OPEN ACCESS

International Review of Social and Cultural Studies | Vol. 1 No. 1 (2025)

Literature Review

Analysis of Bank Syariah Indonesia (BSI) Customer Data Hacking Using Empirical Theory

Nur Shinta
Management Study Program, Universitas Pelita Bangsa, Indonesia
Email: shintanur289@gmail.com

Received:	Revised:	Accepted:	Online:
December 07, 2024	December 27, 2024	January 11, 2025	January 16, 2025

Abstract
Technological advances bring convenience in various activities, one of which is in the banking sector, where transactions can now be carried out without the need to come directly to the bank. However, this progress also presents challenges, one of which is for Islamic banking which faces cybersecurity threats, as experienced by Bank Syariah Indonesia (BSI), which was hit by a ransomware attack that caused data leakage of 15 million customers and employees and transaction disruption for almost a week. This study aims to analyze the efforts made by BSI in handling cyber threats and protecting customer data. The method used is a literature study by collecting data from various sources, such as journals, books, and research reports, and analyzing them using empirical theory. The results show that BSI improves its security system through regular training, adopts advanced security technology, conducts periodic security audits, establishes an incident response team, communicates transparently with customers, and cooperates with law enforcement to catch hackers. This research provides an overview of the importance of improving security systems and preventive measures to overcome cyber threats in the banking world.

Keywords: Ransomware, Bank Syariah Indonesia, Empirical Theory, Cyber Security, Data Leakage

1. Introduction

In an increasingly advanced digital era, Indonesia's Islamic banking sector faces new challenges in the form of cyber threats (Azarine, Agdelia, 2024). One of the incidents that stole the spotlight was the hacking of Bank Syariah Indonesia (BSI) customer data. This case aroused the attention of various parties because it involved personal data that was very sensitive and crucial for customers so that this problem became a very worrying issue in this digital era (Rafie et al., 2024). The leaked data includes identity information, financial transactions, and passwords that should be kept confidential (Wang et al., 2024).

Customer data security is a top priority for financial institutions, including Islamic banks. This hack not only threatens data integrity, but also customer trust in the Islamic banking system (Fazlurrohman et al., 2024). In this context, analyzing the BSI customer data hacking incident is important to understand the modus operandi, the impact, and the mitigation measures taken by the bank.

In early 2023, BSI experienced a massive hack that resulted in a leak of sensitive customer data. BSI's security system initially detected suspicious activity indicating an unauthorized attempt to access customer data. Hackers managed to access the system through a phishing attack that successfully stole the login credentials of bank staff. After gaining access, the hacker used a brute force attack to exploit existing security holes.

According to Teguh Aprianto, a digital security consultant, user data and passwords are suspected to have been leaked and stolen. According to Teguh, the total data stolen is around 1.5 TB of personal data (Tim Redaksi, 2023). Among them were 15 million user data and passwords for internal access and services. BSI's response after finding out that their security system was attacked was to immediately close access to the compromised system to prevent the hackers from taking further action.

This article will analyze the hacking of BSI's customer data using an empirical theory approach. By using an empirical approach and literature study, this research will dig deeper into how the hack occurred, and how Bank Syariah Indonesi (BSI) responded to this incident to protect its customers and restore public trust in BSI.

2. Methods

2.1. Methods

This research leads to the literature study method. Literature study is a theoretical study, references and other scientific literature related to culture, values and norms that develop in the social study being researched. According to Syaibani (2012), literature study is all efforts made by researchers to obtain information that is in accordance with the topic of their research (Azizah, A., & Purwoko, 2017). Researchers outline explanations from various studies such as Wahjosumidjo (1987), Moedjiono (2002) and Asmarazisa (2016). The research is very relevant to the discussion points of various articles. Researchers collect reading material from journals, books and research reports. Then accommodate and combine and conclude from the results of the review of various existing sources.

2.2. Empirical Theory in Cybersecurity

Empirical theory in the analysis of the Bank Syariah Indonesia (BSI) data hack emphasizes the importance of data and tangible evidence in understanding and mitigating security threats. This theory involves collecting, analyzing, and interpreting data to identify patterns and trends that can help in formulating effective security strategies. In the case of the BSI data hack, the empirical approach involved analyzing the hacking incident, the techniques used by the hackers, and the impact on customers and the institution.

3. Results and Discussion

In early 2023, BSI experienced a major hack that resulted in a leak of sensitive customer data. The hack was discovered after BSI's security system detected suspicious activity indicating an unauthorized attempt to access customer data. This led to hackers successfully accessing the system through a phishing attack and successfully stealing the login credentials of bank staff. After gaining access, the hacker used a brute force attack to exploit existing security holes.

The hack was certainly very detrimental to both the bank and the customer. This also shows that there are imperfections in the system used by Bank Syariah Indonesia (BSI), causing the system to be hacked. The mistake is very fatal because it allows customers to experience huge losses, not only physical or material losses (money) but also non-material (personal data). If personal data is leaked into the wrong hands, it can be traded for personal interests, such as data falsification, online loans (pinjol), online gambling and transfer of personal assets.

The hacking techniques used to steal Bank Syariah Indonesia (BSI) customer data used in the case are as follows:

1) Phishing

Phishing involves sending fake emails or messages to BSI staff with fake links directing them to fake login pages to trick users into providing sensitive information such as account numbers, PINs and passwords.

2) Brute Force

After obtaining credentials, hackers use brute force attacks to access internal systems that are less well protected. Brute Force is a hacking technique where the hacker tries all passwords or PINs until they find the correct one. This method can be very effective if the credentials used by the user are simple or short enough to be easily cracked.

3.1. Impact of Hacking

The hacking that occurred at Bank Syariah Indonesia (BSI) can have significant impacts, both in terms of financial, operational and reputation. The following is a detailed explanation of these impacts:

1. Financial Loss

a) System recovery cost: BSI had to spend a lot of money to improve and strengthen their security system, including hiring cybersecurity experts and purchasing new software and other hardware.

b) Customer Compensation: BSI Bank compensates customers affected by the hack, especially if they lose funds and BSI also offers special discounts or promotions for BSI users in purchasing products or food.

2. Reputation Loss

a) Loss of Customer Trust: From this incident, customers' trust in BSI dropped drastically, which negatively impacted the bank's reputation and they moved their funds to other banks.

b) Public Image: News of the hacking could damage BSI's image in the eyes of the public and reduce the credibility of prospective customers and customers, causing hesitation among potential new customers and the possibility that most existing customers will transfer some or all of their assets to other banks.

3. Operational Disruption

System downtime, this can cause BSIs to face operational disruptions when they have to identify and close security gaps and recover lost data and disrupt customer transactions.

4. Legal and Regulatory Issues

a) Sanctions from Regulators: The Financial Services Authority (OJK) may impose sanctions on BSI if it is found that the bank is not complying with the required data security standards.

b) Lawsuits: Aggrieved customers can file lawsuits against BSI, such as demanding compensation for their losses.

5. Customer Impact

Leaked customer personal data such as names, addresses, identity numbers, phone numbers, and financial information can be stolen and misused by irresponsible parties or third parties, causing them financial losses and legal problems.

3.2. Empirical Analysis

3.2.1. Data Collection

The data collected includes hacking incident reports, system activity logs, and customer loss reports. This data was analyzed to identify patterns and security holes exploited by hackers.

Table 1. Hacking Incident Reports Through Mass Media News

News Media	Article/Journal	Release Date
Kompas.com	BSI Hacked by Hackers Called a Trial and Challenge for Indonesian Banking	17 Mei 2023
CNNIndonesia.com	Alleged BSI Bank Hit by Ransomware Attack, Experts Reveal the Characteristics.	10 Mei 2023
Liputan6.com	BSI Suspected of Ransomware, Expert: Antivirus alone may not be able to fight	10 Mei 2023
Bisnis.Tempo.com	BSI Hit by Ransomware Attack, Customers Claim Hundreds of Millions in Losses.	13 Mei 2023

Table 1 shows various reports from several online news media that raised the issue of BSI ransomware or data hacking (Maulana, N., Laurens, T., Faiz, D, H, A., & Patrianti, 2024). It is known that the hack occurred on May 8, 2023 and for almost a week BSI transactions were paralyzed. BSI itself said that the problem was a network error (Azarine, A., 2024). This resulted in the obstruction of the customer transaction process. However, after further investigation it turned out that BSI experienced Ransomware or data hacking.

Table 2. The losses of Bank Syariah Indonesia (BSI) and Its Customers

No	Indicator	Loss
1	Customer/Employee Data	15 million
2	Data Leak	1.5 TB
3	Material Loss	(-)
4	Non-material Loss	(-)
5	Compensation	Article 83, paragraph 5, amounts to 20 million euros or IDR 320 billion

Table 2 shows that around 15 million customer and employee data were hacked, totaling approximately 1.5 TB of leaked data. This resulted in non-material losses due to data that could potentially be misused or sold. So far, it is unclear whether there have been any material losses. Based on Article 83, paragraph 5 of the law, Bank Syariah Indonesia is required to pay compensation amounting to 20 million euros or approximately IDR 320 billion.

3.2.2. Patterns and Trends

Empirical analysis reveals that phishing attacks increase significantly in the months before a major incident occurs. Additionally, weaknesses in two-factor authentication (2FA) were identified as one of the main causes of successful brute force attacks.

3.3. Mitigation Efforts by Bank Syariah Indonesia

3.3.1. Security System Enhancement

To enhance cybersecurity, Bank Syariah Indonesia (BSI) prioritizes building awareness among both staff and customers about the growing risks associated with cyber threats. Regular training sessions are organized to educate staff on identifying phishing attacks, secure password practices, and other basic cybersecurity measures. For customers, BSI provides educational resources on how to recognize potential scams and implement safe online banking practices. By fostering a security-conscious environment, the bank ensures that both employees and customers can help safeguard sensitive data and prevent potential security breaches.

3.3.2. Implementation of Stronger Security Technologies

BSI has adopted more advanced technologies to strengthen its defense systems against cyber-attacks. Multi-factor authentication (MFA) is now mandatory for accessing online banking services, providing an extra layer of security by requiring multiple forms of verification from users. Additionally, the bank uses end-to-end encryption to protect customer data during transmission, ensuring that even if intercepted, the information cannot be read or altered. Intrusion detection systems (IDS) are also in place to monitor and detect unusual activities within the bank’s network, allowing for real-time alerts and a quick response to potential security breaches.

3.3.3. Periodic Security Investigations and Audits

BSI conducts regular security investigations and audits to proactively identify vulnerabilities within their systems. These audits involve reviewing network security protocols, software updates, and physical security measures to ensure that all aspects of the system are secure. The bank works with external cybersecurity experts to perform penetration testing, simulating cyber-attacks to test the resilience of its security infrastructure. By regularly evaluating security measures, BSI can address potential weaknesses before hackers have the opportunity to exploit them.

3.3.4. Rapid Incident Response

In the event of a cyber-attack, BSI has established a dedicated incident response team (IRT) that is trained to respond quickly and efficiently to minimize the impact of a breach. The IRT's primary responsibilities include identifying the source of the attack, isolating affected systems, and implementing strategies to contain and mitigate damage. The team works around the clock to restore normal operations as quickly as possible while ensuring that all data is recovered and security gaps are addressed. This rapid response minimizes disruption to banking services and reduces the potential for further damage.

3.3.5. Transparent Communication with Customers

BSI is committed to maintaining transparency with its customers during cybersecurity incidents. In the event of a data breach, the bank immediately informs affected customers about the nature of the incident, the measures being taken to address the situation, and how their data is being protected. To help customers protect their identities, BSI offers complimentary credit monitoring services and security consulting to assist in mitigating the potential impacts of the breach. This open communication helps to maintain trust between the bank and its customers, showing a commitment to resolving the issue and protecting customer interests.

3.3.6. Cooperation with Law Enforcement

BSI collaborates with local and international law enforcement agencies to investigate and apprehend hackers involved in cyber-attacks. The bank provides relevant information, such as IP addresses, hacking methods, and attack patterns, to help authorities track down the perpetrators. By working closely with law enforcement, BSI aims to ensure that cybercriminals are held accountable for their actions and that similar attacks can be prevented in the future. Additionally, BSI supports the legal process by providing necessary evidence for prosecution and working to enhance the overall security environment in the banking sector.

4. Conclusion

The hacking of Bank Syariah Indonesia (BSI), which resulted in the breach of 15 million customer and employee data records, underscores the importance of adopting an empirical approach to combat cybersecurity threats. By systematically collecting and analyzing data, BSI can identify attack patterns, assess vulnerabilities, and develop strategies to strengthen its security measures. The bank's response to the ransomware attack, which involved enhancing cybersecurity awareness, implementing advanced security technologies like multi-factor authentication and data encryption, and conducting regular security audits, illustrates the effectiveness of data-driven decision-making in addressing emerging threats. This approach allows BSI to stay ahead of potential attacks, adapt its defenses, and continuously refine its security posture based on the insights gained from past incidents.

Additionally, BSI's proactive measures, such as providing training to staff and customers and establishing a rapid incident response team, emphasize the importance of both internal and external collaboration in tackling cybersecurity risks. Regular training ensures that all stakeholders are aware of the latest threats and equipped to recognize and respond to potential breaches. Transparent communication with customers, coupled with the cooperation with law enforcement, further enhances BSI's ability to address cybersecurity challenges. By combining technological advancements, comprehensive training, and data-driven insights, BSI can safeguard its systems and protect its customers from future data breaches, ensuring long-term security in an increasingly complex digital landscape.

5. References

Asmarazisa, D. (2016). Pengaruh motivasi dan kepemimpinan terhadap kinerja karyawan pada pt. Bank BTN Batam. *Jurnal Dimensi*, *5*(2).

Azarine, Agdelia, M. (2024). *Bank BSI Pasca Serangan Siber: Mengungkap Potensi Kompensasi Bagi Nasabah*. LK2 FHUI.

Azizah, Ainul., & Purwoko, B. (2017). *Studi Kepustakaan Mengenai Landasan Teori dan Praktik Konseling Naratif*. Universitas Negeri Surabaya.

Fazlurrohman, M. A., Nita, S., & Aminanto, M. E. (2024). omparative Studies On Trends And Strategies For Combating Cybercrime Between Indonesia And Developed Countries. *Policy, Law, Notary and Regulatory Issues*, *3*(4), 498–515. https://doi.org/10.55047/polri.v3i4.1512

Maulana, Nicky., Laurens, Tito., Faiz, Didar, Hadrian, Afzal., & Patrianti, T. (2024). Manajemen Krisis PT. BSI Tbk Pasca Peretasan Data Nasabah. *INNOVATIVE: Journal of Social Science Research*, *4*(1), 8247.

Moedjiono, I. (2002). *Kepemimpinan dan keorganisasian*. UII Press.

Rafie, P. A., Merta, M. M., & Junaidi, J. (2024). The Enforcement Of Cybercrime Law Within The Legal System Of Indonesia. *Journal of Humanities, Social Sciences and Business (JHSSB)*, *3*(3), 594–600. https://doi.org/10.55047/jhssb.v3i3.1038

Syaibani, R. (2012). Studi Kepustakaan. *Medan: Universitas Sumatera Utara*.

Tim Redaksi. (2023). *Kominfo Klarifikasi Soal Dugaan Bocoran Data BSI yang Beredar*. Cnnindonesia.Com.

Wahjosumidjo, W. (1987). Kepemimpinan Dan Motivasi. *Jakarta: Ghalia Indonesia*.

Wang, S., Asif, M., Shahzad, M. F., & Ashfaq, M. (2024). Data privacy and cybersecurity challenges in the digital transformation of the banking sector. *Computers and Security*, *147*. https://doi.org/10.1016/j.cose.2024.104051