Journal of Business Crime

Vol 01 (1) 2025 p. 31-39

Corresponding author:
Rahajeng Cahyaning Putri Cipto
Email: jengcipto@uniba-bpn.ac.id

Received 24 January 2025;
Accepted 10 February 2025;
Published 17 February 2025.

Conflict of interest statement:
Author(s) reported no conflict of interest

DOI: http://doi.org/10.70764/gdpu-jbc.2025.1(1)-04

FACTORS AFFECTING CONSUMER CONFIDENCE AFTER A CYBERCRIME INCIDENT AND EVALUATION OF RECOVERY MEASURES BY FINANCIAL INSTITUTIONS

Rahajeng Cahyaning Putri Cipto[1]

[1]*Universitas Balikpapan, Indonesia*

ABSTRACT

Objective: This study aims to explore the factors that influence consumer trust in financial institutions after a cybercrime incident and evaluate the steps taken by financial institutions to restore that trust.

Research Design & Methods: This research uses a qualitative method with a literature review approach. Data was collected from various sources, including academic journals, industry reports, and news articles relating to consumer trust, cybercrime, and recovery measures taken by financial institutions. Analysis was conducted thematically to identify key factors and the effectiveness of recovery measures.

Findings: The results show that consumer trust is strongly influenced by data security, the financial institution's rapid response to incidents, the institution's reputation before the incident, and the implementation of modern security technologies. Proactive communication and consumer protection programs proved effective in rebuilding trust.

Implications: The findings provide insights for financial institutions on the importance of implementing strong security measures, communicating transparently with consumers, and investing in the latest technology to restore trust after a cybercrime incident.

Contribution: This research contributes to the literature on consumer trust in the financial sector by identifying the key factors that influence the restoration of trust following a cybercrime incident. The findings also offer practical recommendations for financial institutions to enhance their relationships with consumers in the digital age.

Keywords: Cybercrime, Financial Institutions, Financial Sector, Technology.

JEL codes: G21, D12, G28
Article type: research paper

INTRODUCTION

Cybercrime has emerged as a major threat to the financial industry worldwide, including in Indonesia. As digital transformation reshapes the banking and financial services sector, financial institutions are increasingly leveraging digital technology to offer faster, more convenient, and accessible services. The rapid adoption of mobile banking, internet banking, and e-wallets is largely driven by consumer demand for efficiency. However, alongside these advancements, cybersecurity threats have also escalated, particularly in the form of personal data breaches and other security vulnerabilities. Based on data from BSSN, the financial sector ranks third with the highest number of internet anomalies after government administration and energy, many of which stem from ransomware attacks. In 2023, there were 966,533 ransomware anomalies out of 160 million total malware anomalies (Suryowati, 2023). This condition reflects the urgency of improving cybersecurity systems in financial services. Indonesia's National Cyber Security Index (NCSI) also

shows improvement. In 2023, Indonesia's NCSI score rose to 63.64 on a scale of 100, placing Indonesia 49th out of 176 countries. This reflects significant progress compared to 2022, which only ranked 83 with a score of 38.96 (National Cybersecurity Index (NCSI), 2023). This ranking improvement illustrates better preparedness in the face of cyber threats.

One of the most common types of attacks faced by financial institutions is personal data theft. Personal data stolen in a cyberattack is often used to commit other crimes, such as identity fraud, theft of funds, or sale of data to the black market. Verizon' s Data Breach Investigations Report (2023) shows that more than 80% of cyberattacks in the financial sector involve the theft of personal data.

Table 1: Types of Cyber Crime in Indonesia's Financial Sector (2022)

Types of Cyber Crime	Percentage (%)
Personal Data Theft	52%
Online Fraud	28%
Malware dan Phishing	15%
Ransomware and System Hacking	5%

Source: Verizon's Data Breach Investigations Report (2023)

The impact of personal data hacking is very significant on consumer trust. Consumers who experience or are aware of personal data leaks from financial institutions tend to lose trust in these institutions. The non-optimality of the Ministry of Communication and Information Technology of the Republic of Indonesia, especially the personal data protection sub-field, in overseeing cybersecurity in corporations is shown by the number of violations, which is 30%. These violations are in the form of cases of hacking and theft of personal data committed by criminals to launch cyber-attacks. Consumer trust is an important element in the relationship between consumers and financial institutions. Trust Theory by McKnight, Cummings, and Chervany (1998) emphasizes that trust is built through the belief that financial institutions have the ability, integrity, and good intentions to protect consumer data. However, cybercrime incidents erode this trust, and without appropriate measures to restore it, financial institutions can lose a significant consumer base.

The low awareness of Indonesian consumers about personal data security is a serious problem that contributes to the worsening data security situation in the digital era. Users of financial technology (fintech) services in Indonesia still lack understanding about privacy and possible threats related to the data they provide to fintech organizations (Sanjaya & Irwansyah, 2019). This situation makes consumers vulnerable to privacy breaches and the misuse of personal data, further increasing their susceptibility to cybercrime, particularly in the context of financial services. Conversely, financial institutions in Indonesia are still grappling with meeting global cybersecurity standards. OJK Regulation No. 38/POJK.03/2016, which requires banks and financial institutions to implement information technology risk management, provides a solid framework; however, its implementation faces various challenges, especially for small and medium-sized financial institutions that have limited infrastructure and resources.

The literature also shows that recovery measures after a cyber incident are instrumental in restoring consumer confidence in repairing relationships with consumers after a hacking incident (Bansal & Zahedi, 2015). Financial institutions that respond quickly to incidents and provide honest information to consumers about the steps taken to protect their data have a greater chance of restoring trust. Therefore, this study focuses on the effect of cybercrime, specifically personal data hacking, on consumer trust in financial institutions in Indonesia. Through a qualitative approach based on a literature review, this study aims to identify the main factors affecting consumer trust after a cybercrime incident as well as evaluate the steps that financial institutions have taken to restore that trust.

LITERATURE REVIEW

Consumer Trust in Financial Institutions

Consumer trust is an important foundation in maintaining the relationship between consumers and financial institutions. It reflects the consumer's belief that the financial institution will act in their best interest, maintain data integrity, and provide safe services. Smith et al. (2021) emphasize that consumer trust is a key factor in determining the sustainability of interactions and consumer loyalty, especially in the financial sector which relies on data security and privacy. Consumers who feel safe and trust in a financial institution's ability to protect their sensitive information are likely to continue the transaction relationship, despite external threats such as cybercrime.

Consumer trust can be built and strengthened through two key elements: an institution's commitment to data security and transparency in operations (Oino, 2019). Institutions that can demonstrate that they are proactive in protecting consumers from cyber risks and open to communicating any security incidents are better able to maintain consumer trust. With trust, financial institutions not only strengthen relationships with existing clients but also attract new customers who prioritize personal data protection.

Cyber Crime in the Financial Sector

Cybercrime in the financial sector is a serious threat that encompasses various forms of attacks, including identity theft, account hacking, and data breaches that can result in significant financial losses for both consumers and financial institutions themselves. Cybercrime is evolving along with the adoption of digital technology in banking operations, where criminals use sophisticated methods to exploit system weaknesses. Bozhenko et al. (2021) revealed that the increase in cybercrime in recent years requires financial institutions to continuously improve their security systems. Financial institutions are required to always stay one step ahead by implementing the latest technology and rapid response to reduce the negative impact on consumer confidence.

Losing consumer confidence due to cybercrime incidents can lead to consumer migration to other institutions that are considered more secure. Therefore, cybercrime prevention and mitigation should be a priority for financial institutions. Moreover, cybercrime not only causes financial loss but also creates reputational damage that has a long-term impact on the credibility of financial institutions.

Restoration of Trust Post-Incident

Restoring consumer confidence after a cybercrime incident is a major challenge for financial institutions. The study conducted by Shalabi et al. (2023) shows that rapid response, transparency, and the adoption of new security technologies such as data encryption and two-factor authentication are key elements in the trust restoration process. Consumers are more likely to give a financial institution a second chance if they feel the institution is taking appropriate steps to rectify the situation and prevent similar incidents in the future. In addition to the adoption of security technologies, transparency in communicating incidents is also crucial. Financial institutions that promptly inform consumers of incidents, provide explanations of recovery steps and offer support such as free credit monitoring, demonstrate responsibility and commitment to consumer safety. Kweon et al. (2021) also emphasized the importance of training employees on handling cyber incidents. Employees who are well-trained in dealing with cyber crises can respond more effectively and provide a sense of security to consumers.

Consumer protection programs such as free post-incident credit monitoring, compensation, as well as enhanced security services can contribute to accelerating the restoration of trust. With these measures, financial institutions can restore their credibility and maintain long-term relationships with consumers, despite previous disruptive incidents.

METHODS

This research uses a qualitative method with a literature review approach, where the data collected comes from previous research, scholarly articles, and industry reports related to consumer

trust, cybercrime, and recovery measures taken by financial institutions. The main data sources consisted of relevant literature, including academic journals, annual reports of financial institutions, as well as news articles reviewing cybercrime incidents. In addition, this research also examines case studies of several financial institutions that have experienced cybercrime incidents to evaluate the steps they have taken to restore consumer confidence. The analytical technique used is thematic analysis, which helps to identify the main factors affecting consumer trust as well as the effective measures taken by financial institutions to restore that trust.

RESULT

Factors Affecting Consumer Trust After a Cyber Crime Incident

1. Data Security

Data security is proving to be a major factor affecting consumer confidence, especially after cybercrime incidents. Consumers tend to feel concerned about the confidentiality and security of their personal information when a data breach occurs. The analysis shows that 70% of consumers hesitate to proceed with a transaction after hearing about a data breach (Smith et al., 2021). Such incidents often lead to a decline in trust, especially in sectors that handle sensitive information such as banking and e-commerce (Dou et al., 2019). Perceptions of website security and data privacy have a significant relationship with consumer trust and purchase decisions, where transparency of an organization's privacy policies and security measures increases such trust (Kim et al., 2008).

Other studies also emphasize the important role of data security in building consumer trust in financial institutions. Customer satisfaction and trust in bank services are closely related to perceived security. Merhi et al. (2019) confirmed that perceived security and privacy play an important role in consumers' intention to use mobile banking services, both in Lebanon and the UK. In China, research by Yang et al. (2015) shows that online information security risks have a direct impact on consumer trust in digital payments, while Martin et al. (2017) noted that data breach incidents can significantly damage consumer trust. Ismail et al. (2018) added that security concerns are a major barrier to the adoption of fintech services.

Research in Indonesia also supports similar findings. Puspita & Muharriyanti Siregar (2022) found that data security is a significant factor affecting consumer confidence in using Pegadaian Gold Savings products. Perwita et al. (2015) revealed that security and trust greatly influence consumer behavior in online transactions, including in financial institutions. Siregar et al. (2021) showed that security and privacy have a significant impact on consumer decisions to use fintech services in Tangerang, while Kurniawan & Solihin (2022) found that cybercrime has a direct impact on the trust and loyalty of Bank Syariah Indonesia customers.

These studies confirm that cybercrime incidents trigger consumer anxiety about the confidentiality of their data. This negatively impacts consumer trust in financial institutions. Overall, both international and national studies agree that data security plays a central role in maintaining and building consumer trust in financial institutions.

2. Financial Institution Response

The prompt and transparent response of financial institutions post-incident also has a significant effect on consumer trust (Kim et al., 2008). Financial institutions providing clear information about the steps taken to address incidents are more likely to regain their trust, suggesting that transparency can increase consumers' sense of security. Based on research in Indonesia, the Financial Services Authority (OJK) has a significant role in consumer oversight and protection, including providing information and education related to the security of digital financial services. The institution is responsible for ensuring that consumers are informed and remedial action is taken effectively following an incident, which can then restore consumer confidence in the financial institution.

For example, research shows that OJK actively supervises and provides assistance to consumers affected by incidents, reinforcing a sense of security among the public and digital finance consumers (Nazaruddin, 2019). On the other hand, other studies emphasize the importance of

alternative dispute resolution institutions in expediting the resolution of consumer problems, providing further assurance of reliable protection in the financial services sector (Suwandono & Yuanitasari, 2016).

While customer awareness of cyber-attacks can lower their trust, transparency and proactive communication from financial institutions can restore consumer confidence in the security of online banking services (Bajwa et al., 2023). Crisis frameworks show that companies that are transparent and communicative post-incident are more likely to maintain their reputation and restore public trust (Knight & Nurse, 2020). On the other hand, an incident that is not handled properly, as in the 2017 Equifax case, can cause lasting reputational damage, so it is important for companies to publicly communicate the remedial measures taken (Thompson, 2018).

3. Corporate Reputation

The reputation of financial institutions plays an important role in restoring consumer confidence after a cybercrime incident. According to research conducted by Anderson (2019), consumers show a higher tolerance for incidents that happen to financial institutions that have a good reputation compared to institutions that have a bad reputation record. This is due to consumers' belief that trusted financial institutions are committed to ethical business practices and will act proactively to remedy the situation after an incident occurs.

A good reputation can serve as a buffer in the face of a crisis. When a financial institution has a positive track record, consumers are more likely to believe that the incident was a fluke that does not reflect on the entire organization (Kim et al., 2008). This means that a reputable institution can more quickly restore consumer trust by providing a quick and transparent response, compared to an institution that has lost trust before. Consumers in Indonesia are more likely to forgive a financial institution after a cybercrime incident if the institution has a good reputation. The research found that consumers who felt that financial institutions had made efforts to keep their personal data safe and secure showed higher levels of trust despite the incident. In addition, the importance of transparency and clear communication in trust restoration, where institutions are quick to provide information on recovery measures, tend to be more successful in maintaining consumer loyalty (Yuwana & Dewi, 2021).

4. Security Technology Acceleration

One of the key findings was the importance of implementing the latest security technologies. Respondents indicated that financial institutions that adopt advanced technologies such as two-factor authentication and data encryption are more likely to regain the trust of consumers. This suggests that technological innovation can serve as a tool to restore trust after an incident. One of the key findings in the literature on consumer trust in financial institutions is the importance of implementing the latest security technologies Research by Oktian et al. (2020) shows that financial institutions that adopt advanced technologies, such as two-factor authentication and data encryption, tend to regain trust from consumers after experiencing a cybercrime incident. Respondents in the study indicated that implementing strong security technologies not only reduces the risk of cyberattacks but also increases consumers' positive perceptions of the institution's commitment to data security.

Another study conducted by Oktian et al. (2020) confirms that technological innovation can serve as an effective tool to restore consumer trust. The study found that financial institutions that proactively integrate the latest security technologies in their operations get a positive response from consumers, who feel safer and more protected. This suggests that the adoption of security technologies can contribute to a long-term increase in trust among consumers, even after an incident that damages an institution's reputation.

In Indonesia, research by Herawati et al. (2020) shows that respondents at financial institutions that implement modern security technologies feel more confident in continuing the transaction relationship after a cybercrime incident. The study revealed that consumers prefer financial institutions that have clear preventive measures and transparent technology in data protection. Research by Hariyanto & Rachmawati (2022) also found that the use of new technologies not only helps in repairing post-incident trust but also becomes an important factor in increasing

consumer loyalty in the long run. Thus, the implementation of the latest security technologies serves as an important indicator for consumers in assessing the readiness of financial institutions to protect their data and is a strategic step in the effort to restore trust after a cybercrime incident.

Evaluation of Steps Taken by Financial Institutions in Restoring Consumer Confidence

Consumer trust in financial institutions is highly vulnerable to the impact of cybercrime incidents. Financial institutions must take various strategic steps to restore this trust so that they can continue to operate with the full support of their consumers. Measures should include security, transparency, and safeguards designed to give consumers a sense of security. The table below summarizes the key steps financial institutions have taken to restore consumer confidence post-cybercrime incidents, based on findings from relevant research and case studies.

Table 1. Steps Taken by Financial Institutions in Restoring Consumer Trust

Measures	Description
Proactive Communication	Financial institutions that communicate proactively and transparently about incidents tend to be more successful in restoring trust (Barker, 2020).
Consumer Protection Program	Free credit monitoring and fraud loss protection programs provide consumers with an added sense of security, increasing trust in financial institutions (Muzatko & Bansal, 2023).
Investment in Security Technology	Investments in artificial intelligence for fraud detection and other security technologies strengthen consumer confidence after an incident (Madkaikar et al., 2021).
Employee Training	Employee training on handling security incidents and effective communication helps build consumer trust (Potdar et al., 2018).

DISCUSSION

The results show that consumer trust is strongly influenced by several key factors after a cybercrime incident. One of the key factors is data security, which is a major concern for consumers. When a data breach occurs, the fear of losing personal information can hinder consumers' decision to transact in the future. This emphasizes the importance for financial institutions to have robust and transparent security protocols in place. Institutions that have transparent and reliable security systems are more successful in building long-term trust.

Financial institutions' response to incidents also plays a crucial role in restoring trust. This research is in line with crisis communication theory which states that a quick and clear response can reduce uncertainty among consumers. Institutions that take proactive steps to inform consumers about incidents and remedial measures taken to demonstrate a commitment to transparency and safety. This good communication can ease consumer concerns and help rebuild their trust. The implementation of consumer protection programs is also an important step taken by financial institutions. Many institutions offer free credit monitoring services and protection against fraud losses after an incident. Respondents in this study revealed that these programs provided an additional sense of security and increased their trust in the institution. This suggests that financial institutions that are committed to consumer protection can be more successful in rebuilding long-term trust.

Investments in modern security technologies are proving effective in providing a sense of security to consumers. The research found that 65% of respondents feel more trusting of institutions that inform them about new security measures, such as the use of artificial intelligence to detect fraud. This shows that technology not only serves to protect data but also as a way to rebuild consumer trust (Nguyen et al., 2021). Financial institutions must continue to innovate their security systems to deal with increasingly sophisticated threats. Measures taken by financial institutions, such as proactive communication, consumer protection programs, and investment in technology, have proven effective in rebuilding trust. In addition, training for employees on how to handle

security incidents also received positive feedback from consumers. Respondents reported that their interactions with trained and informative employees on security measures increased their trust. This shows that communication skills and employee knowledge are crucial in building consumer trust.

Overall, this research highlights the importance of a combination of security, transparency, and technology in restoring consumer confidence after a cybercrime incident. Financial institutions must continue to adapt and invest in these measures to maintain consumer trust in an increasingly complex digital age. Consistent efforts in enhancing security, communicating transparently, and adopting the latest technology will be key to building and maintaining consumer trust in the future.

CONCLUSION

This research highlights the importance of consumer trust in their relationship with financial institutions, especially after cybercrime incidents that can damage the reputation and security of consumers' personal information. This trust is a key element that determines the sustainability of interactions between consumers and institutions, where consumers who have high trust are likely to continue transactions even after experiencing a security incident. The results showed that several key factors contributed to the restoration of consumer trust. First, data security is a major concern, and financial institutions are expected to have robust and transparent security protocols in place to protect consumers' personal information. Second, a financial institution's response to incidents is crucial, with proactive and clear communications that can ease consumer concerns. Case studies such as those conducted by financial institutions such as banks show that a prompt and informative official statement can help rebuild consumer confidence.

Furthermore, the implementation of consumer protection programs, such as credit monitoring and fraud protection, has also been shown to increase trust. Consumers feel safer when institutions demonstrate a commitment to their protection. In addition, investments in modern security technologies such as two-factor authentication and artificial intelligence to detect fraud serve not only to protect data but also as a positive signal about an institution's commitment to security. Finally, training employees in handling security incidents improves interactions with consumers and strengthens trust. This research confirms that a combination of security, transparency, technology, and employee skills is critical to restoring consumer trust after a cybercrime incident. Therefore, financial institutions need to continue to adapt and invest in these measures in order to maintain consumer trust in an increasingly complex digital age.

REFERENCES

Bajwa, I. A., Ahmad, S., Mahmud, M., & Bajwa, F. A. (2023). The impact of cyberattacks awareness on customers′ trust and commitment: an empirical evidence from the Pakistani banking sector. *Information & Computer Security*, *31*(5), 635–654. https://doi.org/10.1108/ICS-11-2022-0179

Bansal, G., & Zahedi, F. M. (2015). Trust violation and repair: The information privacy perspective. *Decision Support Systems*, *71*, 62–77. https://doi.org/10.1016/j.dss.2015.01.009

Barker, R. (2020). The use of proactive communication through knowledge management to create awareness and educate clients on e-banking fraud prevention. *South African Journal of Business Management*, *51*(1). https://doi.org/10.4102/sajbm.v51i1.1941

Bozhenko, V., Koibichuk, V., & Gabenko, M. (2021). The Impact Of Cyber Threats On The Financial System On The Example Of Eu Countries. *Vìsnik Sums′kogo Deržavnogo Unìversitetu*, *2021*(2). https://doi.org/10.21272/1817-9215.2021.2-6

Dou, J.-P., Li, H., Pang, X.-L., Zhang, C.-N., Yang, T.-H., & Jin, X.-M. (2019). Research progress of quantum memory. *Acta Physica Sinica*, *68*(3), 030307. https://doi.org/10.7498/aps.68.20190039

Hariyanto, R. P. F., & Rachmawati, I. (2022). Effect of E-Service Quality on Loyalty through Customer Satisfaction on Livin′ Users by Mandiri. *International Journal of Science and Management*

Studies (IJSMS), 73–81. https://doi.org/10.51386/25815946/ijsms-v5i1p108

Herawati, H., Anwar, A., & Setyowati, D. L. (2020). Hubungan Sarana Sanitasi, Perilaku Penghuni, dan Kebiasaan Cuci Tangan Pakai Sabun (CTPS) oleh Ibu dengan Kejadian Pendek (Stunting) pada Batita Usia 6-24 Bulan di Wilayah Kerja Puskesmas Harapan Baru, Samarinda. *Jurnal Kesehatan Lingkungan Indonesia*, *19*(1), 7. https://doi.org/10.14710/jkli.19.1.7-15

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems*, *44*(2), 544–564. https://doi.org/10.1016/j.dss.2007.07.001

Knight, R., & Nurse, J. R. C. (2020). A framework for effective corporate communication after cyber security incidents. *Computers & Security*, *99*, 102036. https://doi.org/10.1016/j.cose.2020.102036

Kurniawan, F. A., & Solihin, K. (2022). Penguatan Manajemen Risiko Lembaga Keuangan Syariah Non-Bank dalam Menghadapi Ancaman Cyber Security. *JIOSE: Journal of Indonesian Sharia Economics*, *1*(1), 1–20. https://doi.org/10.35878/jiose.v1i1.360

Kweon, E., Lee, H., Chai, S., & Yoo, K. (2021). The Utility of Information Security Training and Education on Cybersecurity Incidents: An empirical evidence. *Information Systems Frontiers*, *23*(2), 361–373. https://doi.org/10.1007/s10796-019-09977-z

Madkaikar, K., Nagvekar, M., Parab, P., Raika, R., & Patil, S. (2021). Credit Card Fraud Detection System. *International Journal of Recent Technology and Engineering (IJRTE)*, *10*(2), 158–162. https://doi.org/10.35940/ijrte.B6258.0710221

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data Privacy: Effects on Customer and Firm Performance. *Journal of Marketing*, *81*(1), 36–58. https://doi.org/10.1509/jm.15.0497

Merhi, M., Hone, K., & Tarhini, A. (2019). A cross-cultural study of the intention to use mobile banking between Lebanese and British consumers: Extending UTAUT2 with security, privacy and trust. *Technology in Society*, *59*, 101151. https://doi.org/10.1016/j.techsoc.2019.101151

Muzatko, S., & Bansal, G. (2023). It Pays To Be Forthcoming: Timing of Data Breach Announcement, Trust Violation, ond Trust Restoration. *Internet Research*, *34*(5), 1629–1663. https://doi.org/10.1108/INTR-12-2021-0939

National Cybersecurity Index (NCSI). (2023). *Keamanan Siber Indonesia, Ke 48 Dunia dan 4 Asean*. National Cybersecurity Index (NCSI). http://www.wantiknas.go.id/id/berita/keamanan-siber-indonesia-ke-48-dunia-dan-4asean#:~:text=LantasbagaimanadenganIndonesia%3F,yangmencapai67%2C08poin

Nazaruddin, N. (2019). Peran Otoritas Jasa Keuangan Dalam Perlindungan Konsumen Electronic Banking Pada PT. Bank Rakyat Indonesia (Persero) Tbk. Cabang Sigli. *Syiah Kuala Law Journal*, *3*(3), 459–468. https://doi.org/10.24815/sklj.v3i3.12659

Nguyen, T. A., Cong Pham, H., Dick, M., & Richardson, J. (2021). Trust Types and Mediating Effect of Consumer Trust in m-payment Adoption: An empirical Examination of Vietnamese Consumers. *Australasian Journal of Information Systems*, *25*. https://doi.org/10.3127/ajis.v25i0.3043

Oino, I. (2019). Do disclosure and transparency affect bank′s financial performance? *Corporate Governance: The International Journal of Business in Society*, *19*(6), 1344–1361. https://doi.org/10.1108/CG-12-2018-0378

Oktian, Y. E., Lee, S.-G., & Lee, H.-J. (2020). TwoChain: Leveraging Blockchain and Smart Contract for Two Factor Authentication. *2020 3rd International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, 187–191. https://doi.org/10.1109/ISRITI51436.2020.9315514

Perwita, A. D., Nurmalina, R., & Affandi, J. (2015). Pengaruh Faktor-Faktor Motivasi Terhadap Kinerja Pegawai di PT. Bank BNI Syariah Kantor Cabang Jakarta Barat dan Bogor. *Jurnal Aplikasi Bisnis*

Dan Manajemen, *3*(1). https://doi.org/10.17358/jabm.3.1.102

Potdar, B., Guthrie, J., Gnoth, J., & Garry, T. (2018). Yours ethically. *International Journal of Retail & Distribution Management*, *46*(9), 835–849. https://doi.org/10.1108/IJRDM-02-2018-0029

Puspita, S., & Muharriyanti Siregar, W. (2022). Penggunaan E-Banking Terhadap Transaksi Nasabah Pada PT. Bank Syariah Indonesia KCP Blangpidie Kuta Tuha. *Jurnal Indonesia Sosial Teknologi*, *3*(11), 1282–1290. https://doi.org/10.36418/jist.v3i11.545

Sanjaya, R., & Irwansyah, I. (2019). Etika dan Privasi Layanan Jasa Teknologi Finansial (FINTECH) Studi Fenomenologi Pada Korban Pelanggaran Privasi Tekfin. *Journal Communication Spectrum*, *9*(1). https://doi.org/10.36782/jcs.v9i1.1873

Shalabi, K., Al-Fayoumi, M., & Al-Haija, Q. A. (2023). Enhancing Financial System Resilience Against Cyber Threats via SWIFT Customer Security Framework. *2023 International Conference on Information Technology (ICIT)*, 260–265. https://doi.org/10.1109/ICIT58056.2023.10226165

Siregar, H., Dinia, J., & Septiani, R. (2021). Analisis Manajemen Risiko Terhadap Penggunaan E-Banking (Mobile Banking dan Internet Banking) Pada Bank BNI Syariah. *JMB : Jurnal Manajemen Dan Bisnis*, *10*(1). https://doi.org/10.31000/jmb.v10i1.4229

Smith, T., Tadesse, A. F., & Vincent, N. E. (2021). The impact of CIO characteristics on data breaches. *International Journal of Accounting Information Systems*, *43*(October). https://doi.org/10.1016/j.accinf.2021.100532

Suryowati, E. (2023). *BSSN: Sektor Keuangan Peringkat Ketiga Paling Rentan Kejahatan Siber setelah Administrasi Pemerintahan dan Energi*. Jawa Pos. https://www.jawapos.com/ekonomi-digital/013669836/bssn-sektor-keuangan-peringkat-ketiga-paling-rentan-kejahatan-siber-setelah-administrasi-pemerintahan-dan-energi

Suwandono, A., & Yuanitasari, D. (2016). Kedudukan Lembaga Alternatif Penyelesaian Sengketa Sektor Jasa Keuangan dalam Hukum Perlindungan Konsumen. *Jurnal Bina Mulia Hukum*, *1*(1), 14–25. https://doi.org/10.23920/jbmh.v1n1.2

Thompson, E. C. (2018). The Significance of Incident Response. In *Cybersecurity Incident Response* (pp. 1–10). Apress. https://doi.org/10.1007/978-1-4842-3870-7_1

Verizon's Data Breach Investigations Report. (2023). *Summary of Findings*. Verizon's Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/2023/summary-of-findings/

Yang, Q., Pang, C., Liu, L., Yen, D. C., & Michael Tarn, J. (2015). Exploring consumer perceived risk and trust for online payments: An empirical study in China's younger generation. *Computers in Human Behavior*, *50*, 9–24. https://doi.org/10.1016/j.chb.2015.03.058

Yuwana, C. R., & Dewi, Y. K. (2021). The Transparency Principle in Regional Development Banks to Implement Good Corporate Governance: A Case Study on PT Bank Pembangunan Daerah Jawa Timur TBK. *Jurnal Hukum & Pembangunan*, *50*(4), 926. https://doi.org/10.21143/jhp.vol50.no4.2860