**AL-AMWAL: JURNAL EKONOMI DAN PERBANKAN SYARI'AH (2023) Vol 15 (1) : 86-100**
DOI: 10.24235/amwal.v%vi%i.14124.

Al-Amwal: Jurnal Ekonomi dan Perbankan Syariah
ISSN: 2303-1573 e-ISSN: 2527-3876
Homepage: https://www.syekhnurjati.ac.id/jurnal/index.php/amwal
email: jurnalalamwal@syekhnurjati.ac.id

# Mitigating IT Risk of Bank Syariah Indonesia: A Study of Cyber Attack on May 8, 2023

**Rini Fitriani,[1] Rokhmat Subagiyo,[2] Binti Nur Asiyah[2]**

**UIN Sayyid Ali Rahmatullah Tulungagung[123]**

E-mail: *fitrianirini@gmail.com, rokhmatsubagyo@uinsatu.ac.id, binti.advan@gmail.com*

***Abstract***

*The rapid development of information technology in Indonesia cannot be ignored. Technological updates in all fields must be carried out, including in the banking sector, especially in Islamic banking. Customers demand convenience, smoothness, security, and flexibility in digital banking services. Bank Syariah Indonesia (BSI) is the largest Islamic bank in Indonesia. On May 8, 2023, BSI experienced an attack on its information system, and the hashtag Bank Syariah Indonesia (BSI) became a trending topic for several days after the incident. The paralysis of BSI's information system for several days caused customers to be unable to perform banking transactions, resulting in significant losses for them. The purpose of this study is to identify the efforts of information technology mitigation carried out by BSI regarding the incident. This research adopts a qualitative approach and uses primary data. The primary data is sourced from Twitter, collected from May 4 to May 11, 2023, and reliable websites. The Twitter data is processed and analyzed using Maxqda 2020 and Gephi version 0.9.6 for Windows 10 64-bit software. The conclusion of this study is that BSI's efforts in information technology mitigation are still slow because the bank appears to lack awareness or a full understanding of the importance of information technology risk mitigation.*

***Keywords****: Mitigation risk, Risk Management, Information technology.*

**Abstrak**

Perkembangan teknologi informasi yang sangat pesat di Indonesia tidak dapat dikesampingkan. Pembaharuan teknologi dalam semua bidang harus dilakukan tidak terkecuali dalam dunia perbankan, khususnya perbankan syariah. Nasabah membutuhkan kemudahan, kelancaran, keamanan, dan fleksibilitas dalam layanan digital perbankan. Bank Syariah Indonesia (BSI) merupakan bank syariah terbesar di Indonesia. Pada tanggal 8 Mei 2023 BSI mendapatkan serangan terhadap sistem informasinya dan hashtag Bank Syariah Indonesia (BSI) menjadi trending topic pada beberapa hari setelah tanggal tersebut. Lumpuhnya sistem informasi pengoperasian BSI pada beberapa hari menyebabkan nasabah tidak dapat melakukan transaksi perbankan. Nasabah sangat dirugikan karena kejadian ini. Tujuan dari penelitian ini adalah untuk mengetahui upaya mitigasi teknologi informasi yang dilakukan oleh BSI terkait kejadian tersebut. Penelitian ini menggunakan pendekatan kualitatif dengan menggunakan data primer. Data primer yang digunakan bersumber dari Twitter yang diambil pada tanggal 4 sampai dengan 11 Mei 2023 dan website yang dapat dipercaya. Data dari Twitter diolah dan dianalisis dengan menggunakan bantuan software Maxqda 2020 dan Gephi versi 0.9.6 for windows 10 64 bit. Kesimpulan dari penelitian ini yaitu upaya mitigasi teknologi informasi yang dilakukan oleh BSI masih lambat karena BSI kurang menyadari atau tidak sepenuhnya memahami pentingnya mitigasi risiko teknologi informasi..
**Kata kunci**: *Mitigasi risiko, Manajemen risiko, teknologi informasi*

## INTRODUCTION

The demand for information and communication technology services is growing rapidly to meet various service needs, ranging from e-commerce and work technology to online gaming and streaming. Information and communication technology plays a crucial role in maintaining the continuity of businesses, jobs, education, services, entertainment, and communication. Over the five-year period from 2017 to 2021, the development of information and communication technology in Indonesia also experienced a positive trend (Direktorat Statistik Keuangan, Teknologi Informasi, 2021). With the rapid development of information technology in Indonesia, technological advancements in all fields must be pursued, including in the banking sector, particularly in Islamic banking.

The development of technology cannot be halted as it is directly proportional to the human desire for comfort and convenience in every aspect of their activities (Kholis, 2020). In the banking industry, keeping up with the advancements of the era and digital technology is a necessity. This is due to the constantly changing business ecosystem and customers' demand for convenience, efficiency, security, and flexibility in digital banking services. As a result, banks no longer require physical branches and can transform traditional banking services into digital forms (Laucereno, 2022). Another study states that effective utilization of information technology and adequate funding availability will support the growth and sustainability of the Islamic banking industry. This will help the industry become more stable, play a role in economic recovery, and make a significant contribution to the country's economy (Apriyanti, 2018).

Digital banking services based on information technology require a significant cost. Apart from the inadequate infrastructure conditions, this is also due to Indonesia's unique and vast geographical aspects. Both conventional and Islamic banking and financial institutions have been heavily influenced by the development of products in information technology, to the point where they can no longer function without it. This industry requires product development in the field of information technology to be able to offer services to its customers (Wardiana, 2002). All banks, especially Islamic banks, that fail to keep up with the advancements in information technology will be left behind and unable to compete with their competitors.

The use of information technology in the banking industry faces many challenges, one of which is the hacking of banking information systems by hackers. There have been numerous cases of information system breaches in Indonesia, targeting both conventional and Islamic banks. In Indonesia, the financial sector ranks as the second-largest target of cyber attacks, as reported by the Financial Services Authority (OJK) in May 2022. In 2021, the financial sector experienced 22.4% of all cyber attacks globally, slightly less than the manufacturing sector with 23.2%. Out of all cyber attacks in the financial sector, 70% were directed towards banks, 16% towards insurance companies, and 14% towards other financial sectors (Pransuamitra, 2022). In 2023, a hacking incident and alleged data theft occurred at Bank Syariah Indonesia (BSI). BSI was targeted by the hacking group LockBit. Prior to the hacking, BSI's system also experienced a crash on May 8, 2023 (Chaterine, 2023). The changing landscape of information technology development is closely tied to banks' investment decisions, prompting them to exercise caution when selecting the hardware and software to be utilized (Respati 2008). Therefore, banks require information technology risk management and mitigation measures.

Research conducted by Nurhafiza states that a well-developed risk management system is essential to identify potential deterioration in the asset quality of Islamic banking portfolios. This is important to enable Islamic banks to maintain adequate reserves in dynamic situations, forecast future earnings, and implement risk mitigation techniques in accordance with Sharia principles to manage volatility and remain competitive. The capacity of Islamic banks for risk management significantly contributes to the quality of their risk management practices. Efficient risk management capability is crucial to strategically position Islamic banks in the volatile global market. (Malim, 2015)

Islamic banks face complex risks, both financial and non-financial, including the risk associated with the use of modern technology services. This risk has become increasingly prevalent among millennial customers and is susceptible to cyber threats, highlighting the need for protection measures (Samsul et al., 2022). Another research suggests that there is a lack of expertise in risk management and mitigation in Islamic banks compared to conventional banks (Al Rahahleh et al., 2019). Scientific literature captures several definitions of risk. Risk is defined as the variability of outcomes that can occur over a certain period with uncertainty, which can lead to potential losses and produce results different from expectations. In a study conducted by Yuha, risk is described as a situation that may occur and can result in losses or other unexpected circumstances (Qintharah, 2019).

Based on the above discussion, it is necessary to assess the efforts of information technology risk mitigation at Bank Syariah Indonesia (BSI). The objective of this research is to examine the information technology risk mitigation efforts carried out by

Bank Syariah Indonesia regarding the attack that occurred on May 8, 2023. The aim is to prevent attacks on the banking information system, especially at Bank Syariah Indonesia, and enhance the management of information technology risks.

## LITERATURE REVIEW

### Risk Management

Risk management is the effort to identify, analyze, and manage risks in every business activity with the goal of enhancing efficiency and effectiveness (Darmawi, 2016). Risk management is an approach that introduces a consistent system for managing all risks faced by an organization. According to COSO, the definition of Enterprise Risk Management (ERM) is that organizational risk management is a process influenced by the board of directors, management, and other employees, conducted throughout the organization by establishing strategies and aimed at identifying potential events that may impact the organization as a whole and controlling risks. The goal is to provide reasonable assurance that overall objectives will be achieved (Moeller, 2009).

Risk management is an iterative process that involves policy analysis, planning, implementation, control, and monitoring of policies, as well as measuring the implementation of security policies. Risk management is the process of creating and maintaining information system security within a company (Pratama, 2018). The proper implementation of risk management is expected to reduce the losses incurred by a company due to unexpected circumstances.

According to the Circular Letter of the Financial Services Authority Number 10/SEOJK.03/2014 on the Assessment of the Health Level of Sharia Commercial Banks and Sharia Business Units, there are six indicators for assessing operational risks related to information technology and supporting infrastructure. These indicators include: information technology complexity, changes in information technology systems, vulnerability of information technology systems to threats and attacks, maturity of information technology systems, information technology system failures, and reliability of supporting infrastructure (Otoritas Jasa Keuangan, 2014). There are also six similar indicators related to the assessment of operational risks associated with information technology and supporting infrastructure in commercial banks, as stated in Circular Letter OJK Number 14/SEOJK.03/2017 on the Assessment of the Health Level of Commercial Banks (Otoritas Jasa Keuangan, 2017).

### Mitigation

Mitigation is the activity of understanding and identifying the risks that may arise in carrying out business activities (Ika Gustin Rahayu, 2018). Therefore, mitigation refers to actions taken to reduce the impact of risks or can be interpreted as risk control. Risk control is an important and decisive step in overall risk management. Known risks and their potential consequences must be managed appropriately, effectively, and in line with the company's capabilities (Soehatman, 2010).

The provisions regarding the implementation of information technology by banks are regulated in the Financial Services Authority Regulation (POJK) of the Republic of Indonesia Number 11/POJK.03/2022. This regulation is intended for commercial banks, but Sharia banks can use it as a guideline for the implementation of information technology in banking. The regulation includes articles that regulate the implementation of risk management and information technology in banks, where banks are required to have a disaster recovery plan or mitigation plan. (Komisioner & Jasa, 2022)

**Information Technology**

In addition to using hardware and software, information technology is also utilized in data processing and storage. Furthermore, information technology serves as a communication tool for transmitting information. With the help of communication and information technology, users can generate useful outputs and share information with other users within and outside the organization through networks. (Muhlis, 2018)

Information technology refers to the methods or processes used to gather, prepare, store, process, communicate, analyze, and disseminate information (Komisioner & Jasa, 2022). Currently, banks utilize technology not only to meet internal needs and facilitate tasks but also to provide support to customers and the general public externally. The use of this technology does not restrict anyone; therefore, banks need to have a strong management system that prevents external interference. This is crucial to avoid manipulation by irresponsible individuals who seek to take advantage of the situation. (Samsul et al., 2022).

## METHODS

This study is qualitative research using a primary data approach related to the observed case or problem. The primary data is sourced from Twitter, collected over one week from May 4 to May 11, 2023. Data retrieval was performed by connecting Maxqda 2020 software to Twitter accounts using the search keyword "hashtag Bank Syariah Indonesia," resulting in 1909 pieces of primary data. Subsequently, the data was processed and analyzed using Maxqda 2020 and Gephi version 0.9.6 for Windows 10 64-bit software. Maxqda 2020 software processed the data to determine the relationships between system codes and sub-codes, translated into numerical form. System codes and sub-codes are lexical terms found within the 1909 pieces of data. Gephi application displayed social network analysis based on the processed data from Maxqda 2020 software. In addition to the primary data from Twitter, data was also collected from reliable websites such as *Bbc.com, Kompas.com, Keuangan.kontan.co.id, Liputan6.com*, and *Republika.co.id*, which was used for comparison with the primary data sourced from Twitter. This allowed the validation of Twitter data through reliable website sources.

## RESULT AND DISCUSSION

### Result

Twitter User Data

Every disruption in the use of information technology applications has a cause. A total of 129 filtered narrative texts were found regarding the causes of the information system crash in Bank Syariah Indonesia (BSI) that occurred on May 8, 2023. An analysis of public perceptions regarding the causes of the disruption needs to be conducted to determine the mitigation strategies that should be implemented by BSI's management and the government. Data processing to identify the causes of the disruption was done by creating system codes and sub-codes. The following is a detailed breakdown of the causes of the information system disruption in BSI :

**Table 1**. Data on the causes of the information system disruption in BSI, according to Twitter users

| Causes | Segments | Prosentase |
|---|---|---|
| System failure | 2 | 1,55% |
| Maintenance of information systems | 28 | 21,71% |
| Information system affected by ransomware | 8 | 6,20% |
| Information system affected by a virus | 3 | 2,33% |
| Error in the information system | 28 | 21,71% |
| Damaged hardware or software, which are the infrastructure of the information system | 2 | 1,55% |
| Information system attacked by hackers | 46 | 35,66% |
| Repair of the information system | 3 | 2,33% |
| Maintenance of the information system | 9 | 6,98% |
| Total | 129 | 100% |

Source : Primary data analysis using Maxqda software (2023)

From Table 1, it can be seen that the attack from hackers on BSI's information system is the main reason for the occurrence of the system crash on May 8, 2023. The second reason, based on public perception, is related to system maintenance and errors in the information system, accounting for 21.71%, which is lower than the first reason at 35.66%. The third reason, with a percentage of 6.98%, is attributed to maintenance activities that led to a decrease in system reliability.

The second analysis aims to determine the roles of the public, government, and BSI management. This analysis is important because customers are the ones most affected by disruptions in the banking information system. Furthermore, the analysis aims to identify the actors involved in addressing the information system disruptions at BSI, as perceived by Twitter users in Indonesia. The detailed list of actors involved in mitigating information technology risks is as follows:

**Table 2** Data Actors Involved in Mitigating BSI's Information System According to Twitter Users

| Aktor | Segments | Prosentase |
|---|---|---|
| Commissioner | 20 | 5,10% |
| CEO (Chief Executive Officer) | 11 | 2,81% |
| Board of Directors | 3 | 0,77% |
| IT Director | 1 | 0,26% |
| Managers | 2 | 0,51% |
| IT Team | 4 | 1,02% |
| Parliament Members (DPR) | 2 | 0,51% |
| Minister | 30 | 7,65% |
| MUI (Indonesian Ulema Council) | 1 | 0,26% |
| OJK (Financial Services Authority) | 9 | 2,30% |

| | | |
|---|---|---|
| Customers (Nasabah) | 309 | 78,83% |
| Total | 392 | 100% |

Source : Primary data analysis using Maxqda software (2023)

From the above Table 2, it can be observed that the actor most frequently mentioned in Twitter user comments is the customer (nasabah) with 78.83%. This is because customers are the most affected stakeholders in the event of a crash in BSI's information system on May 8, 2023. The second most mentioned actor is the minister with a percentage of 7.65%, representing the government. The third influential actor in this event is the commissioner with a percentage of 5.1%, representing the management of BSI.

The third analysis is conducted to determine the mitigation actions taken by BSI following the crash of their information system. This analysis is crucial as every bank has an obligation to manage information technology risks, ensuring that risks arising from the use of information technology can be controlled. The following details the actions taken by BSI in mitigating information technology, according to Twitter user feedback :

**Table 3.** Data of Actions Taken by BSI in Mitigating Information System, According to Twitter Users

| Action | Segments | Prosentase |
|---|---|---|
| Public announcement to inform the public that the system is experiencing disruptions | 1 | 2,38% |
| Maintenance of the information system after the occurrence of disruptions | 28 | 66,67% |
| Repair of the information system after the occurrence of disruptions | 3 | 7,14% |
| Enhancement of system reliability to prevent disruptions | 8 | 19,05% |
| Prevention of disruptions through system improvement | 2 | 4,76% |
| Total | 42 | 100% |

Source : Primary data analysis using Maxqda software (2023)

Based on Table 3, it shows that BSI conducted maintenance of the information system after the crash of the BSI information system on May 8, 2023. This action received 66.67% from 42 filtered narrative texts regarding the mitigation of the incident. The second action that needs to be taken is to enhance the system's reliability to prevent similar incidents from occurring again, ensuring that customers are not affected. This action received a percentage of 19.05%. The third action is to promptly repair the information system to prevent further losses for customers. This action received a percentage of 7.14%.

The fourth analysis is an assessment of the impact caused by the crash of the BSI information system. It is important to understand the impact of an event in order to minimize or effectively address the resulting consequences. This is necessary to prevent additional losses for BSI. The detailed impacts are as follows:

**Table 4.** Impacts Arising from Information Technology Risks According to Twitter Users

| Impact | Segments | Prosentase |
|---|---|---|
| BSI's reputation is ruined | 3 | 25,00% |
| Public trust in BSI is damaged | 3 | 25,00% |
| Dissatisfactory services provided by BSI | 6 | 50,00% |
| Total | 12 | 100% |

Source : Primary data analysis using Maxqda software (2023)

Based on Table 4, the most significant impact of the BSI system crash on May 8, 2023, according to Twitter users, is the dissatisfaction with the services provided by BSI, accounting for 50% of the responses. The second impact identified by Twitter users is the destruction of BSI's reputation that was previously built and the erosion of public trust in BSI.

As we know, Twitter offers a multitude of narratives. Therefore, after data coding as mentioned above, further analysis is needed to understand the relationships between the data. Many respondents expressed statements that encompassed multiple aspects related to sub-coded system statements. Therefore, it is important to analyze and discover the relationships between these statements to reach accurate conclusions. To facilitate data interpretation, the analysis was conducted by converting qualitative data into statistical code data and visualizing it.

In further analysis steps, the method of social network analysis was employed. The application of social network analysis enables the depiction of relationships among actors through the visualization of a social network map. This map is represented in the form of a graph, which is a way to illustrate relationships in a social network using nodes and links to represent actors and their connections. This analysis resulted in a modularity graph that indicates how easily the graph can be divided into communities, modules, or clusters, and the strength of these divisions. The following are the results of the social network analysis that provide a comprehensive overview of the respondents' statements.

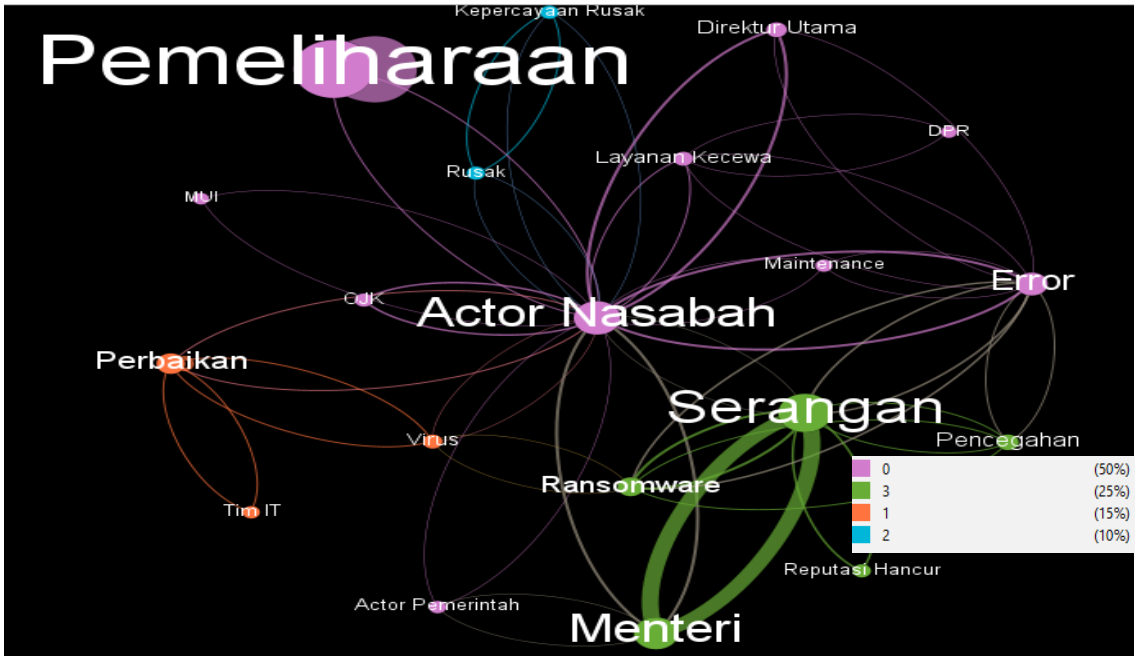


Figure 1: Preview of Relationships between Causes of System Disruption, Involved Individuals, Efforts to Handle Disruptions, and the Resulting Impacts

Source: Analysis of Primary Data Using Gephi version 0.9.6

Based on the above social network analysis, it can be concluded that elements such as customers, ministers, maintenance, attacks, ransomware, and errors have a significant presence in the network based on Twitter users' opinions. This is evident from the larger size of these points, indicating that respondents frequently discussed these aspects in their tweets on Twitter. The graph above also visualizes the relationships between these points. The interconnected relationships are depicted by the direction of the connecting lines. Thicker lines indicate strong and mutual relationships between two points.

**Data from Trusted Website**

A number of cybersecurity experts have confirmed that BSI fell victim to a ransomware attack. Lockbit not only issued threats but also proved that this ransomware group successfully stole and encrypted 1.5 terabytes of data from BSI. The hacking incident likely occurred before May 8, 2023, when the BSI Mobile application was dysfunctional and unusable. It takes a long time to steal 1.5 terabytes of data. To put it into perspective, if the data theft was continuously conducted at a speed of 25 Mbps for 24 hours, it would take 6 days to complete. However, if done carefully to avoid raising suspicion, it could take even longer, up to 12 days (Wardani, 2023). screenshot containing the breached BSI data was uploaded by the Twitter account @DarkTracer, which belongs to Fusion Intelligence Center, a Singapore-based cybersecurity technology company (Santika, 2023). This upload was made on May 13, 2023.

One consequence of this data breach is the exposure of customers' financial conditions, including abnormal account balances. The data theft resulted in the exposure of sensitive information such as M-Bank IDs, online banking services, emails, and more. Personal information of employees and customers was also reported to be compromised in this incident (Wardani, 2023). The sentiment surrounding the BSI data

breach caused the company's stock prices to plummet, leading many investors to abandon BSI.

On May 9, 2023, Bank BSI announced through its Instagram account that their services had been restored and transactions could be carried out at branch offices and BSI ATMs. In an official statement, BSI Corporate Secretary Gunawan Arief Hartoyo stated that approximately 1,200 BSI ATMs had been gradually restored and were ready for use. However, BSI Mobile services were still in the process of recovery. In this regard, BSI did not declare that its services had fully recovered. The new management of Bank BSI announced that all services had been restored on Thursday, May 11, 2023. At that time, BSI's CEO, Hery Gunardi, suspected that all digital service disruptions at BSI were caused by a cyberattack. However, BSI's Deputy Director, Bob Tyasika Ananta, stated that the data remained secure. (Simamora, 2023)

ELSAM, the Institute for Policy Research and Advocacy, argues that Bank BSI should immediately notify its customers about the case of personal data protection failure without unnecessary delays. The notification should be done formally and in writing. At the very least, the notification should include information about the exposed personal data, when and how the data was exposed, and the steps taken to address and recover from the failure. Additionally, BSI is expected to provide explanations regarding contact information that affected individuals can reach out to and mitigation measures that can reduce the risks resulting from the data breach (Simamora, 2023). Ardi Sutedja, the Head of the Indonesia Cyber Security Forum, stated that strengthening infrastructure and regulations alone are not enough. According to Heru, a System Provider (PSE) must be open to cyberattacks and data flow to build a "culture of openness" (BBC, 2023).

The National Cyber and Crypto Agency (BSSN) announced that they have been aware of the disruption of Bank BSI's services since the beginning of the incident on May 8th. BSSN engaged in internal communication and coordination with BSI to initiate the recovery of the affected systems. The coordination with BSI revealed that BSI's cyber incident team independently took responsibility for handling and repairing the impacted systems. On the other hand, Dian Ediana Rae, the Director of Banking Supervision at the Financial Services Authority (OJK), stated that the OJK's IT audit and supervisory team had communicated and coordinated with BSI to determine the cause of the service disruption, urging BSI to expedite the ongoing forensic examination process. OJK also instructed BSI to accelerate their response to customer and public complaints. In response to the incident, BSI management advised customers to maintain the confidentiality of their access, such as passwords, Personal Identification Numbers (PINs), and One Time Passwords (OTPs).(Simamora, 2023)

According to the Head of the Cyber Security Research Institute CISSReC, Dr. Pratama Persadha, the cybersecurity defense system in Indonesian banking is weak. This is evident from the multiple hacking incidents in Indonesian banks. It is "somewhat embarrassing" because despite the numerous attacks, the banks in Indonesia have not taken them as learning opportunities. Furthermore, the Bank of Indonesia has called for the digitization of all banking services to realize a cashless society. Ransomware attacks can be mitigated if the targeted parties have good data backups. BSI's CEO, Hery Gunardi, stated that they will continue to strengthen the company's technological security under the Chief Information and Security Officer (CISO). The CISO will oversee the system to identify its vulnerabilities and make improvements to protect BSI customer data. (BBC, 2023)

Pratama Persadha emphasized that the alleged cyber attacks on Bank BSI should be taken seriously. BSI needs to ensure that their systems are completely free from trojans or malware that can be exploited by hackers. It is also important to pay attention to data backups as they are key assets in restoring the system in the event of a hacker attack. Pratama also urged President Joko Widodo to promptly establish a personal data protection agency under the Personal Data Protection Law, with the aim of protecting the public in cases of repeated personal data breaches. The agency's responsibilities would involve assessing and investigating data breaches and taking action against institutions or companies that inadequately protect individuals' personal data. The series of frequent hacking incidents and data breaches should also serve as a warning for the government to pay more serious attention to the National Cyber and Crypto Agency (BSSN). (BBC, 2023)

During the Annual General Meeting of Shareholders (RUPST) on Monday, May 22, 2023, Bank Syariah Indonesia (BSI) made changes to its board of commissioners and directors. Three new names were added: Muliaman D Hadad as Independent President Commissioner, Saladin D Effendi as Director of Information Technology, and Grandhis Helmi H as Director of Risk Management. Their appointments will take effect after obtaining approval from the Financial Services Authority (OJK), considering their assessment of capability and suitability, and compliance with applicable regulations. (Risalah, 2023)

BSI's President Director, Hery Gunardi, expressed his hope that the changes in the company's management structure would support the ongoing digital and cultural transformation of BSI. The main goal is to drive business growth, strengthen BSI's contribution to the development of Islamic economics and finance, and support the government's efforts to accelerate national economic recovery. (Risalah, 2023)

**Discussion**

Based on the description above, it is evident that the crash of BSI's information system on May 8, 2023, was caused by a hacker attack. This is supported by data from Twitter and reputable websites. Hacker attacks can occur on banking information systems due to weak security measures. If a banking information system lacks adequate security measures such as strong encryption, the use of complex passwords, a robust firewall, or regular software updates, the system can become an easy target for hackers. This is in line with previous research stating the need for innovation in banking security systems to protect against and address electronic transaction crimes, especially in the banking sector (Faridi, 2019).

The maintenance of information technology is not only done for hardware but also for software. Maintenance of software is one way to prevent attacks on an information system that can result in losses for companies and customers. Maintaining software to prevent malware attacks experienced by BSI on May 8, 2023, can be done through several steps. The first step is to identify the source of the malware and classify its type. After determining the source and type of malware, the next step is to update or install an antivirus program that contains data related to the existing malware types in the computer system. If these steps do not successfully remove the malware, the next step is to update the operating system installed on the computer system. If the malware persists despite all efforts, the last resort is to format the partitions on the computer system (Naam, 2017). Before formatting the partitions in the computer system, it is essential to ensure that data backups have been performed.

The most affected party in attacks on banking information systems is the customers (nasabah). This is evident from the social network analysis presented in the findings of this research. Customer data can be disseminated and even traded on the internet by irresponsible parties. Banking data is an example of a category of data referred to as big data. Data encryption is one way to protect big data, such as customer data. Data encryption is a technology that uses special data processing techniques to hide or protect data through a computer network, preventing unauthorized users from understanding the information (Munawar et al., 2020). Service through information systems is one of the factors that influence customer loyalty. A well-functioning information system leads to increased customer satisfaction with a banking company's services, resulting in higher customer loyalty to that bank. This aligns with previous research stating that customer satisfaction significantly affects customer loyalty (Rahmawaty, 2011).

The IT risk mitigation carried out by BSI during the incident of the information system crash on May 8, 2023, is considered to be slow. This is also supported by data from Twitter and reputable websites. The system resumed normal operation on May 11, 2023. The delay in IT risk mitigation is due to several factors, including BSI's lack of awareness or incomplete understanding of the importance of IT risk mitigation. They may not have sufficient understanding of cybersecurity threats and their impact on their operations. This is reinforced by the replacement of BSI's Director of Risk Management (Risalah, 2023). One of the objectives of risk mitigation is to minimize risks associated with banking activities (Karim, 2013).

Internal audit is one of the factors that influence the speed of information technology risk mitigation. Internal audit is an independent assessment activity within an organization to review operations as a service provided to management. Internal audit helps the organization achieve its objectives through a systematic and disciplined approach to evaluating and improving the effectiveness of risk management. Within an organization, internal audit is an independent function whose main task is to conduct ongoing assessments by preparing reports that analyze the methodologies, procedures, and processes involved in risk management. Thus, internal audit evaluates risk management measures to ensure their appropriateness concerning risk exposure (vulnerable objects), which is a primary focus in the supervision of banking risks.(Amelia et al., 2019)

## CONCLUSION

Based on the data analysis in this research, it can be concluded that the efforts of information technology risk mitigation carried out by Bank Syariah Indonesia (BSI) regarding the attack case that occurred on May 8, 2023, are still slow. This indicates that the security of BSI's information system is still weak as the technology infrastructure remains vulnerable to threats and information technology attacks. Another reason is that BSI is still a young institution, and its information system has not fully matured yet. In the advancing digital era, information technology risks have become increasingly significant due to the vast amount of data processed and stored by companies, as well as the complexity of information technology systems and infrastructure. The use of security technologies such as firewalls, antivirus software, data encryption, and software maintenance helps protect systems and data from security threats. Appropriate security technologies will aid in identifying, preventing, and responding to security breaches.

## REFERENCES

Al Rahahleh, N., Ishaq Bhatti, M., & Najuna Misman, F. (2019). Developments in Risk Management in Islamic Finance: A Review. *Journal of Risk and Financial Management*, *12*(1), 37. https://doi.org/10.3390/jrfm12010037

Amelia, E., Ramdan, M. H., Program, S., Prodi, D., Syariah, P., Syarif, U., & Jakarta, H. (2019). PENGARUH AUDIT INTERNAL TERHADAP MITIGASI RISIKO OPERASIONAL PERBANKAN SYARIAH. *Jurnal Ekonomi Dan Bisnis Islam : Ad-Deenar*, *3*(01). https://doi.org/10.30868/ad.v3i01.500

BBC. (2023). *BSI diduga kena serangan siber, pengamat sebut sistem pertahanan bank "tidak kuat."* Bbc.Com. https://www.bbc.com/indonesia/articles/cn01gdr7eero

Chaterine, R. N. (2023). *Bareskrim Mulai Selidiki Kasus Peretasan Sistem BSI*. Kompas.Com. https://nasional.kompas.com/read/2023/05/19/12442961/bareskrim-mulai-selidiki-kasus-peretasan-sistem-bsi

Darmawi, Herman. (2016). *Manajemen Risiko: Edisi 2*. Sinar Grafika Offset.

Direktorat Statistik Keuangan, Teknologi Informasi, dan P. (2021). *Indeks Pembangunan Teknologi Informasi dan Komunikasi 2021*. BPS RI.

Faridi, M. K. (2019). Kejahatan Siber Dalam Bidang Perbankan. *Cyber Security Dan Forensik Digital*, *1*(2), 57–61. https://doi.org/10.14421/csecurity.2018.1.2.1373

Ika Gustin Rahayu, H. (2018). Mitigasi Risiko Pembiayaan Pada Bank Perkreditan Rakyat Syariah (BPRS) SAFIR Cabang Curup Kabupaten Rejang Lebong. *Al Falah: Journal of Islamic Economics*, *3*(2), 2–22.

Karim, A. (2013). *Bank Islam: Analisis Fiqh dan Keuangan*. Raja Grafindo Persada.

Kholis, N. (2020). Perbankan Dalam Era Baru Digital. *Economicus*, *12*(1), 80–88. https://doi.org/10.47860/economicus.v12i1.149

Komisioner, D., & Jasa, O. (2022). *POJK+11-POJK.03-2022+Penyelenggaraan Teknologi Informasi Oleh Bank Umum+2022*.

Laucereno, S. F. (2022). *Bank Jangan Ketinggalan Zaman, Layanan Harus Serba Digital*. Https://Finance.Detik.Com/. https://finance.detik.com/moneter/d-6407809/bank-jangan-ketinggalan-zaman-layanan-harus-serba-digital

Malim, N. A. K. (2015). Islamic Banking and Risk Management: Issues and Challenges. *Journal of Islamic Banking and Finance, Oct.-Dec.*, 64–71.

Moeller, Robert. (2009). *Brink's modern internal auditing : a common body of knowledge* (Vol. 7). John Wiley & Sons, Inc. Hoboken.

Muhlis. (2018). *Menelisik Kinerja Bank Syariah Berbasis Teknologi Informasi, Bank Syariah*. Trust Media Publishing.

Munawar, Z., Kom, M., & Putri, N. I. (2020). KEAMANAN JARINGAN KOMPUTER PADA ERA BIG DATA. In *Jurnal Sistem Informasi-J-SIKA* (Vol. 02).

NAAM, J. (2017). METODA PERTAHAN DIRI PROGRAM VIRUS. *Jurnal MEDIA PROCESSOR*, *8*(2).

Otoritas Jasa Keuangan. (2014). Surat Edaran Otoritas Jasa Keuangan Nomor 10/SEOJK.03/2014 Tentang Penilaian Kesehatan Bank Umum Syariah dan Unit Usaha Syariah. *O*, *110*(9), 1689–1699.

Otoritas Jasa Keuangan. (2017). *Surat Edaran Otoritas Jasa Keuangan Nomor 14/SEOJK.03/2017 Tentang Penilaian Kesehatan Bank Umum*. 1–23.

Pransuamitra, P. A. (2022). *Awas! Bank Sering Diretas, Duit Rp 1,2 Triliun Pernah Lenyap*. CNBC Indonesia. https://www.cnbcindonesia.com/market/20220919000241-17-373057/awas-bank-sering-diretas-duit-rp-12-triliun-pernah-lenyap

Pratama, R. (2018). PENERAPAN MANAJEMEN RISIKO PADA PERBANKAN SYARIAH (Studi Kasus Pada Bank Muamalat & Bank Syariah Mandiri Cabang Kota Ternate) Rheza Pratama Fakultas Ekonomi Universitas Muhammadiyah Maluku Utara INFORMASI ARTIKEL ABSTRAK Jurnal Mitra Manajemen (JMM Online. *Jurnal Mitra Manajemen (JMM Online)*, *2*(6), 597–609.

Qintharah, Y. N. (2019). Perancangan Penerapan Manajemen Risiko. *JRAK: Jurnal Riset Akuntansi Dan Komputerisasi Akuntansi*, *10*(1), 67–86. https://doi.org/10.33558/jrak.v10i1.1645

Rahmawaty, A. (2011). *PENGARUH SERVICE PERFORMANCE, KEPUASAN, TRUST DAN KOMITMEN TERHADAP LOYALITAS NASABAH DI BANK SYARI'AH MANDIRI KUDUS.*

Risalah, D. F. (2023). *BSI Rombak Jajaran Komisaris dan Direksi, Ada Tiga Nama Baru*. Republika.Co.Id. https://sharia.republika.co.id/berita/rv231g502/bsi-rombak-jajaran-komisaris-dan-direksi-ada-tiga-nama-baru-part1

Samsul, Muslimin, S., & Jafar, W. (2022). Risiko Perkembangan Teknologi Perbankan Syariah Era Millenial. *Journal of Islamic Economics*, *4*(1), 1–11. https://doi.org/10.37146/ajie

Santika, E. F. (2023). *Saham BSI Langsung Ambles Setelah Datanya Bocor di "Dark Web."* Katadata.Com. https://databoks.katadata.co.id/datapublish/2023/05/16/saham-bsi-langsung-ambles-setelah-datanya-bocor-di-dark-web

Simamora, N. (2023). *Menengok Kasus BSI dan Masalah Peretasan di Perbankan*. Keuangan.Kontan.Co.Id. https://keuangan.kontan.co.id/news/menengok-kasus-bsi-dan-masalah-peretasan-di-perbankan

Soehatman, R. (2010). *Pedoman praktis manajemen bencana (sisaster management)*. Dian Rakyat.

Wardani, A. S. (2023). *Kronologi BSI Jadi Sasaran Ransomware Lockbit: Aksi Peretasan Diduga Saat Libur Lebaran*. Liputan6.Com. https://www.liputan6.com/tekno/read/5285458/kronologi-bsi-jadi-sasaran-ransomware-lockbit-aksi-peretasan-diduga-saat-libur-lebaran

Wardiana, W. (2002). Perkembangan Teknologi Informasi di Indonesia. *Seminar Dan Pameran Teknologi Informasi*. https://doi.org/10.1007/BF02191578

Werdi Apriyanti, H. (2018). Perkembangan Industri Perbankan Syariah Di Indonesia : Analisis Peluang Dan Tantangan. *Maksimum*, *8*(1), 16. https://doi.org/10.26714/mki.8.1.2018.16-23