# Unlocking FinTech's Potential: The Crucial Role of Cybersecurity and Trust in Malaysia

**Salfariza Rozali[1], Amirul Afif Muhamat[2], Norshima Humaidi[3], Muhammad Hafiz Abd Rashid[4]**

[1]Faculty of Business and Management, Universiti Teknologi MARA, Malaysia

[2]Faculty of Business and Management, Universiti Teknologi MARA, Malaysia

[3]Faculty of Business and Management, Universiti Teknologi MARA, Malaysia

[2]Faculty of Business and Management, Universiti Teknologi MARA, Malaysia

**Abstract**

The rapid emergence of financial technology (FinTech) has revolutionized the banking industry, propelling it into the digital age. However, this transformative shift has also brought critical concerns regarding data protection and cybersecurity to the forefront, issues that remain unresolved and pose significant challenges for the sector. Cybersecurity and trust are paramount as they directly influence customer adoption and the overall success of FinTech initiatives. This study delves into existing research within the Malaysian context, analyzing previous findings to identify the potential precursors that have shaped current trends in the region. The finding presented is a valuable reference point and highlights the current progress in the industry. By examining historical data, socio-economic factors, and relevant policies, this research aims to uncover the underlying forces that have contributed to the present-day landscape.

**Keywords** fintech; cybersecurity; trust; banking; customer adoption

## 1. Introduction

Financial Technology or FinTech businesses are a great ecosystem**.** Modern technology or digital businesses deliver financial services and products. The digital business disrupts old banking practices and transforms traditional banking into a new facet of financial services solutions. With FinTech, the change is wide-ranging, increasing operational efficiencies and productivity, expanding the business platform, increasing customer value, and increasing financial inclusion. Such developments include mobile banking, e-commerce, digital investment, and other digital products and services that have created a new paradigm in digital banking.

Digital transformation has impacted cybersecurity challenges, and the rise of digital banking, mobile payments, and online financial services has created more entry points for cyber threats. The rate of cyber-attacks is spiking, and implementing strong cybersecurity models is one of the appropriate techniques to ensure confidentiality, data integrity and customers' trust (Chaudhry and Hydros (2023). There is a lack of understanding of how trust and cybersecurity influence customer adoption of FinTech services. Therefore, this study presents a conceptual discussion on potential precursors and uncovers forces that shaped current trends in Malaysia.

## 2. Literature Review

### 2.1 Issues

FinTech continues to have prevalent implications for the banking sector. Customers expect faster transactions, frictionless, more customised services, and growing awareness about essential data privacy and security. Digital business models are also becoming more ecosystem-driven through a platform or a network of partnerships. Alongside this, the risk landscape is reshaping. The boundaries within and beyond the financial sector are becoming increasingly interconnected and complex.

The problems and issues plaguing FinTech and digital business across the globe. In this study, two pertinent problems were addressed. Cybersecurity and trust issues are pivotal factors in successfully adopting FinTech services. Both factors have a paramount effect and are interrelated. In a study by Zhang et al.(2023), data security is a crucial element that customers consider before adopting any FinTech services. The critical concern is the sensitive data provided, such as personal data information and bank account details. Undoubtedly, the trust of customers and cybersecurity are interrelated and significantly influence the customer adoption of FinTech services. The statement supported by Dwivedi et al. (2019) on re-examining the unified theory of acceptance of the use of technology (UTAUT) towards a revised theoretical model found that their perception of data security significantly influences customer trust.

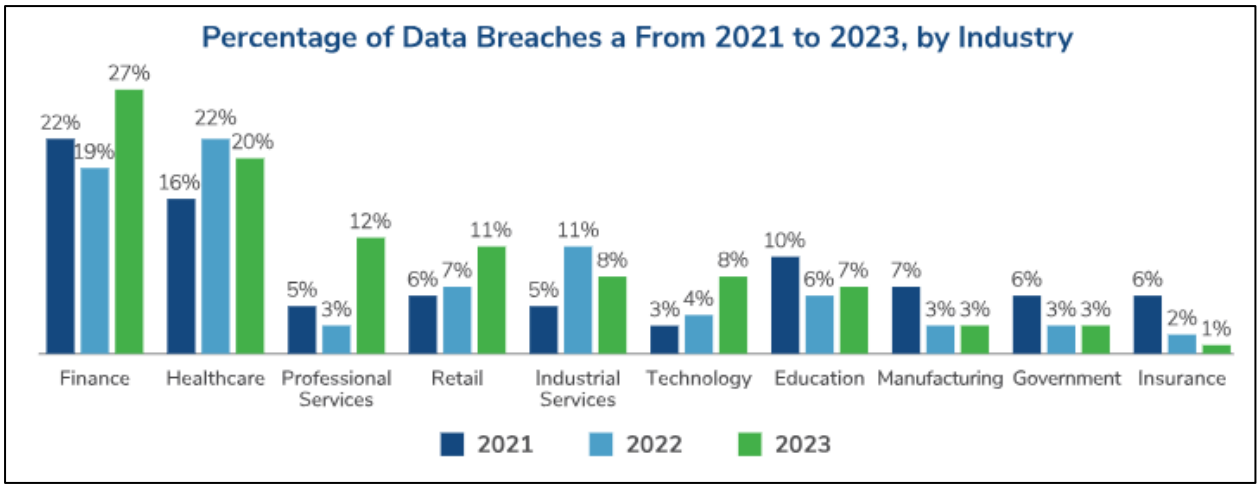


**Diagram 1.** Percentage Of Data Breaches From 2021 To 2023 By Industry
Sources: 2024 Data Breach Outlook | Cyber Risk | Kroll

Diagram 1 shows the percentage of data breaches worldwide from 2021 to 2023. The data reveal that the finance industry has significantly increased data breaches due to cyber threats. The finance industry has the most exposure to cybersecurity risk, which interrupts the adoption of FinTech and lowers customer trust in technology. A survey of Malaysia Cisco's 2024 Cybersecurity Readiness Index found that only two per cent of companies are highly prepared to withstand modern cybersecurity threats. This index benchmarks companies' hyper-connectivity and ability to defend against cyber threats. The significant gap and preparedness leave most companies vulnerable to sophisticated cyber threats.

The consequences of a cybersecurity breach in the banking sector can be devastating, including financial losses, reputational damage, regulatory penalties, and erosion of customer trust. Therefore, addressing cybersecurity issues in FinTech services is not just a technical necessity but a critical component of strategic risk management in the banking industry. The evolving FinTech services in the banking industry have amplified the need for robust cybersecurity measures to protect against evolving threats, ensure regulatory compliance, and maintain the integrity and trustworthiness of financial institutions.

## 2.2 FinTech in the Banking Sector

FinTech, or Financial technology, has recently transformed Malaysia's banking sector. Technology-driven innovations provide a range of products and services to customers. These products and services are expected to improve productivity, efficiency, and convenience (Hu et al., 2019). With the transformation of FinTech and modern technology and the rise of the digital ecosystem, FinTech has become a crucial part of Malaysia's banking sector.

Innovations such as electronic wallets, mobile banking, paperless lending, secure online payment channels, and others are extensively used in Malaysia. An upsurge in internet mobile and internet banking usage in the banking sector between 2019 and 2023 has been noted. These e-channel payments collectively handled transactions of 8,949 million with a value of 55,307,627 million ringgit between 2019 and 2023. Alongside the increasing trends, Malaysia is no exception and has countersigned significant growth in FinTech in recent years.

## 2.3 Strengthen Cybersecurity Readiness and Responsiveness

Malaysia's financial sector is undergoing a comprehensive digital transformation. As cross-border and global supply chain connections deepen, new interdependencies and potential vulnerabilities emerge (National Cybersecurity Agency, 2024). Within this network, each point is a potential target for cyber threats. Unlike most operational risks, a security breach at one point can rapidly impact others. Cybersecurity poses a significant threat to Malaysia's ongoing digitalization of financial services. Digital ecosystems drive innovation and introduce risks such as operational disruptions, data breaches, fraud, and financial losses. These risks can severely affect financial stability, reputation, and the broader economy.

The evolving technology landscape shapes the complexity of cyber threats, with cybercriminal tools constantly evolving to make attacks more creative. A robust cybersecurity foundation is still a critical priority for the financial sector, supporting innovation and digitalization. To proactively address cybersecurity threats, the regulatory body has formulated a comprehensive blueprint to manage and mitigate risks (BNM Financial Blueprint 2022 to 2026). Diagram 2 visually depicts critical factors influencing Malaysia's cybersecurity landscape, including interconnectivity, work arrangements, modernization, increased cloud adoption, and evolving threats. These factors serve as key focal points for addressing cybersecurity challenges, and an advanced strategic plan has been devised to enhance cybersecurity resilience.

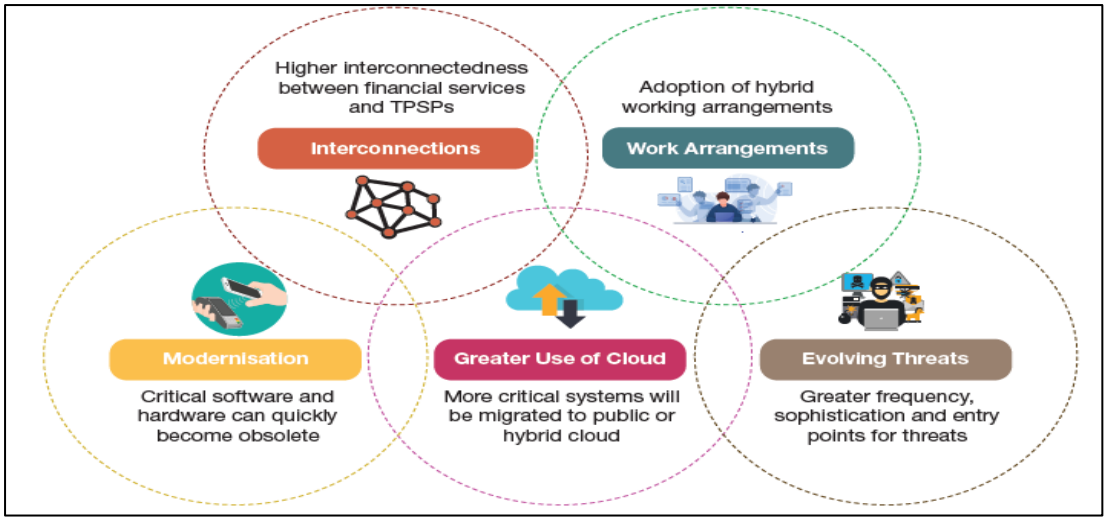


**Diagram 2.** Key Factors Shaping The Cyber Security Landscape In Malaysia
Source: Bank Negara Malaysia

Two preventive measures to strengthen defences include enhancing cybersecurity oversight and monitoring domestic and global capabilities. These strategies emphasise the importance of the financial services industry adhering to robust minimum standards for cyber risk governance and management. Additionally, the escalating concern surrounding third-party service providers (TPSPs) necessitates thoroughly evaluating existing policies. Regulatory develop supplementary frameworks to safeguard the entire financial ecosystem across its value chain. Furthermore, given the growing interdependence with TPSPs, expanding the regulatory perimeter becomes imperative.

As a result, initiative-taking measures are to establish secure technology linkages between the financial system and third-party providers. Malaysia's approach to cybersecurity is comprehensive, involving robust policies, regulatory frameworks, dedicated institutions, and active engagement with the private sector and international community. These practices aim to create a secure digital environment, protecting national interests and individual users from the ever-evolving landscape of cyber threats.

## 2.4 Securing Digital and Customer Trust

Building trust with customers is one crucial factor in adopting technologies. In the FinTech context, trust concerns customers' confidence in digital financial services transactions. Digital Trust encompasses individuals' expectations that digital technologies and services will safeguard all stakeholders' interests while upholding societal norms and values. The FinTech industry is particularly vulnerable to security breaches due to its handling of sensitive and substantial financial information, including passwords, bank account details, and biometric data (Singh et al., 2021). Nangin et al. (2020) concur that strengthening data security is imperative to prevent misuse. Hence, ensuring robust data security remains paramount for facilitating secure financial transactions (Stewart & Jürjens, 2018).

The digital payment landscape is evolving with various e-payments, digital financial platforms and traditional financial services creating new linkages and dependencies in financial ecosystems. Thus, consumers' perceived risk associated with digital trust significantly

influences the acceptance of digital products and services (Ali et al.,2022). Regulators are adopting proactive cybersecurity measures and protocols to mitigate risks linked to digital payment products and services (Krishna et al.,2023).

The lack of trust in institutional structures and mechanisms among customers hinders their willingness to engage in online transactions due to perceived risks. Such distrust can potentially erode the adoption of FinTech products and services. Furthermore, financial institutions should provide convenience, transparency, speed, and secure transactions to increase customer trust in FinTech. Trustworthiness and transparency are needed to comprehend the complexities of trust in financial institutions and how to reduce user's security and privacy concerns.

## 3. Discussion

This section employed the findings and discussion from extant literature studies. According to Zhang et al. (2023), financial services have invested heavily in upgrading their IT infrastructure to improve efficiency. However, the data security of FinTech services remains a questionable and crucial issue. The previous Hu et al. (2019) study found that customer trust significantly influences the purpose of adopting FinTech. Therefore, FinTech innovators should appropriately understand customer attitudes regarding data security and increase transparency for customers' awareness of how the data is stored and used safely. Besides, Ali et al.(2021) cited those perceived benefits positively and significantly impacted customer trust. The result is consistent with the study by Zhang et al. (2023), which showed that trust is one of the factors influencing the adoption of FinTech services. Furthermore, Al Duhaidahawi et al. (2020) found that cybersecurity impacted on the adoption of Fintech services, which has an excellent impact rate. They concluded that bank customers have a very high electronic culture and trust in technology, can face cybersecurity risks, and develop skills continuously to mitigate the risk of cybersecurity.

## 4. Conclusion

In summary, this preliminary conceptual study aims to highlight the potential problems and issues of the crucial role of cybersecurity and customer trust in adopting FinTech services. The multi-faceted relationships involve regulatory frameworks, technological advancements, user behaviours, and market dynamics. Robust cybersecurity measures significantly increase user trust, leading to higher adoption rates of FinTech services. This adoption is crucial for driving economic growth, as it can lead to increased financial inclusion and innovation in financial services.

Strong cybersecurity practices can make Malaysian FinTech companies and banks more attractive to local and international investors, facilitating capital inflow and fostering an environment conducive to innovation. The Cyber Security Bill 2024 introduction aims to design a comprehensive regulatory framework to bolster the FinTech sector's cybersecurity practices. This regulation will enforce FinTech companies' standards, increasing overall trust in the ecosystem. Aligning with international cybersecurity standards can enhance the credibility of Malaysian FinTech firms on a global scale, making cross-border transactions more secure and seamless.

## 5. Implication of Study

The study's practical implications contributed to the body of knowledge for practitioners, policymakers, companies, financial services, consumers, and future researchers. The significant growth of data security and privacy issues accelerates the number of cyber threat attack points. By highlighting the issues and preventive measures, FinTech companies can foster growth, innovation, and economic prosperity while improving a secure and trustworthy environment for stakeholders. For policymakers, the outcomes may be used to formulate strategies and improve existing policies and procedures to become more effective.

The outcomes may also benefit financial services by helping them understand customer culture and preferences. Companies may build trust through robust cybersecurity measures that can increase customer retention and enhance customer experience by ensuring secure FinTech environments. Zhang et al. (2023) uphold that companies should prioritise the development of robust data security measures to address customer trust by providing transparent and reliable services. The study insights exemplify valuable guidance to many stakeholders to enhance FinTech adoption and utilization while ensuring the security and trustworthiness of these digital platforms.

## 6. References


Al Duhaidahawi, H. M. K., Zhang, J., Abdulreza, M. S., Sebai, M., & Harjan, S. A. (2020). Analysing the effects of FinTech variables on cybersecurity: Evidence form Iraqi Banks. International Journal of Research in Business and Social Science, (6), 123-133. https://doi.org/10.20525/ijrbs.v9i6.914

Ali, M., Raza, S. A., Khamis, B., Puah, C. H., & Amin, H. (2021). How perceived risk, benefit and trust determine user Fintech adoption: a new dimension for Islamic finance. foresight, 23(4), 403-420. https://doi.org/10.1108/FS-09-2020-0095

Al-Okaily, M., Al Natour, A. R., Shishan, F., Al-Dmour, A., Alghazzawi, R., & Alsharairi, M. (2021). Sustainable FinTech innovation orientation: a moderated model. Sustainability, 13(24), 13591.https://doi.org/10.3390/su132413591

Bank Negara Malaysia, " Financial Sector Blueprint 2022 to 2026", available at https://www.bnm.gov.my/documents/20124/5915429/fsb3_en_book.pdf (accessed 27 May 2024)

Bank Negara Malaysia " Payment Statistic" available at https://www.bnm.gov.my/payment-statistics (Access 27 May 2024)

Chaudhry, U. B., & Hydros, A. K. (2023). Zero-trust-based security model against data breaches in the banking sector: A blockchain consensus algorithm. IET blockchain, 3(2), 98-115. https://doi.org/10.1049/blc2.12028

Dwivedi, Y. K., Rana, N. P., Jeyaraj, A., Clement, M., & Williams, M. D. (2019). Re-examining the unified theory of acceptance and use of technology (UTAUT): Towards a revised theoretical model. Information systems frontiers, 21, 719-734. https://doi.org/10.1007/s10796-017-9774-y

Hu, Z., Ding, S., Li, S., Chen, L., & Yang, S. (2019). Adoption of fintech services for bank

users: An empirical examination with an extended technology acceptance model. Symmetry, 11(3), 340. https://doi.org/10.3390/sym11030340

Kherk Ying. C and Kan.S (2024), Legislation: A new era for cybersecurity in Malaysia. Legislation: A new era for cybersecurity in Malaysia (theedgemalaysia.com) (accessed 27 May 2024)

Krishna, B., Krishnan, S., & Sebastian, M. P. (2023). Understanding the process of building institutional trust among digital payment users through national cybersecurity commitment trustworthiness cues: a critical realist perspective. Information Technology & People. https://doi.org/10.1108/ITP-05-2023-0434

Murgiah.S (2024), "Only 2% of Malaysian organisations resilient against cyber threats — Cisco", available at Only 2% of Malaysian organisations resilient against cyberthreats — Cisco (theedgemalaysia.com) (accessed 29 March 2024)

National Cyber Security Agency. Malaysia Cyber Law. Retrieved May,25,2024, from https://www.nacsa.gov.my/legal.php

Nangin, M. A., Barus, I. R. G., & Wahyoedi, S. (2020). The effects of perceived ease of use, security, and promotion on trust and its implications on fintech adoption. Journal of Consumer Sciences, 5(2), 124-138. https://doi.org/10.29244/jcs.5.2.124-138

PWC, Putting security at epicenter of innovation: Findings from the 2024 Global Digital Trust Insights, Dec 2023. 2024 Digital Trust Insights- Malaysia Report (pwc.com)

Singh, G., Gupta, R., & Vatsa, V. (2021, November). A framework for enhancing cyber security in fintech applications in India. In 2021 International Conference on Technological Advancements and Innovations (ICTAI) (pp. 274-279). IEEE. https://doi.org/10.1109/ICTAI53825.2021.9673277

Stewart, H., & Jürjens, J. (2018). Data security and consumer trust in FinTech innovation in Germany. Information & Computer Security, 26 (1), 109–128. https://doi.org/10.1108/ICS-06-2017-0039

Venkatesh, V., & Zhang, X. (2010). Unified theory of acceptance and use of technology: US vs. China. Journal of Global Information Technology Management, 13(1), 5-27. https://doi.org/10.1080/1097198X.2010.10856507

White.D, (2024) "Data Breach Outlook: Finance Surpasses Healthcare as Most Breached Industry in 2023" available at _2024 Data Breach Outlook | Cyber Risk | Kroll (accessed 7 February 2024)

Zhang, W., Siyal, S., Riaz, S., Ahmad, R., Hilmi, M. F., & Li, Z. (2023). Data Security, Customer Trust and Intention for Adoption of Fintech Services: An Empirical Analysis From Commercial Bank Users in Pakistan. SAGE Open, 13(3), 21582440231181388. https://doi.org/10.1177/21582440231181388