Indonesian Banking Review
Volume 3, Number 1, 2024

Cybersecurity Challenges and Strategies in Banking and Fintech in Indonesia

Indi Djastuti [1]

[1] Universitas Diponegoro, Semarang, Indonesia

Abstract

Article history:
Received: January 8, 2024
Revised: February 22, 2024
Accepted: April 21, 2024
Published: June 30, 2024

Keywords:
Banking,
Cybersecurity,
Fintech,
Indonesia
Regulation.

Identifier:
Zera Open
Page: 1-18
https://zeraopen.com/journal/ibr

Digital transformation has significantly changed the landscape of the financial sector, particularly banking and fintech. Digital innovation improves efficiency, accessibility, and financial inclusion, but on the other hand, poses increasingly complex cybersecurity risks. This research aims to analyze how cybercrime threats affect financial sector stability, assess the effectiveness of existing regulations and policies, and formulate collaborative strategies to strengthen cyber resilience. Using the literature study method on academic publications and real cases from the last five years, this study found that despite regulatory efforts through OJK, BI, and BSSN, implementation still faces challenges in the form of limited resources, suboptimal policy evaluation, and weak collaboration between institutions. Fintech and Islamic banks face specific challenges related to data protection and sharia compliance, which demand a more adaptive security strategy. In conclusion, the integration of financial risk management with cybersecurity, as well as strengthening the synergy between regulators, industry, and law enforcement is the key to maintaining public trust and financial stability in the digital era.

*Corresponding author:
(Indi Djastuti)

1. Introduction

Digital transformation has become a global trend in the financial and banking sectors, driving service innovation as well as system efficiency. The development of information technology, such as cloud computing, big data, artificial intelligence, and blockchain, has changed the way banks and fintechs operate and provide services to customers. In Indonesia, the digitalization of the financial sector is increasingly massive with the increasing number of mobile banking and fintech service users, which at the same time increases the exposure to cybercrime risks. Dependence on digital technology has a positive impact on financial access and inclusion, but on the other hand, it poses a new threat in the form of cybercrime (Burton et al., 2022).

Phenomena such as hacking, phishing, ransomware, and data leaks are becoming more frequent and threaten the stability of the financial system. The impact of cybercrime is not only in the form of financial losses, but also has implications for public trust and the reputation of financial institutions. According to Anwary (2022), the weak network security system in Indonesia's financial sector is one of the main factors that increase vulnerability to cyberattacks. Recent data shows an increasing trend in global cyber attack incidents, including in the financial sector. The study by Mehrban et al. (2020) confirms that cyber risks have a significant impact on fintech adoption, especially related to customer data security and digital application vulnerabilities.

In Indonesia, several cases of data leaks and ransomware attacks have been reported on banks and digital payment service providers, highlighting weak risk management and cyber defense strategies. Regulations and policies have been

developed by authorities, including Financial Services Authority (*Otoritas Jasa Keuangan*/OJK), Bank Indonesia (BI), National Cyber and Crypto Agency (*Badan Siber dan Sandi Negara*/BSSN). For example, Banking Information Technology Master Plan (*Rencana Induk Teknologi Informasi Perbankan*/RITI) evaluated by Sidik (2020) provides strategic direction regarding the implementation of cybersecurity. However, regulatory implementation often faces challenges in the form of limited human resources (HR), high investment costs, and weak evaluation of policy effectiveness.

The main gap in strengthening cybersecurity in Indonesia's financial sector is the lack of collaboration between institutions. According to Kharisma (2021), the protection of fintech customer data requires close cooperation between banks, technology providers, regulators, and law enforcement. In addition, specialized sectors such as Islamic banks face additional challenges related to sharia compliance, liquidity management, and secure and regulatory technology integration. The urgency of this research lies in the need for a strategy that integrates financial risk management with cybersecurity. Although the relevant literature is evolving, there are still gaps in understanding policy effectiveness, technology implementation, and cross-sector collaboration.

Therefore, the objectives of this study are to: (1) explain how cybercrime threats affect the financial and banking sectors, (2) examine the role of regulation and collaboration in strengthening cybersecurity, and (3) provide recommendations for prevention strategies and evaluation of cybersecurity policies in the financial sector. With a literature review approach, this paper seeks to provide a

comprehensive overview of the current conditions, challenges, and opportunities in building cyber resilience in the financial sector in Indonesia and globally. This is important to maintain financial system stability, strengthen public trust, and support the sustainability of healthy and safe digital transformation.

2. Literature Review

2.1. Digital Transformation and Cyber Risk in the Financial Sector

Digital transformation has been a key driver of change in the financial industry, creating opportunities to improve efficiency, accessibility, and service innovation. In Indonesia, the digitization of banking services is growing rapidly through mobile banking, internet banking, and integration with fintech platforms. These changes contribute to increased financial inclusion, especially for people who previously had difficulty accessing formal banking services. However, digitalization also increases the risk of exposure to cyber threats. Technological developments are often followed by the emergence of new modes of crime, such as hacking, phishing, ransomware, and distributed denial of service (DDoS) attacks. The massive digital transformation in Indonesia's banking sector has made this industry increasingly dependent on digital infrastructure, so its vulnerability to cyber threats has increased. In the global context, Jameaba (2020) emphasized that the digital revolution and fintech disruption have encouraged the need to strengthen systemic risk management.

Therefore, the financial sector needs to balance digital innovation efforts and an adequate cyber defense strategy to maintain stability and public trust. Awareness

of these risks is crucial, as cyberattacks threaten not only customers' data and financial assets, but also the integrity and reputation of the financial institution itself (Dupont, 2019). Financial losses from a cyberattack can be substantial, including system restoration costs, customer compensation, and regulatory fines. In addition, the loss of public trust can have a long-term impact, hindering business growth and further adoption of digital services. Faced with these dynamics, a proactive approach to cybersecurity, from investing in advanced technology to customer education, is imperative. The growing reliance on the digital ecosystem demands collaboration between financial institutions, regulators, and technology providers to create a more resilient and secure digital environment.

2.2. Cybersecurity Regulations and Policies

Regulation is an important foundation in building cyber resilience in the financial sector. The Government of Indonesia through OJK, Bank Indonesia (BI), dan BSSN has issued policies that regulate banking and fintech digital security standards. One of the important initiatives is RITI, which serves as a guideline in developing financial technology safely. Sidik (2020) emphasized that although RITI is an important reference, its implementation still faces obstacles in the form of limited human resources, costs, and lack of coordination across institutions. In addition, Anwary (2022) revealed that the Indonesian financial sector still has significant weaknesses in the computer network security system, so there is a need for stricter regulations and more consistent supervision.

Thus, existing policies are not fully able to answer the challenges of cyber threat dynamics, so they need to be strengthened through coordination, continuous

evaluation, and the implementation of international standards. The challenges in the implementation of these regulations show that there is a gap between the policies designed and the reality on the ground (Lavee et al., 2018). Budget constraints and technical expertise at some financial institutions, especially smaller ones, often hinder the adoption of required security standards. Therefore, more concrete government support, such as training programs and fiscal incentives, is needed to help financial institutions meet these standards. In addition, closer coordination between regulators is urgently needed to avoid policy overlap and ensure a rapid and integrated response to cyber incidents. International standards such as ISO 27001 can serve as additional guidance to strengthen security frameworks, ensuring that security practices in Indonesia are aligned with global best practices.

2.3. Challenges of Fintech and Islamic Banks in Cybersecurity

Fintech is one of the sectors most affected by cybersecurity risks due to its digital-based characteristics and involvement in managing customers' personal data. Cyber threats to fintech not only impact financial losses, but also on consumer trust that greatly determines the sustainability of services. Suryono et al. (2020) shows that cyber risks significantly affect fintech adoption because consumers are becoming more cautious in using digital financial applications. Another challenge arises in the Islamic banking sector which in addition to having to face technological risks, is also required to comply with sharia principles in its operations. This makes cyber risk management more complex because it must integrate compliance with sharia regulations with digital defense strategies. According to Rabbani (2022), digital wallets based on Islamic economics require a strong security design while in

accordance with sharia principles in order to encourage financial inclusion based on Islamic values.

Therefore, the security strategy of fintech and Islamic banking must be holistic, including aspects of technology, regulation, and consumer trust. In the case of fintech, rapid innovation often comes with security risks that have not been fully tested, leaving the platform vulnerable to attacks. The protection of customers' personal data is a top priority, considering the large volume of data managed and its sensitivity. Meanwhile, for Islamic banking, the main challenge is to ensure that any digital security solution does not conflict with Islamic principles, such as the prohibition of usury and speculation (Chong, 2021). This requires the development of unique solutions, for example in terms of data storage and auditing, that comply with sharia guidelines. This holistic approach should also include user education, which is often the weakest point in the security chain, as well as collaboration with cybersecurity experts and regulatory bodies to ensure that existing solutions can effectively protect digital assets and customer trust.

3. Methods

This study uses the literature study method as the main approach in analyzing cybersecurity in the financial and banking sectors. The literature study was chosen because it was able to provide a comprehensive overview of the current conditions, challenges, and strategies that have been implemented in various countries, including Indonesia. Through searching academic literature, regulatory reports, and publications from authority institutions such as OJK, Bank Indonesia (BI), and

BSSN, this study seeks to identify existing research patterns, trends, and gaps. The process of collecting literature data is carried out by accessing various scientific sources from online databases, including Google Scholar, Elsevier, and national/international journal portals.

The publication time span used is the last five years to ensure relevance to the current dynamics in the field of digital transformation and cybersecurity. Keywords used in searches include "cybersecurity in banking sector," "fintech security," "financial regulation Indonesia," and "cybercrime in financial services." In addition, the selected articles are screened based on relevance to the topic, the quality of publications, and the availability of empirical data and conceptual studies that support the research objectives. Data obtained from various literature were then analyzed with a descriptive-analytical approach. Descriptive analysis is used to describe the general conditions of digital transformation, cybersecurity regulations, as well as cases of cyberattacks in the financial sector.

Furthermore, an analytical analysis is conducted to evaluate the effectiveness of policies, identify implementation challenges, and formulate strategies that can improve cyber resilience in the banking and fintech sectors. In this case, the research not only exposes information, but also criticizes the gap between theory, regulation, and practice in the field. The next stage is to categorize the literature based on the main themes, namely: (1) digital transformation and cyber risk, (2) cybersecurity regulations and policies, and (3) fintech and Islamic bank challenges. This categorization aims to facilitate the synthesis of information while showing how

various aspects are interrelated in forming a cybersecurity framework in the financial sector.

The results of the analysis from each category were then used to formulate the main arguments of the study, which included the impact of cybercrime threats on financial sector stability, the role of regulation in strengthening cyber defense, and recommendations for collaborative strategies between institutions and industry players. With this approach to literature study, the research is expected to make theoretical and practical contributions. From the theoretical side, the research enriches academic studies on the relationship between digital transformation, regulation, and cybersecurity in the financial sector. From a practical perspective, the research is expected to be able to provide literature-based recommendations that can be used by regulators, banks, fintech, and other stakeholders in formulating more effective cybersecurity policies and strategies.

4. Results

Digital transformation in the financial sector is bringing significant changes to the way banks, fintechs, and other financial institutions operate. The digitization of services improves transaction efficiency, expands financial inclusion, and creates new opportunities for economic growth. However, this positive impact is followed by an increasing threat of increasingly complex cyber attacks. The results of the literature study show that despite the various security policies and strategies in place, the financial sector still faces major challenges in maintaining stability and public trust. One of the key findings is the increased exposure to cyber risks due to the

acceleration of digitalization. Banking in Indonesia, for example, increasingly relies on digital services such as mobile banking, internet banking, and integration with fintech. According to Gunawan et al. (2022), digital transformation in Indonesia's banking sector has expanded financial access for the public, but on the other hand it has increased dependence on digital infrastructure that is prone to attack. This vulnerability is seen in a number of data leak cases involving customers' personal information and ransomware attacks that disrupt payment services.

Another important finding is the weak readiness of the financial sector in dealing with cyberattacks that continue to evolve. Suhartanto et al. (2022) emphasized that network security systems in many financial institutions in Indonesia are not adequate to counteract advanced digital threats. One of the main problems is the limited number of human resources who have expertise in the field of cybersecurity. Many banks still consider investment in this area to be an additional cost, rather than a strategic necessity, thus delaying the adoption of more advanced defense technologies. In addition, the literature shows that cyber threats not only impact financial losses, but also on aspects of public trust and the reputation of financial institutions. Suryono et al. (2020) explained that cyber risk has a significant impact on the level of fintech adoption because consumers are increasingly selective in using digital financial applications.

Cases of customer data leakage or theft of funds through phishing attacks can reduce public interest in utilizing digital financial services, which can ultimately hinder the development of fintech. This decline in trust poses a serious threat to business sustainability, especially for fintechs that rely heavily on massive user

adoption. As news of cyberattacks or data breaches widespread, consumers become more wary and reluctant to share their personal information or store their funds on digital platforms. This creates a negative cycle where high cyber risk leads to low trust, which in turn stifles growth. To break this cycle, financial institutions need to proactively communicate their security strategies to customers, demonstrate transparency, and take concrete steps to protect data.

Cybersecurity regulations and policies have been drafted by the government and relevant authorities. One of the important regulatory frameworks is RITI. Sidik (2020) found that although RITI provides a clear direction for banks in implementing information technology, its effectiveness is still limited due to weak inter-agency coordination and low industry compliance. This is exacerbated by the limited periodic evaluation of regulatory implementation, so that the strategies implemented are not always relevant to the latest cyber threat developments. Lack of coordination between institutions such as OJK, BI, and BSSN can create overlapping regulations or oversight loopholes that can be exploited by cybercriminals.

In addition, low compliance from the industry, which may be due to high costs or lack of understanding, undermines regulatory objectives. Without continuous evaluation and adjustment, regulations become obsolete and unable to address the rapidly growing cyber challenges. Therefore, a more holistic and dynamic approach is needed in cybersecurity regulation, which includes better coordination between agencies, stricter law enforcement, and regular evaluation mechanisms.

Regulators must also work closely with industry to understand the practical challenges they face and provide the necessary support to improve compliance.

The fintech sector faces different challenges from conventional banking. Fintechs are more vulnerable to cyber threats because all of their operations are digital-based. The main risks are personal data theft, transaction manipulation, and misuse of digital identities. According to Kharisma (2021), the data protection of fintech customers in Indonesia is still not optimal because many service providers do not have security standards equivalent to banks. This makes consumers more vulnerable to becoming victims of cyberattacks, while regulators struggle to carry out supervision due to the growing number of fintech operators. Islamic banks also face more complex challenges. In addition to having to face the same cyber threats as conventional banks, Islamic banks are required to ensure that their financial systems are in accordance with Islamic principles.

Rabbani (2022) emphasized that the use of digital wallets based on Islamic economics must be designed with a security system that is sharia-compliant while being strong in the face of digital threats. Non-compliance with sharia principles can raise legitimacy issues, while weak security can undermine the trust of the Muslim community in Islamic banks. This dual challenge puts Islamic banks in a unique position that requires innovation in security that also considers ethical and religious compliance aspects. Both fintechs and Islamic banks must develop security strategies that are not only technically strong but also adaptive to the unique business models and values they embrace. This includes investing in scalable and flexible security

technologies, as well as working with experts who understand their specific challenges.

From a global perspective, financial digitalization also has implications for the stability of the financial system as a whole. Jameaba (2020) shows that digitalization and new technologies in the banking sector provide opportunities for economic growth, but also increase systemic risks if cybersecurity is not managed properly. Widespread cyberattacks can disrupt payment systems, reduce public trust in financial institutions, and even trigger financial crises if not addressed quickly. Therefore, cybersecurity is no longer a problem faced by only one entity, but rather a systemic problem that requires a global approach. Another relevant finding is the importance of collaboration between institutions in strengthening cyber resilience. Cyberattacks are cross-border and can attack multiple sectors simultaneously.

Therefore, banks, fintechs, regulators, and law enforcement officials must work together in building a strong cybersecurity ecosystem. According to Maiti and Ghosh (2021), the ecosystem of digital financial applications such as mobile banking and e-wallets is very vulnerable to malware and phishing attacks, so a collective strategy is needed between application developers, regulators, and security service providers. This collaboration should include sharing threat intelligence information, developing joint incident response protocols, and conducting joint exercises to improve readiness. Building a resilient ecosystem requires a commitment from all parties to work together, overcome sectoral egos, and view cybersecurity as a shared responsibility. Thus, the financial sector can take full advantage of the potential of digital transformation while effectively mitigating the risks that come with it.

The results of the literature study show that Indonesia's financial sector is in a critical phase in its digital transformation. Digitalization brings great benefits in driving financial inclusion, but the ever-evolving cyber risks are a major barrier. Regulations are already available, but their implementation is still ineffective. Fintech and Islamic banks face specific challenges that demand more adaptive security strategies. Inter-agency collaboration and integration of cybersecurity strategies with financial risk management are the main keys to building sustainable resilience. This transformation is not just about adopting new technologies, but also about building a strong security foundation to protect systems, data, and, most importantly, public trust.

5. Discussion

The results show that digital transformation in the financial sector is inseparable from the increasing cyber threats. These findings are consistent with the international literature that confirms that the acceleration of financial digitalization is often accompanied by an increased risk of cybercrime. In Indonesia, the high dependence on digital infrastructure makes the banking and fintech sectors easy targets for cybercriminals. This shows that there is a trade-off between the benefits of digitalization and the need for large investments in strengthening cybersecurity. Government policies through regulations such as RITI have played an important role in building the security foundation.

However, policy implementation still faces limitations at the industry level. The gap between regulation and practice in the field makes defense strategies not

optimal. As noted by Srinivas et al. (2019), continuous coordination and evaluation are very important so that regulations are not only formal, but also able to respond to cyber threats that continue to develop. Thus, regulations must be dynamic and adaptive to technological changes. The discussion also highlighted the unique challenges faced by fintechs and Islamic banks. Fintechs are particularly vulnerable to cyberattacks because their entire business model is digital-based.

Cases of data theft and digital identity leakage can quickly lower consumer trust. Mehrban et al. (2020) emphasized that consumer trust is a determining factor for the sustainability of fintech adoption, so personal data protection is a top priority. Meanwhile, Islamic banks face a dual challenge: ensuring compliance with sharia principles while maintaining the security of the digital financial system. This demands regulatory innovation and technological design that can integrate religious aspects with global security standards. In addition to regulatory and technological aspects, collaboration between institutions is also an important issue in cybersecurity discussions. Cyber threats are cross-border and cannot be partially addressed by a single institution.

Synergy between banks, fintech, regulators, and law enforcement is needed to build a resilient security ecosystem. According to Maiti and Ghosh (2021), the digital financial application ecosystem requires a collective approach between app developers, regulators, and cybersecurity providers to reduce vulnerability to malware and phishing. Thus, multistakeholder collaboration is the main key in strengthening cyber resilience in the financial sector. This discussion emphasized that cybersecurity strategies must be integrated with financial risk management. This

means that risk management focuses not only on financial aspects, but also on data protection, system reliability, and public trust. Without this integration, the financial sector will remain vulnerable to shocks due to cyberattacks that have the potential to disrupt national economic stability.

6. Conclusion

Digital transformation in the financial sector brings great opportunities for efficiency, innovation, and expansion of financial inclusion. However, this development also increases vulnerability to increasingly complex cyber threats. The results of the study show that cyber risks not only impact financial losses, but also affect public trust and the reputation of financial institutions. Thus, cybersecurity is no longer just a technical need, but a strategic element in maintaining financial system stability. Regulations and policies that have been formulated by the authorities play an important role as a basic framework for protection.

However, the effectiveness of its implementation still faces obstacles, both in terms of human resources, costs, and coordination between institutions. The fintech and Islamic banking sectors have specific challenges that demand integration between compliance, innovation, and digital security. Therefore, the strategies taken must be adaptive, comprehensive, and collaboration-based. This research emphasizes the urgency of building a stronger cybersecurity ecosystem through the synergy of regulators, banks, fintech, and law enforcement officials. With this approach, the financial sector is not only able to survive cyber threats, but also can

continue to develop sustainably, support economic stability, and maintain public trust in the digital era.

References

Anwary, I. (2022). The Role of Public Administration in combating cybercrime: An Analysis of the Legal Framework in Indonesia. *International Journal of Cyber Criminology*, *16*(2), 216-227.

Burton, A., Cooper, C., Dar, A., Mathews, L., & Tripathi, K. (2022). Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimisation: A realist review. *Experimental gerontology*, *159*, 111678.

Chong, F. H. L. (2021). Enhancing trust through digital Islamic finance and blockchain technology. *Qualitative Research in Financial Markets*, *13*(3), 328-341.

Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. *Journal of cybersecurity*, *5*(1), tyz013.

Gunawan, J., Permatasari, P., & Sharma, U. (2022). Exploring sustainability and green banking disclosures: a study of banking sector. *Environment, Development and Sustainability*, *24*(9), 11153-11194.

Jameaba, M. S. (2020). Digitization Revolution, FinTech Disruption, and Financial stability: Using the Case of Indonesian Banking Ecosystem to highlight wide-ranging digitization opportunities and major challenges. *SSRN Electronic Journal*, 1-44.

Kharisma, D. B. (2021). Urgency of financial technology (Fintech) laws in Indonesia. *International Journal of Law and Management*, *63*(3), 320-331.

Lavee, E., Cohen, N., & Nouman, H. (2018). Reinforcing public responsibility? Influences and practices in street-level bureaucrats' engagement in policy design. *Public Administration*, *96*(2), 333-348.

Maiti, M., & Ghosh, U. (2021). Next-generation internet of things in fintech ecosystem. *IEEE Internet of Things Journal*, *10*(3), 2104-2111.

Mehrban, S., Nadeem, M. W., Hussain, M., Ahmed, M. M., Hakeem, O., Saqib, S., ... & Khan, M. A. (2020). Towards secure FinTech: A survey, taxonomy, and open research challenges. *Ieee Access*, *8*, 23391-23406.

Rabbani, M. R. (2022). Fintech innovations, scope, challenges, and implications in Islamic Finance: A systematic analysis. *International Journal of Computing and Digital Systems*, *11*(1), 1-28.

Sidik, M. (2020). Cyber security applied for financial sector in Indonesia. *Jurnal Pajak dan Bisnis*, *1*(1), 30-47.

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future generation computer systems*, *92*, 178-188.

Suhartanto, D., Syarief, M. E., Chandra Nugraha, A., Suhaeni, T., Masthura, A., & Amin, H. (2022). Millennial loyalty towards artificial intelligence-enabled mobile banking: evidence from Indonesian Islamic banks. *Journal of Islamic Marketing*, *13*(9), 1958-1972.

Suryono, R. R., Budi, I., & Purwandari, B. (2020). Challenges and trends of financial technology (Fintech): a systematic literature review. *Information*, *11*(12), 590.