DIJEFA: Dinasti International Journal of Economics, Finance & Accounting
E-ISSN: 2721-303X
P-ISSN: 2721-3021
https://dinastipub.org/DIJEFA dinasti.info@gmail.com +62 811 7404 455
DOI: https://doi.org/10.38035/dijefa.v6i4

Cyber Attacks on Financial Performance: Sharia and SDGs Perspective

Hartutik[1], Dwi Nita Aryani[2*]
[1]Universitas Muhammadiyah Jakarta, Indonesia, hartutik@umj.ac.id
[2]STIE Malangkucecwara, Malang, Indonesia, dwinita@stie-mce.ac.id

[*]Corresponding Author: dwinita@stie-mce.ac.id[2]

Abstract: The objective of this study is to analyse the impact of cyber-attacks on the performance stability of Bank Syariah Indonesia (BSI) on financial and non-financial performance indicators, including Capital Adequacy, Asset Quality, Management Quality, Income, and Liquidity. The research method employed is descriptive qualitative, with trend analysis conducted based on secondary data from BSI's annual and quarterly reports prior to and following the cyberattack incident. The findings indicated an upward trend in several performance indicators, reflecting the resilience of the financial performance despite the cyber-attack. BSI was able to maintain customer trust and recorded an increase in both sources of funds and assets. Furthermore, the research evaluated BSI's Shariah compliance and its contribution to the achievement of Sustainable Development Goal (SDG) 16, which focuses on strengthening inclusive, transparent, and accountable institutions. BSI's risk management was found to be at the composite level 2 (low-moderate). It is recommended that improvements be made to the cybersecurity systems, risk management, and the supervision of the Sharia Supervisory Board (DPS) in order to ensure the sustainability of Sharia compliance in every aspect of operations.

Keywords: Cyberattacks, Financial Stability, Bank Syariah Indonesia, Customer Trust, SDGs 16 JEL: O16, P47, M21.

INTRODUCTION

The issue of cybersecurity has become an increasingly urgent concern within the global banking industry, with the occurrence of cyberattacks representing a significant and growing threat to the sector. The advent of digital systems has facilitated the development of technology-driven banking transaction activities. It is estimated that 72% of Indonesian consumers opt for digital transactions on a daily basis. The value of digital bank transactions in Indonesia reached 58,478 trillion rupiah in 2023, and is projected to grow by 9.11% in 2024 (Vida, 2024). The rapid development of information technology and digital transaction innovation will undoubtedly result in increased cyber security risks for banks. As service companies, banks must prioritize trust and loyalty to maintain their customer base. Islamic

banks, as an integral part of the global financial system, are particularly vulnerable to various threats, including cyber-attacks. Incidents of cyber-attacks can not only disrupt bank operations, but also potentially reduce customer confidence and undermine the financial stability of the bank.

The issue of cybersecurity has become an increasingly urgent concern within the global banking industry, with the occurrence of cyberattacks representing a significant and growing threat to the sector. The advent of digital systems has facilitated the development of technology-driven banking transaction activities. It is estimated that 72% of Indonesian consumers opt for digital transactions on a daily basis. The value of digital bank transactions in Indonesia reached 58,478 trillion rupiah in 2023, and is projected to grow by 9.11% in 2024 (Vida, 2024). The rapid development of information technology and digital transaction innovation will undoubtedly result in increased cyber security risks for banks. As service companies, banks must prioritize trust and loyalty to maintain their customer base. Islamic banks, as an integral part of the global financial system, are particularly vulnerable to various threats, including cyber-attacks. Incidents of cyber-attacks can not only disrupt bank operations, but also potentially reduce customer confidence and undermine the financial stability of the bank.

Indonesia has a multitude of Islamic financial institutions. Of the 10 largest Islamic banks in Indonesia, Bank Syariah Indonesia (BSI) is the largest, with assets of IDR357.9 trillion, a figure that is considerably higher than that of the second and third largest banks, namely Bank Muamalat and UUS PT Bank CIMB Niaga Tbk (BNGA) or CIMB Niaga Syariah (Burhan, 2024). As a significant actor within the Indonesian Islamic banking sector, BSI is confronted with considerable obstacles in ensuring the security and integrity of its information systems. This challenge is further exacerbated by the emergence of sophisticated and malevolent cyberattacks. In May 2023, Bank Syariah Indonesia (BSI) was the subject of a cyberattack, which was significant in scale and attracted the attention of the public and supervisory authorities. The BSI service error is believed to have occurred between 8 and 11 May 2023. The BSI service error resulted in customers being unable to conduct financial transactions at branch offices, automated teller machines (ATMs), and even BSI Mobile (Hardiansyah, 2023).

In May 2023, Bank Syariah Indonesia (BSI) was the victim of a cyber-attack. The incident resulted in the disruption of a number of services, including mobile banking, automated teller machines (ATMs), and several other services. The incident not only disrupted the bank's day-to-day operations but also prompted concerns regarding the security of customer data and the bank's ability to maintain public trust. In this context, it is important to evaluate the direct impact of this hacking incident on BSI's financial performance, which reflects not only the stability of the bank's operations but also the confidence of customers and investors. Previous research has demonstrated that cybercrime experienced by the banking industry impacts customer trust, resulting in issues, dissatisfaction and a lack of loyalty (Wardhana et al., 2023).

The occurrence of cyberattacks and the security of banking operations are directly related to Sustainable Development Goal (SDG) 16, which pertains to "Peace, Justice, and Strong Institutions." These incidents have a direct impact on the stability and integrity of financial institutions. SDG 16 underscores the significance of fostering robust, transparent, and reliable institutions, and instilling a sense of assurance in each transaction. The maintenance of robust cybersecurity is a crucial element in achieving this goal, particularly in maintaining public trust in Islamic banking institutions (Van Halderen et al., 2019). It is therefore imperative that banks enhance their cyber resilience, which in turn will encourage them to implement robust cyber security risk management regulations. This is set out in the Circular Letter of the Financial Services Authority of the Republic of Indonesia Number 29 /SEOJK.03/2022 concerning Cyber Resilience and Security for Commercial Banks.

The findings of Cavaliere et al. (2021) indicate that cyber-crime has a markedly detrimental impact on the financial performance of banking institutions. There is a clear

correlation between the prevalence of internet fraud and the deterioration of a bank's financial standing. Furthermore, the occurrence of cyberattacks will result in a reduction in customer reputation and trust. As posited by Hasan, Ali, Kurnia, and Thurasamy (2021), the negative impacts of cyberattacks include losses due to revenue, high recovery costs, a decline in reputation, and the leakage of important and confidential data. Consequently, it is of paramount importance to ensure the readiness of human resources, technology, regulations, procedures, and commitment in order to maintain cyber security (Deloitte, 2016).

From the perspective of sharia principles, cyberattack incidents have the potential to violate two key principles: amanah (trust) and hifz al-mal (protection of wealth). From the perspective of amanah, Islamic financial institutions are obliged to maintain customer trust in every financial interaction. Furthermore, the principle of hifz al-mal demands that banks protect customer assets and property rights from external threats, including cyberattacks. Consequently, the maintenance of cyber security is not merely a technological concern; it is also a moral and ethical obligation that ensures the equilibrium of Sharia principles. Wealth is a trust from Allah that must be developed and used honestly and earnestly for the elimination of poverty, the fulfilment of the needs of all people, the creation of a comfortable life for all, and the promotion of an equitable distribution of income and wealth (Chapra, 2008).

This study will analyse the impact of the cyber-attack experienced by BSI Bank on the bank's financial performance. To this end, a performance evaluation approach will be employed that includes the following five areas: capital adequacy, asset quality, management, earnings, and liquidity. In addition, the study will consider information technology risk management. The objective of this research is to conduct a comprehensive analysis of the impact of the hacking incident on BSI's financial performance. This will be achieved by utilising secondary financial data sourced from the bank's annual and quarterly reports. A trend analysis approach will be employed to identify patterns and significant changes in BSI's financial performance before and after the incident.

This analysis will not only highlight the direct financial impact of the hacking incident, but also provide insights into the recovery strategies adopted by BSI to mitigate the risks and negative impacts and restore public confidence. The analysis also identifies the strategies adopted by BSI to restore stability and trust, which are compliant with Shariah principles and support the achievement of SDG 16. With a deeper understanding of the complexity and impact of hacking incidents on the financial performance of Islamic banks, it is hoped that this article can make a meaningful contribution in raising awareness of cybersecurity within the banking industry, as well as offer practical guidance for other banks facing similar challenges in the future. In addition, it is hoped that the results of this study will make a valuable contribution to raising banks' awareness of the importance of maintaining cybersecurity and promoting stronger, less risky financial institutions.

Literature Review

The Concept of Financial Stability in Islamic Banking

Financial stability is a crucial element in maintaining the soundness and resilience of financial institutions, including Islamic banks. Financial stability can be defined as the ability of a bank to withstand external and internal shocks without experiencing significant losses (OJK, 2017b). In contrast to conventional banking institutions, Islamic banks operate in accordance with Sharia principles, which prohibit the practice of usury (interest), maisir (speculation), and gharar (uncertainty) (OJK, 2017a). The practice of usury, or the use of interest, is prohibited in Sharia principles due to its potential to undermine economic stability and cause injustice. In Islam, financing transactions must be asset-based, which can reduce speculation and thus contribute to financial stability. Gharar, or uncertainty, often arises in speculative transactions and can create instability in economic transactions.

Cyberattacks in the Banking Sector

The banking sector is facing a significant threat from cyberattacks, given the increasing reliance on information technology. Cyber-attacks may manifest in a number of ways, including phishing, ransomware, DDoS (Distributed Denial of Service), and malware (Bpptik, 2023). The consequences of cyberattacks on banking institutions can be severe, encompassing financial losses, reputational harm, and diminished customer confidence (Maulana & Fitriana, 2023). The occurrence of cyberattacks on a number of prominent banking institutions has resulted in the loss of billions of dollars and the disruption of banking operations (Zefanya, 2023). A review of case studies examining cyberattacks against specific banks provides insight into the potential impact of such attacks on the financial stability and operational resilience of banking institutions. In the circular letter of Otoritas Jasa Keuangan (OJK) Number 29/SEOJK.03/2022, the determination of inherent risk levels related to cybersecurity is categorised into the following six levels: Rating 1 (low), Rating 2 (low to moderate), Rating 3 (moderate), Rating 4 (moderate to high), and Rating 5 (high). A lower rating indicates a greater capacity for maintaining cybersecurity. Each bank is obliged to mitigate cyber risk and provide a report on how it is managed in the event of a risk.

Impact of Cyberattacks on Islamic Banks

Islamic banks, as financial institutions that operate in accordance with Sharia principles, offer a range of products and services that are distinct from those provided by conventional banks. Furthermore, Islamic banks encounter obstacles in maintaining robust customer confidence in their adherence to sharia principles. The occurrence of cyberattacks on Islamic banks has the potential to result in a number of adverse consequences, including operational disruptions, financial losses and a reduction in customer confidence (Azizah & Udayana, 2022). Prior research has demonstrated that information security and technology are crucial for safeguarding Islamic banks from cyber threats (Maulana & Fitriana, 2023).

CAMEL Model in Evaluating the Performance of Islamic Banks

The CAMEL analysis is employed to assess the performance and financial stability of Bank Syariah Indonesia (BSI). The CAMEL method is a comprehensive approach to assessing the financial health of banks, as employed by banking authorities. Each component of the CAMEL model namely capital adequacy, asset quality, management quality, earnings and liquidity, play an important role in the evaluation of bank risk and performance.

Capital Adequacy

The term 'capital adequacy' is used to describe a bank's capacity to withstand unforeseen losses and to safeguard the interests of depositors and shareholders. The ratio employed for the measurement of capital adequacy is the Capital Adequacy Ratio (CAR). The CAR formula is calculated by dividing the total capital by the average total monthly outstanding loans and deposits ratio (ATMR), with the result multiplied by 100%. The Basel Committee on Banking Supervision (BCBS) has set the recommended ratio standard at 8% (Committee, 2011), a figure that is also referenced in the Financial Services Authority regulation Number 11/POJK.03/2016 concerning the provision of minimum capital for commercial banks, article 2 paragraph 3 (OJK, 2016).

Asset Quality

Asset quality is a measure of the efficacy with which a banking institution manages its credit risk. The most commonly employed ratios for the assessment of asset quality are the Non-Performing Financing (NPF) Ratio and the Financing to Deposit Ratio (FDR). The NPF formula is calculated by dividing the total nonperforming financing by the total financing, and

then multiplying the result by 100%. Similarly, the FDR formula is calculated by dividing the total financing by the total deposits, and then multiplying the result by 100%. The NPF standard recommended by the OJK and included in the healthy category for Islamic banks is less than 5%, while the ideal FDR is between 85% and 100% (Financial Services Authority, 2022).

Management Quality

Management Quality assesses the efficiency and effectiveness of bank management in the context of operational management and risk management. The most frequently employed ratio is that of operating expenses to operating income (BOPO). The optimal BOPO ratio, as defined by Bank Indonesia, is 85% (Simamora, 2024). An elevated BOPO ratio indicates a lack of operational efficiency.

Earnings (income)

The level of profitability is indicative of the efficiency and effectiveness of management in the utilisation of resources to generate profits. Profitability represents a crucial indicator for evaluating the overall financial performance of a banking institution. In the context of CAMELS analysis, the profitability of a financial institution is gauged through the application of a number of key ratios. In a healthy financial institution, the ROA is expected to fall within the range of 0.5% to 1.25%. The return on equity (ROE), a healthy standard for this ratio is 5%–12.5%. The net interest margin (NIM) , a healthy standard for this ratio is 1.5%–2%. These ratios are defined in the 2004 guidelines from Bank Indonesia (BI).

Liquidity

Liquidity measures the bank's ability to meet its financial obligations in the short term. The ratio used is the Financing to Deposit Ratio (FDR) with standards 85%-100%. SDG 16, which encompasses peace, justice, and strong institutions, is a crucial component of the broader Sustainable Development Goals (SDGs) framework. SDG 16 acknowledges the significance of fostering peaceful and inclusive societies, ensuring access to justice for all, and establishing effective, accountable, and inclusive institutions. Additionally, SDG 16 emphasises the importance of the rule of law, the reduction of violence, and the enhancement of the quality of public institutions (UN, 2023). SDG 16 comprises a number of indicators that are used to assess progress in achieving its stated goals. These include the reduction of violence, the implementation of an effective rule of law, the protection of human rights, and the strengthening of public institutions.

The quality of institutions and the level of public trust are also pivotal in achieving SDG 16 (Maseka, 2021). The attainment of SDG 16 may be impeded by a number of factors, including corruption, injustice and human rights violations. A review of the literature reveals that deficiencies in public institutions and the rule of law can precipitate social instability and chaos. Consequently, SDG 16 necessitates a concentration on the reform of institutions and the enhancement of the legal system (Kaufmann et al., 2009).

Sharia Principles of Amanah and Hifz al-Maal

In Islamic doctrine, the concept of amanah (trust) denotes the moral obligation to safeguard and uphold the trust that has been placed in one's care. This principle is elucidated in the Qur'an and Hadith as a component of ethical and moral conduct in human interactions. The following verses and hadiths illustrate this principle:

Al-Quran and Hadith

QS Al-Anfal (8:27): 'O you who believe, betray not Allah and His Messenger, and betray not the trusts entrusted to you while you know.' This verse underscores the significance of

upholding the trust placed in one, including in the context of accountability towards others. QS Al-Isra (17:34): "And fulfill your promises, for promises will be held accountable." This verse demonstrates the necessity of fulfilling and maintaining all promises and trusts in an appropriate manner. All customer assets deposited in Bank Syariah Indonesia are held in trust by the bank, which is expected to act in a trustworthy manner.

In his teachings, the Prophet Muhammad (SAW) placed great emphasis on the importance of fulfilling trust and promises in all aspects of life. "If someone is entrusted with a responsibility, it is their obligation to fulfil it." "Furthermore, if an individual makes a commitment, they are obliged to honour it." (According to the hadith collections of Al-Bukhari and Muslim). It can be argued that trust is an integral aspect of faith. "And whoever betrays a trust is not to be considered a member of our community." (HR. Abu Dawud). This hadith elucidates the notion that trust constitutes an essential tenet of Islamic faith. The betrayal of a trust inevitably results in destruction. The Companions enquired as to how it could be considered to have been misused. In response, the Hadith states that if a matter is handed over to someone who is not an expert, then destruction is inevitable (HR: Al-Bukhari, no. 59). This Hadīth emphasises the importance of fulfilling trusts and warns of the adverse consequences if trusts are not fulfilled, especially if tasks or responsibilities are handed over to incompetent people.

Sustainable Development Goals

Almost countries in the world promised to save the planet with 17 goals, namely no poverty, zero hunger, good health and well-being, quality education, gender equality, clean water and sanitation, affordable and clean energy, decent work and economic growth, industry, innovation and infrastructure, reduced inequality, sustainable cities and communities, responsible consumption and production, climate action, life below water, life on land, Peace and justice strong institution, partnership to achieve the goal. The goal number 16 is in line with this study, where strong and accountable institution must be achieved for any companies particularly banking.

METHOD

This study is a qualitative research, employing a systematic investigation of phenomena through the collection of data amenable to statistical, mathematical, or computational techniques (Ummul et al., 2022). This research employs a descriptive qualitative approach with a focus on trend analysis. The research aimed to analyse the impact of the hacking incident on the financial and non financial performance of Bank Syariah Indonesia (BSI) before and after the cyber incident, taking into account aspects of financial stability, restoration of trust, as well as compliance with Sharia principles and SDGs. The model is comprised of five principal components, namely: Capital adequacy is a measure of the strength of a bank's capital, indicating its capacity to absorb losses. Asset Quality: This component assesses the risks associated with a bank's assets, Management Quality: Evaluate management effectiveness and competence; Earnings: Analyse profitability and stability of earnings; Liquidity: Assess the bank's ability to meet short-term obligations (Van Greuning & Brajovic-Bratanovic, 1999). In addition, it will also be analysed how risk management related to cyber-attack is implemented by BSI.

Data, Data Sources and Data Collection Methods

This research employs secondary data obtained from a variety of sources, including: BSI Financial Statements: The data from BSI's annual and quarterly reports, both prior to and following the hacking incident, will be used in this study. These reports can be found at this link (https://ir.bankbsi.co.id/annual_reports.html). Information regarding the

hacking incident obtained from news sources, cybersecurity reports, and official reports from BSI. Non-financial data obtained from the 2023 Sustainability Report of PT Bank Syariah Indonesia is used to analyse the achievement of peace, justice, and strong institutions, as well as the evaluation of sharia compliance (Kallman, 2023).

Research Procedures and Interpretation of Results

This research employed descriptive qualitative methods for the analysis of the data. The analysis was conducted in accordance with the following steps: 1) A description of the financial condition was provided. A description of the financial condition of BSI was provided, both before and after the hacking incident, based on the CAMEL indicators. 2) Indicator Comparison: A comparison of the CAMEL indicators before and after the hacking incident was conducted to identify significant changes. 3) Trend analysis. The objective is to analyse the trend of changes in CAMEL indicators over a period of time in order to gain insight into the long-term impact of the cyberattack. The risk management strategy is based on the risk profile composite rating, which is determined through a self-assessment conducted by the bank.

This research employs Microsoft Excel for preliminary data processing and elementary statistical analysis. The research procedure is conducted in three stages: first, data related to hacking incidents are collected; second, the data are processed by calculating CAMEL indicators from the collected data; and third, the data are analysed using descriptive methods to identify and analysed the impact of hacking. In the final stage, the results of the analysis are interpreted, and conclusions are drawn regarding the impact of hacking on BSI's financial stability.

Trend Analysis

Trend analysis is used to understand the pattern of increase or decrease in each financial indicator over the period analysed. The results of the trend analysis will provide insight into how the cyberattack affected BSI's financial stability, and which areas experienced the most significant impact. Trend analysis was conducted using the base year as a reference point (Gar, 2018).

RESULTS AND DISCUSSION

The principal objective of this research is to examine the influence of the cyber-attack on the financial stability of Bank Syariah Indonesia (BSI) through the application of the CAMEL model and risk management. A quantitative approach is employed for the descriptive analysis of BSI's financial condition prior to and following the hacking incident. The following data is derived from the quarterly financial statements of Bank Syariah Indonesia.

Financial Data

The data analysed comprises eight key financial indicators: The following financial indicators were considered: Third Party Funds (DPK), Assets, Financing to Deposit Ratio (FDR), Return on Assets (ROA), Return on Equity (ROE), Non Performing Financing (NPF), Capital Adequacy Ratio (CAR), and Operating Expenses to Operating Income (BOPO). These indicators were selected for their comprehensive representation of BSI's financial performance and risk profile.

Table 1 shows that each indicator demonstrates an improvement in condition subsequent to the cyber-attack in comparison to the preceding period. The indicators of deposits, assets, ROA, ROE, and CAR exhibited an increase, while NPF and BOPO demonstrated a decline, indicating a favorable financial condition. BSI was also able to maintain its risk at score 2 (low to moderate), providing evidence that despite experiencing a

cyberattack, BSI was still able to maintain its financial performance, customer confidence, and risk mitigation strategies.

Table 1. Indicators before and after cyber-attack

Indicator	Indicator (before and after cyber-attack)							
	Before	After	Before	After	Before	After	Before	After
	June 2022	June 2023	Sep-2022	Sep-23	Dec 2022	Dec 2023	Mar 2023	Mar 2024
Third party fund	244,663,546	252,515,628	245,176,434	262,115,758	261,490,981	293,775,929	269,257,913	297,338,614
ASET	277,342,955	313,612,591	280,002,034	319,846,454	305,727,438	353,624,124	313,252,694	357,903,623
FDR	78.14	87.80	81.45	88.31	79.37	81.73	79.14	83.05
ROA	2.03	2.36	2.08	2.34	1.98	2.35	2.48	2.51
ROE	17.66	17.27	17.44	16.85	16.84	16.88	18.16	18.30
NPF	0.74	0.62	0.59	0.61	0.57	0.55	0.54	0.55
CAR	0.1733	0.2060	0.1721	0.2110	0.2054	0.2139	0.2064	0.2155
BOPO	74.5	70.87	74.02	71.43	75.88	71.27	69.65	68.94
RISK	2	2	2	2	2	2	2	2

Non-Financial Data

Complaint and Survey results

Table 2 allows us to identify the main problems. The majority of grievances pertain to the BI Fast Transfer, BSI ATM Cash Withdrawal, and Top Up Funds services. This indicates that the majority of complaints originate from digital transaction services. This is a matter of concern for BSI, as the figure of approximately 19,900 complaints per month, or 664 per day, is nevertheless relatively high.

Regarding the prioritisation of service improvement, the highest number of complaints pertaining to BI Fast Transfers (71,039 complaints) and BSI ATM Cash Withdrawals (58,362 complaints) indicates that BSI should prioritise enhancing the stability and convenience of digital transactions as a means of reducing the number of complaints in the future. Based on the improvement customer satisfaction, notwithstanding the considerable number of grievances, the customer satisfaction rating increased from 52.50% in 2022 to 60.60% in 2023. This suggests that, although the number of complaints remains high, BSI has implemented measures that have led to an improvement in customer satisfaction, with an increase of 8.10%.

Table 2. Top five of complaints and satisfaction results

No.	Complaint type	Number of complaint
1	Transfer BI Fast	71,039
2	With drawl through ATM	58,362
3	Deposit through Top Up	41,054
4	Buying troughs Top Up	39,809
5	Deposit throughs ATM	28,555
Total complaint		238,819

Result of Satisfaction Survey		
year	Survey	Satisfaction
2022	satisfaction	52.50%
2023	Satisfaction	60,60%
increase		8,10%

Table 3 reveals that the largest number of complaints with totaling 324,105, were submitted via the mobile banking channel. This indicates that a considerable proportion of BSI

customers opt to utilise the mobile application as the primary channel for submitting complaints. The Call Centre and Branch Offices also recorded a notable number of complaints, with 56,828 and 85,996 complaints, respectively. This demonstrates that customers continue to utilise a range of channels to lodge complaints. Consequently, BSI must prioritise the enhancement of efficiency and responsiveness across all channels.

A 100% of complaints were successfully resolved, indicating that BSI effectively addressed all grievances received in 2023. This is a positive indicator in terms of customer satisfaction management and transparency of the problem resolution process. The majority of complaints, 435,122 (93%), were related to the transaction process and facilities. This indicates that the primary source of customer dissatisfaction is the transaction process and facilities. Therefore, BSI should prioritise enhancing the stability and reliability of its transaction services and banking facilities.

Table 3. Complaint Receiving Channel

No.	Channel	Number of complaints
1	Call Center	56,828
2	Mobile Banking	324,105
3	Media Sosial	2,246
4	On-site Branch office	85,996
5	On-site Main office	706
Total		469,851
Status complaint (100% Closed)		
No.	Type of complaint	Number of complaints
1	Transaction Process and Facilities	435,122
2	External Banking Crime	5,150
3	Product	28,461
4	Services	1,118
Total complaint with 100% closed		469,851

Anti-Fraud Policy, Risk Management, and GCG Assessment

BSI has pledged to guarantee the uninterrupted integrity and transparency of its operations in all respects. In accordance with this commitment, the company has adopted a comprehensive anti-fraud policy that encompasses a range of stages, including prevention, detection, investigation, reporting, sanctioning, monitoring, evaluation, and follow-up. The objective of this policy is to identify, prevent and follow up on any form of fraud that may occur within the company. A comprehensive account of the policy, including detailed procedures, responsibilities, and reporting processes, is accessible to all interested parties via the company's official website. The results of BSI's governance assessment from the Indonesian Institute for Corporate Governance (IICG) indicated a score of 91.5, which is indicative of a very trusted predicate. The governance structure score was 30.27, the governance process score was 30.02, and the governance results score was 31.21 (BSI, 2023b). The results of the risk management self-assessment indicate that BSI has a score of 2 (low to moderate), which demonstrates the company's commitment to comply with OJK regulations and its implementation of effective risk management practices. Therefore, the financial and non-financial performance remains good even though BSI just attacked by cyber-crime.

Trend Analysis

Following the presentation of data on eight key financial indicators, an analysis was conducted using quarterly data for the three periods preceding and following the hacking incident. This section will present the trends of changes that occurred in each of these financial indicators, as well as provide an in-depth interpretation of the impact of the cyberattack on

BSI's financial stability. The results of the trend analysis demonstrate notable alterations in the following financial indicators:

Trend Analysis Prior to the Cyberattack

Table 4 below illustrates the trend changes in BSI's eight key financial indicators prior to the cyberattack. The calculation of trends is based on the percentage change from the value of the indicator in the base period (June 2022) to the following three periods. Furthermore, trend averages are presented in order to provide an overview of the changes observed in the indicators over the period under analysis.

Table 4. Trend Indicator before cyber-attack

Trend before cyber-attack				
	June-Sept 2022	**June-Dec 2022**	**June 2022 - Mar 2023**	**Average**
DEPOSIT	0.21%	6.88%	10.05%	5.71%
ASSET	0.96%	10.23%	12.95%	8.05%
FDR	4.24%	1.57%	1.28%	2.36%
ROA	2.46%	-2.46%	22.17%	7.39%
ROE	-1.25%	-4.64%	2.83%	-1.02%
NPF	-20.27%	-22.97%	-27.03%	-23.42%
CAR	-0.71%	18.50%	19.10%	12.30%
BOPO	-0.64%	1.85%	-6.51%	-1.77%
RISK	0	0	0	0

As illustrated in table 4, certain indicators exhibited notable fluctuations prior to the occurrence of the hacking incident. This analysis provides a basis for comparing the financial performance of BSI subsequent to the cyberattacks. The trend of change in deposits demonstrates a gradual increase, with an average of 5.71%. This increase indicates that customer confidence in the bank remains high, despite fluctuations in the period under analysis. The total assets exhibited an upward trajectory, with an average growth rate of 8.05%. This indicates consistent growth in the bank's assets, which is a positive indicator of financial stability and the bank's ability to manage its assets. The FDR trend shows an increase with an average of 2.36%. This increase reflects the bank's growing effectiveness in redirecting third-party funds into productive financing, although there are minor fluctuations. The ROA trends exhibit considerable volatility, with an average of 7.39%. The considerable increase observed in the final quarter may be indicative of enhanced asset utilisation efficiency, resulting in augmented profitability. The ROE trend exhibits an average value of -1.02%, thereby indicating a decline in the efficiency of equity utilisation during certain periods.

Nevertheless, the rise observed in the final quarter indicates the possibility of further advancement. The NPF trend exhibited a notable decline, with an average of -23.42%. This decline suggests an enhancement in the quality of the bank's financing assets and more effective risk management. The trend in the capital adequacy ratio (CAR) exhibited an upward trajectory, with an average increase of 12.30%. This suggests that the bank has sufficient capital to withstand potential losses, which is an important indicator in assessing financial stability. The BOPO trend demonstrates a degree of volatility, with an average value of -1.77%. This fluctuation indicates that the bank would benefit from improvements in operational efficiency, with a view to reducing operating expenses in comparison to income generated. The BSI has demonstrated its capacity to maintain effective risk management, as evidenced by its consistent score of 2.

A review of the trend analysis for each indicator indicates that, despite fluctuations in some indicators, BSI's financial performance exhibited a favourable trajectory prior to the hacking incident. The observed increases in deposits, assets, and CAR indicate that the bank is in a favourable financial position and possesses the capacity to effectively manage risks. Nevertheless, greater attention must be devoted to operational efficiency and equity utilisation.

Trend Analysis After to the Cyberattack

A trend analysis of each of BSI's key financial indicators subsequent to the hacking incident, based on quarterly data in Table 5, can be described as follows: Subsequent to the cyber-attack, the trend of deposits exhibited an increase, with an average of 12.63%. This increase is notable in comparison to the preceding period, suggesting that the bank was able to sustain and potentially enhance customer confidence in the wake of the incident. The trend in assets demonstrated an increase, with an average growth rate of 9.62%. Although slightly lower than the pre-hacking period, this increase nevertheless reflects a steady growth in the bank's assets, thereby demonstrating BSI's ability to maintain financial stability. The FDR trends exhibited a decline, with an average of -3.91%. This decline suggests that BSI encountered difficulties in redirecting third-party funds into productive financing following the cyber-attack. ROA trends exhibited fluctuations, with an average of 1.69%. Despite a decline in the initial period following the hack, the subsequent increase indicates that BSI began to recuperate and enhance the efficacy of utilizing assets to generate profits. The ROE trend demonstrated a decline, with an average of 0.42%.

Table 5. Trend Indicator After cyber-attack

Trend After Cyber-Attack				
Indicator	**Jun-Sept 2023**	**Jun-Dec 2023**	**June 2023 - Mar 2024**	**Average**
DEPOSIT	3.80%	16.34%	17.75%	12.63%
ASET	1.99%	12.76%	14.12%	9.62%
FDR	0.58%	-6.91%	-5.41%	-3.91%
ROA	-0.85%	-0.42%	6.36%	1.69%
ROE	-2.43%	-2.26%	5.96%	0.42%
NPF	-1.61%	-11.29%	-11.29%	-8.06%
CAR	2.39%	3.81%	4.61%	3.61%
BOPO	0.79%	0.56%	-2.72%	-0.46%
RISK	0	0	0	0

These findings suggest that the efficacy of leveraging equity to generate profits has diminished in the wake of the cyberattack, although there was a modest uptick in the final period. The NPF trend exhibited a decline, with an average decrease of 8.06%. This decline suggests an enhancement in the caliber of financing assets, which implies that BSI's credit risk management remains efficacious in the aftermath of the hacking incident. The CAR trend exhibited an increase, with an average of 3.61%. This suggests that BSI was able to maintain a sufficient level of capital adequacy to absorb potential losses following the cyberattack. The BOPO trend exhibited fluctuations, with an average of -0.46%. Although there was a decline in operational efficiency in some periods, the overall trend demonstrates that BSI made efforts to enhance its operational efficiency in the wake of the hacking incident.

The post-hacking trend analysis demonstrates that, although BSI encountered some difficulties in the areas of financing disbursement and equity utilisation, the bank was nevertheless able to sustain growth in both assets and deposits. The enhancements in NPF and CAR demonstrate effective risk management and capital adequacy. Nevertheless, further

initiatives are required to enhance operational efficiency and the effective utilisation of equity. With regard to risk management, the figures remain at a low-to-moderate level (2).

4.3.3 Comparison of Average Trends Before and After the Hacking Incident Table-6 displays the average trend of changes in the eight key financial indicators of Bank Syariah Indonesia (BSI) before and after the hacking incident, as well as the difference in increase or decrease in each indicator.

Table 6. Average of Trend

Indicator	Average of trend		Increase/decrease
	Before cyber-attack	After cyber attack	
DEPOSIT	5.71%	12.63%	7%
ASSET	8.05%	9.62%	2%
FDR	2.36%	-3.91%	-6%
ROA	7.39%	1.69%	-6%
ROE	-1.02%	0.42%	1%
NPF	-23.42%	-8.06%	15%
CAR	12.30%	3.61%	-9%
BOPO	-1.77%	-0.46%	1%
RISK	0	0	0

The average 7% increase in deposits demonstrates that BSI was able to markedly enhance customer confidence in the wake of the cyber-attack. This may be attributed to the implementation of efficacious recovery strategies and the maintenance of effective communication with customers. The mean value of assets demonstrated an increase of 2%. Although this increase was not as considerable as that observed in deposits, it nevertheless demonstrates a consistent expansion in the bank's assets subsequent to the cyber-attack. The average FDR exhibited a decline of 6%, suggesting that BSI encountered challenges in redirecting third party funds into productive financing following the cyber-attack. This could be attributed to the heightened caution in disbursing financing due to the elevated risk profile. The ROA exhibited a decline of approximately 6%, suggesting a reduction in the efficiency with which assets were utilized to generate profits following the cyber-attack. This may be indicative of a detrimental impact on the bank's profitability resulting from the hacking incident. The return on equity (ROE) exhibited an average increase of 1%.

Although modest in scale, this increase signals an enhancement in the utilisation of equity as a means of generating profit in the wake of adverse events. The net profit factor (NPF) exhibited an average improvement of 15%, indicative of enhanced asset quality in financing. The considerable reduction in nonperforming loans (NPF) demonstrates that BSI's credit risk management strategy remained effective in the aftermath of the cyberattack. The CAR exhibited an average decline of 9%, suggesting that BSI experienced a reduction in capital adequacy following the cyberattack. Nevertheless, the positive CAR value indicates that the bank continues to possess adequate capital adequacy. The BOPO ratio exhibited an average increase of 1%. Although modest in scale, this increase suggests that BSI must enhance its operational efficiency in the wake of the hacking incident.

The analysis of the average increase/decrease trend indicates that, despite the challenges experienced by BSI following the cyberattack, including a reduction in FDR and ROA, the bank was able to maintain and even enhance certain pivotal financial indicators, such as DPK and NPF. The enhancements in NPF and DPK suggest that customer confidence and credit risk management remain robust, whereas the declines in FDR and ROA indicate areas that necessitate further attention for recovery and enhanced financial performance.

Analysis of SDGs 16 Achievement and Sharia Compliance

The close influence of corporate stability in this digital era, a solid cyber security framework is needed (Mishra, Alzoubi, Anwar, and Gill (2022). This is in line with SDG 16 where everyone should be guaranteed access to justice. As in the case of BSI, where even though it was broken into the data, but BSI is still able to show its existence. By maintaining cyber security, it will support SDG 16 (Sulich, Rutkowska, Krawczyk-Jezierska, Jezierski, & Zema, 2021). Because this is in accordance with the SDG 16 goals which are expected to ensure security, accountable, fairness of the bank.

The relationship between cyber-attacks in banking, Sustainable Development Goals (SDGs), and Sharia compliance is multifaceted and increasingly relevant in today's digital economy. Cyber-attacks pose significant threats to financial institutions, including Islamic banks, which are governed by Sharia principles that emphasize ethical and responsible financial practices. The integrity of banking systems is crucial for achieving SDGs, particularly those related to economic growth and reduced inequalities. Cybersecurity breaches can undermine public trust in financial institutions, leading to decreased investment and economic instability, which directly contradicts the objectives of sustainable development (Siswanti, 2024). Furthermore, the digital transformation of banking, while offering opportunities for enhanced efficiency and transparency, also introduces vulnerabilities that can be exploited by malicious actors, thereby jeopardizing the sustainability of banking operations and their alignment with Sharia principles (Andespa, 2024). Islamic banking, which operates under Sharia law, emphasizes risk-sharing and ethical investments, making it particularly sensitive to the implications of cyber threats. The adherence to Sharia principles necessitates a commitment to transparency and accountability, which can be compromised by cyber-attacks that lead to data breaches or financial fraud (Andespa, 2024).

The negative impact of such incidents extends beyond individual institutions; it can affect entire communities that rely on these banks for sustainable economic development. For instance, the Islamic finance sector has been identified as a key player in promoting sustainable development through ethical investments, but its potential can only be realized if robust cybersecurity measures are in place to protect against threats that could undermine its operations (Siswanti, 2024). Thus, the intersection of cybersecurity, Islamic banking, and SDGs highlights the need for comprehensive strategies that address both technological vulnerabilities and the ethical imperatives of Sharia compliance. Moreover, the integration of cybersecurity measures within Islamic banking frameworks can enhance the resilience of these institutions against cyber threats, thereby supporting the broader goals of sustainable development. By investing in advanced cybersecurity technologies and fostering a culture of awareness among employees and customers, Islamic banks can mitigate the risks associated with cyber-attacks (Okokpujie et al., 2023). This proactive approach aligns with the SDGs, particularly those focused on industry innovation and infrastructure (SDG 9) and peace, justice, and strong institutions (SDG 16).

Furthermore, the promotion of green financing and sustainable investment strategies within Islamic banking can serve as a model for other financial institutions, demonstrating how adherence to ethical principles can coexist with the demands of modern technology and cybersecurity (Bansal, 2023). In conclusion, the relationship between cyber-attacks, banking, SDGs, and Sharia compliance underscores the necessity for a holistic approach that integrates ethical considerations with technological advancements to foster a sustainable financial ecosystem.

Bank Syariah Indonesia (BSI) is a financial institution that operates in accordance with Islamic principles and is therefore obliged to comply with Islamic law in all aspects of its operations. The hacking incident experienced by BSI in 2023 represented a significant challenge for the bank in maintaining compliance with sharia principles, particularly in the

areas of amanah (trust) and hifz al-mal (protection of property) Maghaireh (2008). In accordance with the 2023 Shariah Supervisory Board (DPS) Report, BSI has demonstrated continued compliance with the fatwas issued by the National Shariah Council (DSN-MUI) with respect to the products and services it offers. All financing products, deposits, and technology-based services remain in compliance with DSN-MUI fatwas, including digital banking products utilised by customers for their everyday transactions. This encompasses the compliance of products with regard to the Sharia contracts utilised in transactions, including those pertaining to Mudharabah, Musyarakah, and Murabahah.

CONCLUSION

In conclusion, The fundamental benefits of cryptocurrency cannot be manipulated and is transparent, therefore it has the potential to revolutionise numerous sectors and enterprises around the world. The blockchain revolution will simplify transactions at all levels of society, including MSMEs and farmers, who already benefit from internet access.

With current technical advancements, developing country has the ability to grow at a rate comparable to other countries, especially established countries that are actively building business through this technology. Blockchain technology has the potential to boost corporate competitiveness and reinforce developing country, for example, Indonesia's position as the only Southeast Asian country with a GDP that ranks among the top 20 in the world.

The potential benefits of blockchain have drawn attention from both business and governments around the world. Advanced economies see adoption of new digital technologies to fuel economic growth and improve business and governmental processes. Blockchain technology offers promising solutions especially for transactions where trust is prominent, with its transparency, auditability, and accountability features.

The study's findings reveal that the effectiveness of blockchain applications and their contribution to country development are dependent on a country's degree of development, politicians' attitudes towards transparency, and the country's technological infrastructure. For example, the high level of political instability in many African nations may make it difficult to deploy blockchain initiatives.

Another issue is the degree of technology infrastructure required to execute blockchain solutions. Many developing countries lack the digital infrastructure and cash required to construct such infrastructure. However, infrastructural constraints may also be opportunities. A lack of telephone infrastructure, as observed two decades ago, led to a more The findings of this study indicate that, despite the cyber-attack incident, BSI was able to maintain and even enhance customer confidence, as evidenced by the increase in third-party funds. The average increase of 9.62% in stable asset growth after the attack is indicative of BSI's capacity to maintain financial stability and growth. The decline in FDR indicates that there are difficulties in converting third party funds into productive financing, which suggests that there has been an increase in caution in financing activities following the attack. The decline in ROA suggests a reduction in the efficacy of asset utilisation in generating profits subsequent to the cyberattack. The slight increase in ROE following the attack suggests an attempt to more effectively utilise equity for profit generation, although further enhancements are still required. The considerable reduction in NPF subsequent to the attack is indicative of effective credit risk management and enhanced financing asset quality. The decline in CAR suggests a reduction in capital adequacy, although the ratio remains positive, indicating that the institution has sufficient capital to absorb potential losses. A modest uptick in BOPO signals the necessity for enhanced operational efficiency to curtail costs in relation to revenue following the attack. The BSI has demonstrated an ability to maintain financial stability, which may be attributed to the implementation of effective risk management strategies at an early stage. This has enabled the BSI to withstand the impact of a cyber-attack, minimising its adverse effect on performance.

Overall, the analysis showed that although BSI faced several challenges in the aftermath of the cyber -attack, such as reduced efficiency in the use of assets and capital, the bank showed resilience in maintaining customer confidence, asset growth and credit quality. The findings highlight the importance of robust risk management and operational efficiency in maintaining financial stability.

Based on the results of the IICG assessment, which gives a score of 91.5 with the predicate "highly reliable", it can be concluded that BSI not only has good corporate governance but has also implemented Sharia principles in its operations. Strong governance structures, processes and outcomes reflect BSI's adherence to the principles of amanah, hifz al-mal and justice, which are at the core of Sharia principles. With good governance, BSI is able to maintain stability and customer confidence even after hacking incidents, demonstrating the bank's ability to balance profitability and sharia compliance. It also supports the achievement of SDG 16, particularly in relation to building strong, fair, accountable and transparent institutions.

REFERENCES

Andespa, R. (2024). Sustainable development of islamic banks by creating islamic branding: challenges, importance, and strategies of islamic branding. International Journal of Sustainable Development and Planning, 19 (2), 637-650. https://doi.org/10.18280/ijsdp.190221.

Azizah, B. P., & Udayana, I. B. N. (2022). Pengaruh Kepercayaan Dan Kepuasan Terhadap Loyalitas Nasabah Bank Syariah. Jurnal Ilmiah Manajemen “E M O R,” 6(1), 88. https://doi.org/10.32529/jim.v6i1.1504

Bank Syariah Indonesia. (2023). Laporan Publikasi Keuangan Triwulan Oktober (investor daily). 2022 (September), 14040. https://ir.bankbsi.co.id/misc/Laporan-Keuangan/Tahun-Laporan-2023/Laporan-Publikasi-Triwulan-Sep-ID.pdf bankbsi. (2022). Laporan Keuangan Triwulan

Bansal, N. (2023). Green financing as a bridge between green banking strategies and environmental performance in Punjab, India. International Journal of Sustainable Development and Planning, 18(10), 3155-3167. https://doi.org/10.18280/ijsdp.181017

BSI. In Https://Ir.Bankbsi.Co.Id/. https://ir.bankbsi.co.id/financial_reports.html

BI. (2004). Lampiran1 –Matrik Perhituangan /Analisis risiko Komponen Faktor. Lampiran 1 a Lampiran 1 b Lampiran 1 c Lampiran 1 d Lampiran 1 e Lampiran 1 f Permodalan (Capital) Kualitas Aset (Asset Quality) Manajemen (Manageme).

Bpptik. (2023). Jenis-jenis Serangan Siber di Era Digital. Kementrian Kominfo. https://bpptik.kominfo.go.id/Publikasi/detail/jenis-jenis-serangan-siber-diera-digital

BSI. (2022a). https://www.bankbsi.co.id/.

BSI. (2023a). Best Islamic Bank in Indonesia Best Islamic Finance Bank Penghargaan pihak ketiga BSI Mobile. 2022, 2023. https://www.bankbsi.co.id

BSI. (2023b). Ekspansi dan Akselerasi Bisnis Untuk Pertumbuhan Berkelanjutan. Laporan Tahunan 2023 PT Bank Syariah Indonesia TBK. https://ir.bankbsi.co.id/misc/AR/AR2023-ID.pdf

BSI. (2023c). Laporan Keuangan Triwulan Maret 2023. https://www.bankbsi.co.id/.

Burhan, F. A. (2024). Top 10 Bank Syariah di Indonesia Terbaru, Nomor satu Aset Tembus Rp. 350 Triliun. Bisnis.Com. https://finansial.bisnis.com/read/20240516/231/1765830/top-10-banksyariah-di-indonesia-terbaru-nomor-satu-aset-tembus-rp350-triliun

Cavaliere, L. P. L., Subhash, N., Rao, P. V. D., Mittal, P., Koti, K., Chakravarthi, M. K., Regin, R. (2021). The Impact of Internet Fraud on Financial Performanceof Banks. Turkish Online Journal of Qualitative Inquiry, 12(6), 8126-8158.

Chapra, M. U. (2008). Vision of Development in the Light of Maqāsid Al-Sharī'ah. January 2008. https://doi.org/10.13140/RG.2.1.4188.5047

Committee, B. (2011). BASEL III a global regulatory framework. In Basel Committee on Banking Supervision, Basel (Issue June). http://www.bis.org/publ/bcbs189_dec2010.pdf

Deloitte. (2016). Cyber Crisis Management: Readiness, Response, and Recovery.

Gar, R. H. G. (2018). Managerial Accounting (16th ed.). McGraw-Hill Education. https://ebooks.papacambridge.com/directories/CAIE/CAIEebooks/upload/managerialaccounting,16thedition.pdf

Hardiansyah, Z. (2023). Kronologi Layanan BSI Error , Down Berhari-hari dan Dipalak Hacker Ransomware Ratusan Miliar. Kompas.Com. https://tekno.kompas.com/read/2023/05/17/09010077/kronologi-layanan-bsieror-down-berhari-hari-dan-dipalak-hacker-ransomware?page=all

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. Journal of Information Security and Applications, 58, 102726. doi: https://doi.org/10.1016/j.jisa.2020.102726

Indonesia, G. B. (2023). Peraturan Bank Indonesia Nomor 5 Tahun 2023 Tentang Pembiayaan Likuiditas Jangka Pendek Berdasarkan Prinsip Syariah Bagi Bank Umum Syariah. https://peraturan.bpk.go.id/Details/260647/peraturanbi-no-5

Kallman, J. (2023). Melaju Dengan Aksi Berkelanjutan. 1–100. https://ir.bankbsi.co.id/misc/SR/SR2023-ID.pdf

Kaufmann, D., Kraay, A., & Mastruzzi, M. (2009). Governance matters VII: Aggregate and individual governance indicators 1996-2007. Non-State Actors as Standard Setters, June, 146–188. https://doi.org/10.1017/CBO9780511635519.007

Laporan Keuangan BSI .2024. https://ir.bankbsi.co.id/misc/AR/AR2023ID/2/index.html

Maghaireh, A. (2008). Shariah Law and Cyber-Sectarian Conflict: How can Islamic Criminal Law respond to cyber crime? International Journal of Cyber Criminology; Thirunelveli, 2(2), 337-345.

Maseka, N. (2021). Peace, Justice and Strong Institutions. Encyclopedia of Law and Development, March. https://doi.org/10.4337/9781788117975.00064

Maulana, L., & Fitriana, N. (2023). Analisis Dampak Insiden BSI Eror Dan Dugaan Hacking Bank Syariah Indonesia (BSI) Terhadap Kepercayaan Dan Loyalitas Nasabah Bank Syariah Indonesia Di Kabupaten Subang. Jurnal Ilmu Islam, 7(3), 1755–1768.

Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. Computers & Security, 120, 102820. https://doi.org/10.1016/j.cose.2022.102820

Okokpujie, K., Kennedy, C., Nnodu, K., & Noma-Osaghae, E. (2023). Cybersecurity awareness: investigating students' susceptibility to phishing attacks for sustainable safe email usage in academic environment (a case study of a nigerian leading university). International Journal of Sustainable Development and Planning, 18(1), 255-263. https://doi.org/10.18280/ijsdp.180127

Simamora. (2024). Rasio BOPO dan CIR Tinggi Sejumlah Bank ini Berupaya Tekan Beban Biaya Tahun ini. Kontan.Co.Id. https://keuangan.kontan.co.id/news/rasio-bopo-dan-cir-tinggi-sejumlahbank-ini-berupaya-tekan-beban-biaya-tahun-ini

Siswanti, I. (2024). Digital transformation's moderating role on financing and capital quality impacts for sustainable islamic rural banking in indonesia. International Journal of Sustainable Development and Planning, 19(3), 991-1001. https://doi.org/10.18280/ijsdp.190317

Sulich, A., Rutkowska, M., Krawczyk-Jezierska, A., Jezierski, J., & Zema, T. (2021). Cybersecurity and Sustainable Development. Procedia Computer Science, 192, 20-28. doi: https://doi.org/10.1016/j.procs.2021.08.003

OJK. (2016). POJK No 11 Tentang Konversi KPMM. OJK.Go.Id, 1–82.

OJK. (2017a). Prinsip dan Konsep Dasar Perbankan Syariah. Otoritas Jasa Keuangan. https://ojk.go.id/id/kanal/syariah/tentang-syariah/Pages/Prinsipdan-Konsep-PB-yariah.aspx

OJK. (2017b). Stabilitas Sistem Keuangan. Otoritas Jasa Keuangan. https://ojk.go.id/id/kanal/perbankan/stabilitas-sistemkeuangan/Pages/Ikhtisar.aspx

Otoritas Jasa Keuangan. (2022). Ringkasan Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 2/Pojk.03/2022 Tentang Penilaian Kualitas Aset Bank Umum Syariah Dan Unit Usaha Syariah Latar. 1, הארץ(8.5.2017), 2003– 2005.

Ummul, Aiman Hasda, Suryadin, Masita, Eka Sari. (2022). Metodologi Penelitian Kuantitatif. In Yayasan Penerbit Muhammad Zaini.

UN. (2023). What is goal 16 - Peace, Justice, and Strong Institutions? Department of Global Communications, 1–2. https://www.un.org/sustainabledevelopment/wpcontent/uploads/2019/01/Goal-16-Fast-Facts.pdf

Van Greuning, H., & Brajovic-Bratanovic, S. (1999). Analyzing banking risk. In Analyzing banking risk. https://doi.org/10.1596/0-8213-4417-x

Van Halderen, G., Bidarbakht Nia, A., & Bisogno, E. (2019). SDG16: Peace, Justice and Strong Institutions Walking through Asian and Pacific Territories 1. August. http://www.unescap.org/resource-series/sd-working-papersvida. (2024). 5 Alasan Industri Keuangan Menjadi Target Serangan Siber. Web Vida. https://vida.id/id/blog/5-alasan-industri-keuangan-menjadi-targetserangan-siber

Wardhana, M. A., Hayati, N., & Mustaqim, Y. (2023). Kepuasan Elektronik, Loyalitas Elektronik Dan Kunjungan Kembali Situs Pada Tindak Kejahatan Siber (Cyber Crime) Perbankan. Jurnal Ekonomi Syariah Dan Akuntansi, 4(2), 91–97. https://ejr.umku.ac.id/index.php/JEISA/article/view/2277%0A, https://ejr.umku.ac.id/index.php/JEISA/article/download/2277/1269

Zefanya Aprilia &, T. N. (2023). Serangan Siber di Sektor Keuangan, bukan cuma BCA & BPD Bali. CNBC Indonesia. https://www.cnbcindonesia.com/market/20231117134511-17-489875/serangan-siber-di-sektor-keuangan-bukan-cuma-bca-bpd-bali

Chiu, W., Zeng, S., & Cheng, P. S. T. (2016). The influence of destination image and tourist satisfaction on tourist loyalty: a case study of Chinese tourists in Korea. *Journal International Journal of Culture, Tourism, and Hospitality Research*, *10*(2), 223-234.

Çoban, S. (2012). The Effects of the Image of Destination on Tourist Satisfaction and Loyalty: The Case of Cappadocia *European Journal of Social Sciences*, *29*(2), 222-232.

Gengqing, C. (2005). *A Study of Developing Destination Loyalty Model.* (Doctor of Philosophy), Oklahoma State University, Oklahoma

Hajjid, I., Soetomo, H., Kristaung, R., & Susanto, A. (2022). Empirical Testing Of Emotional Brand Attachment and Brand Love Mediation Between Brand Satisfaction and Brand Loyalty. *International Journal of Digital Entrepreneurship and Business*, *3*(2), 49-59.

Halim, P., Swasto, B., Hamid, D., & Firdaus, M. R. (2014). The Influence of Product Quality, Brand Image, and Quality of Service to Customer Trust and Implication on Customer Loyalty (Survey on Customer Brand Sharp Electronics Product at the South Kalimantan Province). *European Journal of Business and Management*, *6*, 159-166.

Hudson, S., & Thal, K. (2013). The Impact of Social Media on the Consumer Decision Process: Implications for Tourism Marketing. *Journal of Travel & Tourism Marketing*, *30*, 156-160. https://doi.org/10.1080/10548408.2013.751276

Iqbal, U. P., Hamza, V. K., Nooney, L. K., & Sainudeen, S. (2023). Exploring the determinants of destination satisfaction: a multidimensional approach. *Future Business Journal, 9*(1), 59. https://doi.org/10.1186/s43093-023-00240-1

Judmar, Z., Joseph, R. A., Cristobal Sannelyn, Cortes Mark Lester Daxen, & G, L. B. L. (2024). From Feeling to Fidelity: Exploring the Role of Emotional Structures on Brand Satisfaction and Loyalty. *International Journal of Advanced Multidisciplinary Research and Studies, 4*(3), 569-574.

Karim, K., Ilyas, G. B., Umar, Z. A., Tajibu, M. J., & Junaidi, J. (2023). Consumers' awareness and loyalty in Indonesia banking sector: does emotional bonding effect matters? *Journal of Islamic Marketing, 14*(10), 2668-2686. https://doi.org/10.1108/JIMA-03-2022-0092

Kim, S.-H., Holland, S., & Han, H.-S. (2013). A Structural Model for Examining how Destination Image, Perceived Value, and Service Quality Affect Destination Loyalty: a Case Study of Orlando. *International Journal of Tourism Research, 15*, 313-328. https://doi.org/10.1002/jtr.1877

Kozak, M., & Rimmington, M. (2000). Tourist Satisfaction with Mallorca, Spain, as an Off-Season Holiday Destination. *Journal of Travel Research, 38*(3), 260-269. https://doi.org/10.1177/004728750003800308

Lamidi, & Rahadhini, M. D. (2013). Pengaruh Citra Objek Wisata Umbul Tlatar Boyolali Terhadap Loyalitas Pengunjung Dengan Kepuasan Sebagai Variabel Mediasi. *Jurnal Ekonomi dan Kewirausahaan, 13*(1), 139-150.

Luvsandavaajav, O., Narantuya, G., Dalaibaatar, E., & Raffay, Z. (2022). A Longitudinal Study of Destination Image, Tourist Satisfaction, and Revisit Intention. *Journal of Tourism and Services, 13*(24), 128-149. https://doi.org/10.29036/jots.v13i24.341

Mahdzar, M., Shuib, A. S. M., Ramachandran, S., & Afandi, S. H. M. (2015). *The role of destination attributes and memorable tourism experience in understanding tourist revisit intentions*.

Manoppo, S., & Santosa, S. B. (2023). Pengaruh Destination Image, Destination Service Quality, Perceived Value Terhadap Revisit Intention Dengan Tourist Satisfaction Sebagai Variabel Intervening (Studi Pada Wisata Taman Nasional Bunaken). *Diponegoro Journal Of Management, 12*(3), 1-10.

Noori, A. (2019). An Investigation On How Brand Image Influences Tourist Destination And Customer Satisfaction: A Case Of The Tourism Secto. *International Journal Of Scientific & Technology Research, 8*(11), 3553-3559.

Oliver, R. L. (1999). Whence Consumer Loyalty? *Journal of Marketing, 63*(4_suppl1), 33-44. https://doi.org/10.1177/00222429990634s105

Oppermann, M. (2000). Tourism Destination Loyalty. *Journal of Travel Research, 39*(1), 78-84. https://doi.org/10.1177/004728750003900110

Paludi, S. (2016). Analisis Pengaruh Electronic Word Of Mouth (E-Wom) Terhadap Citra Destinasi, Kepuasan Wisatawan, Dan Loyalitas Destinasi Perkampungan Budaya Betawi (PBB) Setu Babakan Jakarta Selatan. *Jurnal Ekonomi, Pendidikan Dan Pariwisata, 11*(1), 1-22.

Pratminingsih, S. A., Rudatin, C. L., & Rimenta, T. (2014). Roles of Motivation and Destination Image in Predicting Tourist Revisit Intention: A Case of Bandung – Indonesia *International Journal of Innovation, Management and Technology, 5*(1), 19-24.

Qomariah, N. (2018). Impact of Customer Value, Brand Image and Product Attributes to Satisfaction and Loyalty Tourism Visitors in Jember Regency. *Mediterranean Journal of Social Sciences, 8*, 129-135. https://doi.org/10.2478/mjss-2018-0105

Ramseook-Munhurrun, P., Seebaluck, V. N., & Naidoo, P. (2015). Examining the Structural Relationships of Destination Image, Perceived Value, Tourist Satisfaction and Loyalty:

Case of Mauritius. *Procedia - Social and Behavioral Sciences, 175*, 252-259. doi: https://doi.org/10.1016/j.sbspro.2015.01.1198

Shafaei, F., & Mohamed, B. (2015). Involvement and brand equity: A conceptual model for Muslim tourists. *International Journal of Culture, Tourism and Hospitality Research, 9*, 54-67. https://doi.org/10.1108/IJCTHR-06-2014-0050

Shafiee, S., Rajabzadeh Ghatari, A., Hasanzadeh, A., & Jahanyan, S. (2020). Smart Tourism Destinations:A Systematic Review of Research Using the Paradigm Funnel Approach. *Tourism Management Studies, 15*(49), 33-62. https://doi.org/10.22054/tms.2020.11045

Sun, X., Chi, C., & Xu, H. (2013). Developing destination loyalty: The case of hainan island. *Annals of Tourism Research, 43*, 547–577. https://doi.org/10.1016/j.annals.2013.04.006

Thakur, R. (2016). Understanding Customer Engagement and Loyalty: A Case of Mobile Devices for Shopping. *Journal of Retailing and Consumer Services, 32*(C), 151-163.

Thompson, D. V., & Malaviya, P. (2013). Consumer-Generated Ads: Does Awareness of Advertising Co-Creation Help or Hurt Persuasion? *Journal of Marketing, 77*(3), 33-47. https://doi.org/10.1509/jm.11.0403

Zhang, H., Fu, X., Cai, L., & Lu, L. (2014). Destination image and tourist loyalty: A meta-analysis. *Tourism Management, 40*, 213-223. doi: 10.1016/j.tourman.2013.06.006

Zikmund, W. G., McLeod, R., & Gilbert, F. W. (2003). *Customer Relationship Management: Integrating Marketing Strategy and Information Technology*: Wiley.