assess the operational and financial effects of cyber attacks and the effectiveness of currently in place practices of cybersecurity risk management in banks. Primary data were gathered with the help of the descriptive and analytical research design based on the structured questionnaire that was distributed among the banking professionals and analyzed with the help of the percentage-based descriptive statistics. The results indicate that the most common cybersecurity threats are phishing and social engineering attacks, malware and ransomware, and data breaches, which result in massive financial losses, interference with operations, and reputational losses. Even though banks are majorly dependent on technical controls like firewalls and intrusion detection systems, there exist gaps in incident responds planning and third-party risk management. It is concluded in the study that cybersecurity risk is a strategic enterprise-wide matter and that it should be incorporated into the enterprise and through a combination of governance, increased employee awareness, solid response, and additional control over external partners, resilience and sustainability in an ever-more digital banking landscape can be achieved.

Keywords: *Cybersecurity Risk, Banking Systems, Risk Management, Phishing Attacks, Operational Risk, Financial Losses.*

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume: 1 Issue: 2
February 2026
Impact Factor: 11.9
Subject: Management

1. INTRODUCTION

The unprecedented digitalization of banking systems has created a profound efficiency, accessibility, and convenience factor in terms of online banking, mobile apps, cloud computing, and fintech integrations. Yet, this growing use of digital technologies has made banking institutions vulnerable to a broad extent of cybersecurity threats as well. Phishing, malware, ransomware, and data breaches are more common and advanced types of cyber threats that are arduously challenging the confidentiality, integrity, and availability of sensitive financial data. Cybersecurity has become an issue of concern with direct implications in financial stability and trust with banks as they handle enormous amounts of transactional and personal data.

Risk of cybersecurity in contemporary banking is not only technical interference but it is also loss of money, disruption of operations, damage to reputation and non-conformity to regulation. The impact of cyber incidents might be direct financial damages through fraud and recovery expenses, as well as the loss of customer trust and legal or regulatory fines. Thus, cybersecurity is not considered as just an information technology problem, but it is a strategic risk that has to be included in the overall enterprise risk management strategies. Risk management in the banking is therefore required not only to control the technological risks, but also human factors, the governance structure, and dependencies on third parties.

In this regard, the measurement of cybersecurity risk and its future impact on risk management has become a critical aspect in the assurance of resiliency and sustainability of the contemporary banking systems. Knowledge of the level of cyber threats, the level of operational and financial losses, and the efficiency of current risk management approaches may assist the banks in determining the gaps in preparedness and in enhancing the defensive strategies to eliminate the threat. The current research aims to offer the empirical evidence on cybersecurity threats that banking institutions experience and present the necessity to implement the holistic, proactive, and integrated approach to cybersecurity risk management in increasingly digitalizing banking environment.

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume: 1 Issue: 2
February 2026
Impact Factor: 11.9
Subject: Management

2. LITERATURE REVIEW

Al-Alawi and Al-Bassam (2020) investigated the application of the cybersecurity systems to the risk management in the banking and financial industry. Their research highlighted that effective cybersecurity systems had been important in mitigating operational and financial risk by cyberattacks. The authors also discovered that well-developed cybersecurity mechanisms increased the security of data, guaranteed the continuity of services, and facilitated the compliance with the rules, which improved the overall risk management activities within banking institutions. The analysis has found that cybersecurity became an unavoidable part of enterprise risk management instead of a technical protection.

Al-Alawi and Al-Bassam (2019) explored how cybersecurity awareness can be affected in the banking industry. Their results showed that organizational culture, training programs, and employee awareness had impacted greatly on the efficiency of cybersecurity measures. The analysis noted that although there are high-technological controls in place, low awareness rates among the banking personnel made them susceptible to phishing and social engineering attacks. The authors pointed out a proper role of constant training and management backing in cultivating a robust cybersecurity-conscious background among banks.

Alkhdour, AlWadi, and Alrawad (2024) evaluated the cybersecurity threats and risks on banking and financial services. Their study was able to note phishing, malware, ransomware and data breaches as the most important threats to the current financial institutions. The paper also observed that the rising level of digitalization and dependence on the internet had increased the rate and seriousness of cyber-attacks. The authors came to a conclusion that currently available risk mitigation strategies were frequently inadequate and suggested a more coordinated approach to risk management of cybersecurity issues involving a combination of technical controls, governance, and proactive incident response planning.

Azura, Azad, and Ahmed (2025) presented a unified system of cybersecurity risks management of online banking in particular. They highlighted the fact that silo-based and traditional security strategies were insufficient in mitigating the emerging and dynamic cyber threat environment of digital banking platforms. The authors proved the concept that the coordination of risk

ISSN: 2320-3714
Volume: 1 Issue: 2
February 2026
Impact Factor: 11.9
Subject: Management

identification, assessment, mitigation, and the ongoing monitoring into a single framework was the key to enhancing the capability of banks to predict and react to the cyber threats. These results indicated the need to harmonize cybersecurity risk management and organizational governance framework and strategic goals to improve the overall resiliency of online banking systems.

Berdyugin and Revenkov (2019) analyzed different methodologies of quantifying risks of cyberattacks on remote banking in Russia. Their study centered on the quantitative risk assessment techniques, such as the probabilistic models and the threat impact evaluation techniques, to estimate possible losses related to cyber incidents. This paper identified that precise quantification of cyber risks had been critical in informed decision-making and proper security resources allocation. The authors found that the absence of standardized risk measurement tools had constrained the capacity of banks to manage the cybersecurity risks in an effective manner, and thus they urged that more structured and data-driven assessment models in remote and digital banking spaces are created.

3. RESEARCH METHODOLOGY

The research design used was descriptive and analytical research design and the primary research data was collected and gathered using a structured questionnaire that is administered to banking professionals who were selected using purposive sampling technique. The analysis of data was conducted based on the percentage-based data description and presented in the form of tables and graphs to evaluate cybersecurity threats, their effects, and how well current risk management practice is implemented in contemporary banking systems.

3.1 Research Design

The research design that is followed in the study is descriptive and analytical research design to measure cybersecurity risks and their implications towards management of risks in a modern banking system. Such a design is suitable because it will allow conducting a logical analysis of common cybersecurity threats, the impact of their operation, and the usefulness of established risk management practices in the quantitative terms.

3.2 Population and Sample

ISSN: 2320-3714
Volume: 1 Issue: 2
February 2026
Impact Factor: 11.9
Subject: Management

The study target population is banking institutions that are already in the digital and technology-driven environment, which will be composed of both public sector banks, banks in the private sector, as well as selected financial institutions providing online and mobile banking services. The method applied in the sample was purposive sampling to select respondents who possess relevant knowledge and experience in the area of cybersecurity and management of risk. It was a sample comprising of IT managers, risk management officers, cybersecurity professionals, and senior operational staff of the chosen banks.

3.3 Data Collection Method

The research is premised on primary data, which will be gathered with the help of a structured questionnaire that will evaluate cybersecurity threats, operational impacts, and risk management practices. This questionnaire was composed of closed questions whose response was measured based on a percentage scale. To complement the main findings and give them a context, secondary data were also referred to published research articles, regulatory reports, banking guidelines, and cybersecurity frameworks.

3.4 Data Analysis Techniques

The obtained data were processed with the help of descriptive statistical tools, mostly with the percentage analysis, in order to identify distribution and comparative significance of cybersecurity threats, cybersecurity effects, and cybersecurity management practices. The findings have been presented in a tabular and graphical format to make it more clear and easier to interpret. The relevance of this approach to the aim of determining the prevalent risk factors and evaluating the current level of cybersecurity preparedness in the banking system lies here.

4. RESULT

The findings indicate that phishing, malware, and financial losses present the highest cybersecurity risks to the contemporary banking systems, where human-related and economic impacts prevail as the general risk exposure. Although the technical and preventive controls are important to banks, and there are potential loopholes in incident response and third-party risk management, a more integrated and strategic approach to cybersecurity risk management is necessary.

Airo International Journal
Peer-Reviewed
Multidisciplinary

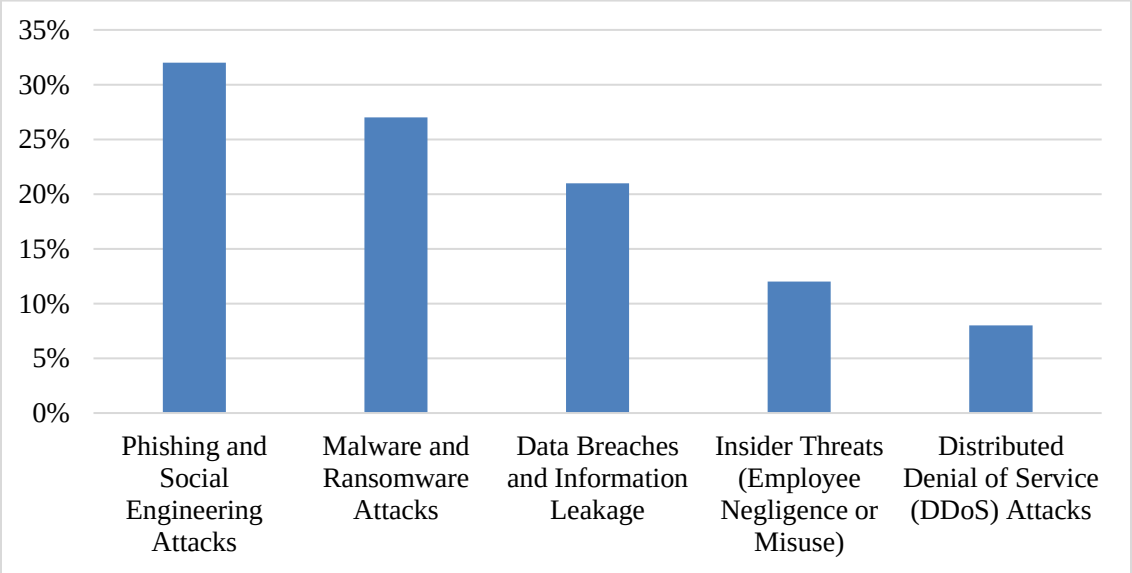
ISSN: 2320-3714
Volume: 1 Issue: 2
February 2026
Impact Factor: 11.9
Subject: Management

4.1. Prevalence of Major Cybersecurity Threats

Table 1 shows the percentage distribution of the key cybersecurity threats to the banking systems. The data indicate that the most common type of attack is phishing and social engineering attacks (32%), then malware and ransomware attacks are in the second (27%) and third (27) positions. Breach of the data and leakage of information (21%) makes up a good part of reported cases as well. Comparatively, insider threats (12%) and Distributed Denial of Service (DDoS) attack are less reported (8%). These variations are graphically illustrated in figure 1 which makes it obvious that there are relatively more externally driven cyber threats than there are internal and infrastructure based attacks.

Table 1: Prevalence of Cybersecurity Threats in Banking Systems

Type of Cybersecurity Threat	Percentage of Banks Affected (%)
Phishing and Social Engineering Attacks	32%
Malware and Ransomware Attacks	27%
Data Breaches and Information Leakage	21%
Insider Threats (Employee Negligence or Misuse)	12%
Distributed Denial of Service (DDoS) Attacks	8%



Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume: 1 Issue: 2
February 2026
Impact Factor: 11.9
Subject: Management

Figure 1: Graphical Representation of Prevalence of Cybersecurity Threats in Banking Systems

The results show that the cyber threats of human nature and deception are the biggest threat to contemporary banking systems. A large number of phishing and social engineering attacks also indicates that employees and customers are still one of the weak points regardless of the technological protection. The high percentage of malware and ransomware attacks indicates the growing complexity of cybercrime to monetize by interfering with the banking business. The insider threats and DDoS attacks are not as high, but their possible consequences to operational continuity and data integrity cannot be underestimated.

4.2 Impact of Cybersecurity Incidents on Banking Operations

Table 2 shows the probability of cybersecurity incidents on the different areas of operation of the banking institutions. The outcomes indicate that the most severe impact is financial losses (35%), which comprise loss on fraud and recovery expenses. Second is operational disruptions (29%), which is an issue that impacts the continuity of services and availability of the system. The loss of customer trust and reputational damage (22%), and regulatory and legal penalties (14%), are a large non-financial impact and the lowest-reported impact, respectively. These variations are illustrated graphically in figure 2, as the percentage ratio of cybersecurity attacks on financial and operational stability is evidently disproportionate.

Table 2: Impact of Cybersecurity Incidents on Banking Operations

Impact Area	Percentage Impact (%)
Financial Losses (Fraud, Recovery Costs)	35%
Operational Disruptions	29%
Loss of Customer Trust and Reputation	22%
Regulatory and Legal Penalties	14%

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume: 1 Issue: 2
February 2026
Impact Factor: 11.9
Subject: Management

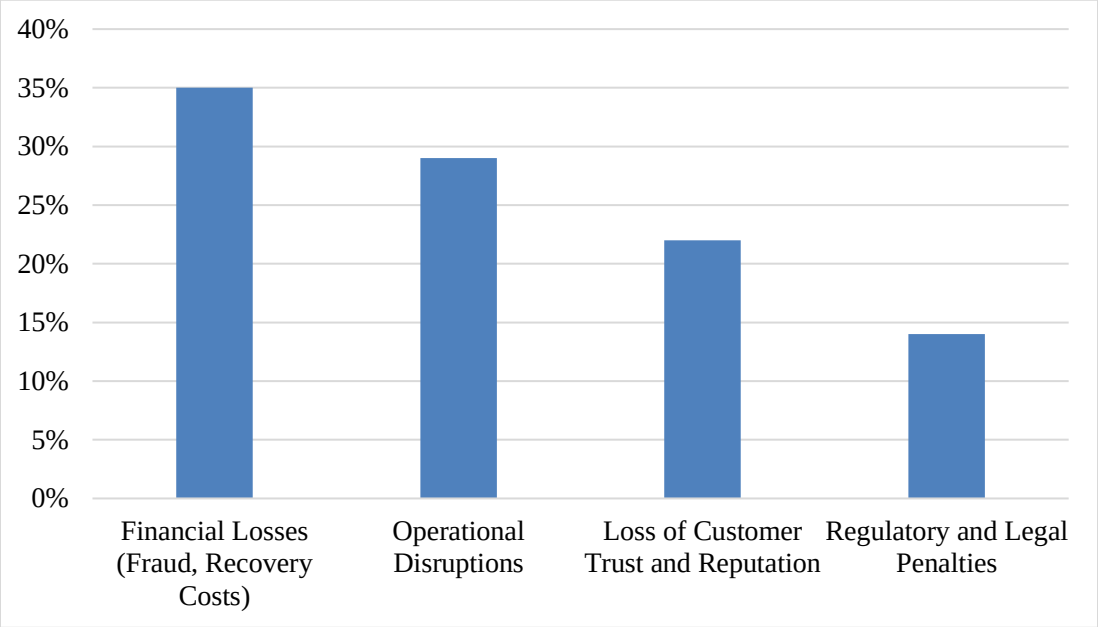


Figure 2: Graphical Representation of Impact of Cybersecurity Incidents on Banking Operations

The results suggest that cybersecurity breaches have short and long-term effects on the banking processes. The prevalence of financial losses can be used to highlight the direct economic cost of cyberattacks, which can be associated with significant investment in the recovery and restoration of the system. The crisis in the functioning is another factor that illustrates the susceptibility of digital banking systems to hackers. Even though regulatory penalty has a relatively lower percentage, it has serious compliance and governance consequences. The significant customer trust change highlights that cybersecurity is not only a technical concern, but a strategic risk to institutional credibility and competitiveness, which conflict with the need to implement comprehensive and active risk management strategies in the contemporary banking systems.

4.3 Effectiveness of Existing Cybersecurity Risk Management Practices

Table 3 shows the perceived efficacy of different cybersecurity risk management strategies followed by the banking institutions. According to the results, the firewalls and intrusion detection systems (30 percent) are deemed the most effective controls, with the second place going to the employee cybersecurity training programs (25 percent) and regular security audits and risk assessment (23 percent). Conversely, incident response and recovery planning (15%), and third-

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume: 1 Issue: 2
February 2026
Impact Factor: 11.9
Subject: Management

party risk management controls (7%) are rated relatively lowly in their effectiveness. These differences are shown graphically in figure 3 and their significance can be seen in the higher level of dependency on preventive and technical safeguards as opposed to response-oriented and external risk controls.

Table 3: Effectiveness of Cybersecurity Risk Management Measures

Risk Management Measure	Effectiveness Rating (%)
Firewalls and Intrusion Detection Systems	30%
Employee Cybersecurity Training Programs	25%
Regular Security Audits and Risk Assessments	23%
Incident Response and Recovery Planning	15%
Third-Party Risk Management Controls	7%

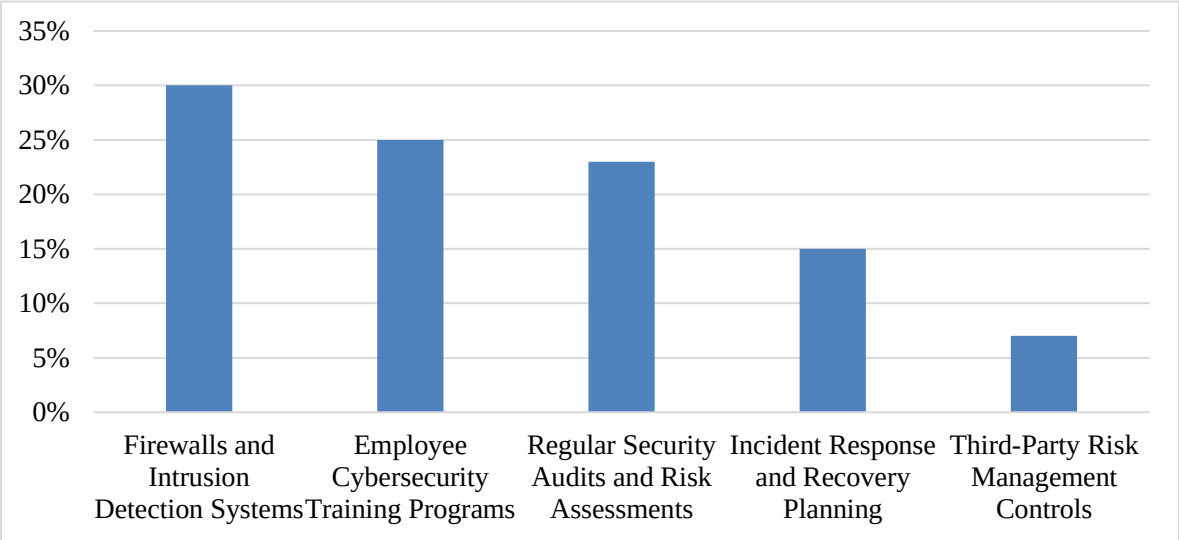


Figure 3: Graphical Representation of Effectiveness of Cybersecurity Risk Management Measures

The results indicate that banks still value technical and preventive security controls as the main tool in handling the cybersecurity threats. The comparatively high score of employee training can be interpreted as the increasing level of awareness of the human aspects of cybersecurity resilience.

ISSN: 2320-3714
Volume: 1 Issue: 2
February 2026
Impact Factor: 11.9
Subject: Management

Nevertheless, the reduced efficacy of incident response planning implies the possible flaws in the preparedness and recovery readiness during cyber events. The fact that the importance of managing risks-related to third-party is the least alarming is concerning, as the banks are becoming more and more reliant on the fintech partners, cloud utilities, and external vendors. On the whole, the findings indicate that a more balanced approach to cybersecurity should be implemented, to make response mechanisms and third-party supervision more effective in addition to the existing preventive measures.

5. DISCUSSION

These findings indicate clearly that the operational weaknesses, financial exposure, and human-centric threats are the most dominant factors that have contributed to the cybersecurity risk in contemporary banking systems. The prevalence of phishing and malware attacks is alarmingly high, which points to the ongoing gaps in user awareness and endpoint security, and the high financial and operational effects demonstrate direct economic and service-related effects of cyber attacks. Despite the extensive investment of the banks in preventive and technical controls including firewalls and intrusion detection systems, relatively low efficiency of incident response planning and third-party risk management points to the major weaknesses in resilience and preparedness. These results imply that cybersecurity should be considered the strategic, enterprise-wide risk, which should be better embedded in the risk governance systems, better trained employees, better incidence responses, and better monitoring of the service providers to assure sustainable banking functions in the more digital environment.

6. CONCLUSION

This paper concludes that the issue of cybersecurity risk has become a major strategic dilemma to the modern banking systems due to human-based threats, financial collision, and vulnerability of the operations. Phishing and malware attacks prevail, and the financial and reputational effects are huge, which underscores the increased complexity of the cyber risk environment. Although banks have invested in preventive and technical security significantly, it is clear that incident response preparedness and third-party risk management are still vulnerable. Thus, the complex and proactive strategy involving a combination of technological protection measures and staff

ISSN: 2320-3714
Volume: 1 Issue: 2
February 2026
Impact Factor: 11.9
Subject: Management

education, solid regulatory frameworks, and overall control over the external service providers can be viewed as an effective way of managing cybersecurity risks in banking and enhancing institutional resilience in the growing digital banking space.

REFERENCES

1. *Al-Alawi, A. I., & Al-Bassam, M. S. A. (2020). The significance of cybersecurity system in helping managing risk in banking and financial sector. Journal of Xidian University, 14(7), 1523-1536.*
2. *Al-Alawi, A. I., & Al-Bassam, S. A. (2019). Assessing the factors of cybersecurity awareness in the banking sector. Arab Gulf Journal of Scientific Research, 37(4), 17-32.*
3. *Alkhdour, T., AlWadi, B. M., & Alrawad, M. (2024). Assessment of cybersecurity risks and threats on banking and financial services. Journal of Internet Services and Information Security, 14(3), 167-190.*
4. *Azura, Y. T. Y., Azad, M. A., & Ahmed, Y. (2025). An integrated cyber security risk management framework for online banking systems. Journal of Banking and Financial Technology, 1-20.*
5. *Berdyugin, A. A., & Revenkov, P. V. (2019). Approaches to measuring the risk of cyberattacks in remote banking services of Russia. Безопасность информационных технологий, 26(4), 83-92.*
6. *Cele, N. N., & Kwenda, S. (2025). Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. Journal of Financial Crime, 32(1), 31-48.*
7. *Darem, A. A., Alhashmi, A. A., Alkhaldi, T. M., Alashjaee, A. M., Alanazi, S. M., & Ebad, S. A. (2023). Cyber threats classifications and countermeasures in banking and financial sector. IEEe Access, 11, 125138-125158.*
8. *Khan, H. U., Malik, M. Z., Nazir, S., & Khan, F. (2023). Utilizing bio metric system for enhancing cyber security in banking sector: A systematic analysis. Ieee Access, 11, 80181-80198.*

ISSN: 2320-3714
Volume: 1 Issue: 2
February 2026
Impact Factor: 11.9
Subject: Management

9. *Kristian, A., Az-Zahra, A. R., Hidayat, F., Fauzi, A. Y., & Kallas, E. (2024). Enhancing Cybersecurity Risk Management Strategies in Financial Institutions: A Comprehensive Analysis of Threats and Mitigation Approaches. Journal of Computer Science and Technology Application, 1(2), 96-103.*

10. *Oyewole, A. T., Okoye, C. C., Ofodile, O. C., & Ugochukwu, C. E. (2024). Cybersecurity risks in online banking: A detailed review and preventive strategies application. World Journal of Advanced Research and Reviews, 21(3), 625-643.*

11. *Shulha, O., Yanenkova, I., Kuzub, M., Muda, I., & Nazarenko, V. (2022). Banking information resource cybersecurity system modeling. Journal of Open Innovation: Technology, Market, and Complexity, 8(2), 80.*

12. *Stanikzai, A. Q., & Shah, M. A. (2021, December). Evaluation of cyber security threats in banking systems. In 2021 IEEE Symposium Series on Computational Intelligence (SSCI) (pp. 1-4). IEEE.*

13. *Thach, N. N., Hanh, H. T., Huy, D. T. N., Nga, L. T. V., Huong, L. T. T., & Vu, Q. N. (2021). technology quality management of the industry 4.0 and cybersecurity risk management on current banking activities in emerging markets-the case in Vietnam. International Journal for Quality Research, 15(3), 845.*

14. *Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability. Risk Management, 22(4), 239-309.*

15. *Waliullah, M., George, M. Z. H., Hasan, M. T., Alam, M. K., Munira, M. S. K., & Siddiqui, N. A. (2025). Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: a systematic literature review. arXiv preprint arXiv:2503.22710.*

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume: 1 Issue: 2
February 2026
Impact Factor: 11.9
Subject: Management

Author's Declaration

As an author of the above research paper/article, here by, declare that the content of this paper is prepared by me and if any person having copyright issue or patent or anything otherwise related to the content, I shall always be legally responsible for any issue. For the reason of invisibility of my research paper on the website /amendments /updates, I have resubmitted my paper for publication on the same date. If any data or information given by me is not correct, I shall always be legally responsible. With my whole responsibility legally and formally have intimated the publisher (Publisher) that my paper has been checked by my guide (if any) or expert to make it sure that paper is technically right and there is no unaccepted plagiarism and hentriacontane is genuinely mine. If any issue arises related to Plagiarism/ Guide Name/ Educational Qualification /Designation /Address of my university/ college/institution/ Structure or Formatting/ Resubmission /Submission /Copyright /Patent /Submission for any higher degree or Job/Primary Data/Secondary Data Issues. I will be solely/entirely responsible for any legal issues. I have been informed that the most of the data from the website is invisible, shuffled, or vanished from the database due to some technical fault or hacking and therefore the process of resubmission is there for the scholars/students who find trouble in getting their paper on the website. At the time of resubmission of my paper I take all the legal and formal responsibilities, If I hide or do not submit the copy of my original documents (Andhra/Driving License/Any Identity Proof and Photo) in spite of demand from the publisher, then my paper may be rejected or removed from the website anytime and may not be consider for verification. I accept the fact that as the content of this paper and the resubmission legal responsibilities and reasons are only mine then the Publisher (Airo International Journal/Airo National Research Journal) is never responsible. I also declare that if publisher finds any complication or error or anything hidden or implemented otherwise, my paper may be removed from the website, or the watermark of remark/actuality may be mentioned on my paper. Even if anything is found illegal publisher may also take legal action against me.

Sukumarn Nair. B
Dr.Pradeep Meghwal

*****