

CITATION

Aminah A, Damayanti T, Murtini H, Sari YP, (2026). Financial Resilience after a Cyberattack in Islamic Banking: A CAMEL Case Study of Bank Syariah Indonesia. *Ijomata International Journal of Tax and Accounting*. 7 (4), doi: 10.61194/ijtc.v7i4.2396

TYPE Original Research

PUBLISHED 31 October 2026
DOI 10.61194/ijtc.v7i4.2396
VOL 7 Issue 4 October 2026

COPYRIGHT

© 2026 Aminah, Damayanti, Murtini and Sari. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner(s) are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.

Financial Resilience after a Cyberattack in Islamic Banking: A CAMEL Case Study of Bank Syariah Indonesia

Aminah Aminah¹, Tri Damayanti², Henny Murtini³, Yenni Priatna Sari⁴

¹²Universitas Bandar Lampung, Lampung, Indonesia, ³Universitas Negeri Semarang, Central Java, Indonesia, ⁴Universitas Harkat Negeri, Central Java, Indonesia

Correspondence: tri.damayanti@ubl.ac.id²

Abstract

Cybercrime poses significant risks to the banking sector through operational disruptions, data breaches, declining public trust, and increased recovery costs. In Islamic banking, these risks are particularly important because customer confidence and institutional integrity are closely linked to ethical and Shariah principles. Despite growing concerns over cyber resilience, empirical evidence on annual financial performance following major cyber incidents in Islamic banking remains limited, particularly from a CAMEL-based perspective. This study addresses this gap by assessing the annual financial resilience of Bank Syariah Indonesia (BSI), comparing the pre-incident fiscal year (2022) with the incident year (2023) using audited consolidated financial statements and a comparative case study approach. The analysis focuses on cumulative annual financial performance rather than short-term post-attack effects. The findings show that observed financial indicators did not deteriorate overall during the incident year: the capital adequacy ratio (CAR) increased from 20.29% to 21.04%, non-performing financing (NPF) decreased from 2.42% to 2.08%, and return on assets (ROA) increased from 1.98% to 2.35%. The Financing-to-Deposit Ratio (FDR) also increased from 79.37% to 81.73%, while information technology investment increased by 263%, from IDR 266 billion to IDR 968 billion. Overall, the findings indicate that annual financial soundness was maintained during the incident year, while the observed changes coincided with increased IT investment. These patterns should be interpreted as descriptive associations, as annual financial performance may also reflect broader economic conditions, institutional factors, and managerial decisions.

KEYWORDS

cybersecurity; financial resilience; CAMEL analysis; Islamic banking; risk management; IT investment.

Introduction

Cyberattacks pose significant risks to the banking sector by disrupting operations, compromising sensitive data, and eroding customer trust. In Islamic banking, these risks are particularly critical because trust is closely associated with Islamic ethical and Shariah principles. The 2023 cyberattack on Bank Syariah Indonesia (BSI), which temporarily disrupted banking services, highlighted the importance of understanding whether Islamic banks can maintain financial resilience following major cybersecurity incidents. Although cyberattacks are widely recognized for causing operational disruptions and financial as well as non-financial losses, empirical evidence on their implications for the annual financial resilience of Islamic banks remains limited. Existing studies have primarily focused on cybersecurity, operational continuity, and risk management, while comparatively little attention has been given to post-incident financial performance. This study addresses that gap by evaluating BSI's financial resilience before and after the cyberattack using the CAMEL framework.

Cyberattacks are increasingly prevalent and sophisticated, posing systemic threats to financial institutions that serve as the backbone of national and global economies.

Financial institutions not only facilitate payments, savings, and credit creation but also underpin critical economic functions, making them prime targets for cybercriminals (Gulyas & Kiss, 2023). Large-scale attacks can disrupt payment infrastructure, compromise sensitive data, and expand operational vulnerabilities as digitalization deepens the attack surface of banking systems. Such disruptions can have broader economic implications, including liquidity stress, reputational damage, and reduced confidence in financial systems.

The economic impact of cybercrime is increasing significantly. Recent studies indicate that global losses resulting from cybercrime are estimated to reach USD 10.5 trillion annually by 2025, highlighting the increasing economic consequences of cyber threats (Ramli et al., 2026). In Indonesia, this trend is equally concerning. Data from the National Cyber and Crypto Agency (BSSN) indicates that cyber incidents approached one billion cases in 2022, with malware accounting for the majority, followed by data leaks, Trojan attacks, and other forms of cyber threats. These figures highlight the urgent need for organizations to enhance cybersecurity awareness and strengthen their digital resilience.

The growing dependence on digital systems has made critical infrastructure—such as banking, energy, transportation, and healthcare—more vulnerable to cyber threats. Disruptions in these sectors can have far-reaching consequences for economic stability and public services. This concern became particularly evident in May 2023 when Bank Syariah Indonesia (BSI) experienced a major ransomware attack that disrupted banking services and exposed potential vulnerabilities in digital banking operations. The incident raised important questions regarding the ability of Islamic banks to maintain financial resilience and recover from cybersecurity disruptions. This incident demonstrates how cyberattacks can severely affect institutional operations and emphasizes the importance of integrating cybersecurity into organizational risk management strategies.

Within organizations, cyber assets include hardware, software, data, network infrastructure, user identities, and third-party systems. Damage to these assets not only results in direct financial losses, such as system recovery costs and infrastructure replacement, but also creates reputational risks. In the banking sector, where trust is a fundamental element, cyber incidents can significantly undermine customer confidence. Customers who perceive weaknesses in data protection may shift to other financial institutions, potentially affecting a bank's financial performance and long-term sustainability.

This issue became particularly salient in the case of Bank Syariah Indonesia (BSI), which experienced a cyber incident on 8 May 2023 that disrupted its banking systems and services (Bank Syariah Indonesia, 2023). BSI subsequently reported that corrective and recovery measures had been implemented, including efforts to strengthen its cybersecurity infrastructure (Bank Syariah Indonesia, 2023). The Financial Services Authority of Indonesia (OJK) reported that BSI's services were gradually returning to normal and that its supervisory and information technology examination teams were assessing the source of the disruption, with a forensic audit still underway (OJK, 2023). Separately, media reports indicated that the LockBit ransomware group had claimed responsibility for the incident and alleged that customer and employee data had been obtained; however, these claims were not independently verified (Reuters, 2023). Thus, the occurrence of the cyber incident, service disruption, and OJK examination are supported by official sources, whereas the attribution to LockBit and the alleged acquisition of customer and employee data should be treated as reported allegations rather than independently established facts. Beyond the

immediate operational disruption, cyber incidents may expose banks to financial, behavioural, and reputational risks, including potential customer attrition and changes in deposit behaviour. Prior research has likewise suggested that cybersecurity incidents may influence customer behaviour and short-term financial performance.

Existing studies on the 2023 cyberattack on Bank Syariah Indonesia (BSI) have primarily examined market and behavioural responses. For example, Fatikhatus Nisa & Cahyono (2024) focused on stock performance, while Timur et al. (2024) analysed customer churn, sentiment, and emotions following the incident. Although these studies provide valuable insights into external stakeholder reactions, they offer limited evidence regarding the bank's underlying financial resilience. Moreover, previous research has rarely employed a comprehensive framework to assess overall bank soundness after a cyberattack. The CAMEL framework, which evaluates capital adequacy, asset quality, management efficiency, earnings, and liquidity, provides a more integrated assessment of financial resilience. This perspective is particularly relevant in Islamic banking, where financial stability is closely linked to trust, governance, and Shariah compliance. Therefore, this study contributes to the literature by examining the financial resilience of BSI before and after the 2023 cyberattack using the CAMEL framework.

Empirical evidence on financial resilience following cyberattacks in Islamic banking remains limited despite the sector's distinctive governance and risk-sharing characteristics (Timur et al., 2024; Anand et al., 2026). Moreover, while prior studies largely emphasize the costs and adverse consequences of cyberattacks (Antczak, 2020; Razavi et al., 2023; Alsakini et al., 2024) less attention has been given to how management responses, cybersecurity investments, and recovery strategies may support financial resilience after such incidents.

Therefore, this study aims to evaluate the financial performance of Bank Syariah Indonesia before and after the 2023 cyberattack using the CAMEL framework. By comparing key financial indicators across the pre- and post-attack periods, this study seeks to provide a comprehensive assessment of the bank's financial resilience. In doing so, this research contributes to the literature by offering empirical evidence on how Islamic banks respond to cyber risks and by highlighting the importance of effective management strategies and IT investment in maintaining financial stability in the digital era.

Methods

This study employs a comparative case study design based on secondary financial data. The analysis applies the CAMEL framework to compare key financial ratios between the pre-incident fiscal year (2022) and the incident year (2023) in order to assess Bank Syariah Indonesia's financial resilience during the fiscal year in which the cyberattack occurred.

Research Type

This study employs a comparative case study design based on secondary financial data. Using the CAMEL framework, the study compares key financial ratios of Bank Syariah Indonesia during the pre-incident fiscal year (2022) and incident year (2023) to assess its financial resilience following the cyberattack. The case study approach enables an in-depth examination of a specific cybersecurity incident within its organizational and financial context.

Population and Sample/Informants

This study focuses on Bank Syariah Indonesia (BSI) as a purposively selected case. BSI was chosen because it is the largest Islamic bank in Indonesia and experienced a major cyberattack in May 2023, making it a relevant case for

Table 1. Data Sources and Financial Statement References for CAMEL Indicators

CAMEL Indicator	Source Document	Page	Note/Table
CAR	2022 Annual Report	p.15	Risk Profile / Capital Adequacy
	2023 Annual Report	p.15	
NPF	2022 Annual Report	p.15	Financing Quality
	2023 Annual Report	p.15	
ROA	2022 Annual Report	p.15	Statement of Profit or Loss
	2023 Annual Report	p.15	
CIR	2022 Annual Report	p.15	Financial Ratio Table
	2023 Annual Report	p.15	
FDR	2022 Annual Report	p.15	Liquidity Ratio
	2023 Annual Report	p.15	
IT Investment	2022 Annual Report	p.226	Information Technology / Capital Expenditure
	2023 Annual Report	p.226-231	

Source: BSI's Annual Report (2022, 2023)

Table 2. The assessment of the CAMEL Indicators

Indicator(s)	Measurement(s)	Score(s)*	Value(s)*
Capital	$CAR = \frac{Capital}{Risk - Weighted Assets} \times 100\%$	> 8%	Sound
		7.9 – 8 %	Moderate
		6.5 – 7.9 %	Less
		< 6.5%	Unsound
Asset quality	$NPF = \frac{Total\ Default\ (Financing)}{Total\ Financing} \times 100\%$	< 2%	Sound
		2 – 5%	Moderate
		5 – 8%	Less
		8 – 12%	Unsound
		>12%	Fundamentally unsound
Management	$NPM = \frac{Net\ Income}{Operating\ Income} \times 100\%$	≥ 100%	Sound
		81– 100%	Moderate
		66– 81%	Less
		51– 66%	Unsound
		< 51%	Fundamentally unsound
Earnings	$ROA = \frac{Net\ income}{Total\ Asset} \times 100\%$	>1.22 %	Sound
		0.99 – 1.21%	Moderate
		0.77 – 0.98%	Less
		< 0.76%	Unsound
	$CIR = \frac{Operating\ Expenses}{Operating\ Income} \times 100\%$	< 93.52%	Sound
93.52 – 94.73%		Moderate	
94.73 – 95.92%		Less	
> 95.92%		Unsound	
Liquidity	$FDR = \frac{Total\ Financing}{Total\ Deposits} \times 100\%$	< 94.75%	Sound
		94.75 – 98.75%	Moderate
		98.75 – 102.25%	Less
		> 102.25%	Unsound

Source: Bank Indonesia, accessed in 2025

Table 3. Data Matrix and Sources

Variable	Formula	Indicator	Data Source		Period
CAR	Capital/Risk-Weighted Assets × 100%	Capital	Audited Statements	Financial	2022, 2023
NPF	Non-Performing Financing/ Total Financing × 100%	Asset Quality	Audited Statements	Financial	2022, 2023
NPM	Net Profit / Operating Income × 100%	Management	Audited Statements/ Annual Report	Financial	2022, 2023
ROA	Net Income/Total Assets × 100%	Earnings	Audited Statements	Financial	2022, 2023
CIR	Operating Expenses/ Operating Income × 100%	Earnings Efficiency	Audited Statements	Financial	2022, 2023
FDR	Financing/Total Deposits × 100%	Liquidity	Audited Statements	Financial	2022, 2023
IT Investment	Annual IT Expenditure	Supporting Indicator	Annual Report		2022, 2023

examining financial resilience following a cybersecurity incident. In addition, the availability of audited financial statements and governance disclosures enables a systematic assessment of the bank's financial condition before and after the incident. While the findings are specific to BSI, they provide insights that may be relevant to other Islamic banking institutions facing similar cybersecurity challenges.

Research Location

This study focuses on Bank Syariah Indonesia (BSI), the largest Islamic bank in Indonesia. The analysis is based on BSI's audited Consolidated Financial Statements and Annual Reports for the fiscal years ended 31 December 2022 and 31 December 2023. These documents were obtained from the official websites of Bank Syariah Indonesia and the Indonesia Stock Exchange and were accessed on May 10, 2025. The analysis uses consolidated financial data reported by the Bank. The CAMEL ratios were calculated from figures presented in the audited financial statements, while supporting information, including information technology investment and corporate governance disclosures, was obtained from the corresponding Annual Reports. Table 1 identifies the financial statement notes and annual report sections used to derive each CAMEL indicator.

Instrumentation or Tools

This study employs the CAMEL framework (Capital, Asset Quality, Management, Earnings, and Liquidity) as its principal analytical framework to assess the financial resilience of Bank Syariah Indonesia. The framework is widely used in banking performance evaluation and is consistent with Bank Indonesia Regulation No. 9/1/PBI/2007. The analysis includes six financial ratios: Capital Adequacy Ratio (CAR), Non-Performing Financing (NPF), Net Profit Margin (NPM), Return on Assets (ROA), Cost-to-Income Ratio (CIR), and Financing-to-Deposit Ratio (FDR). The Management component is proxied by NPM because direct assessment of managerial quality requires supervisory information that is not publicly available in publicly disclosed financial statements. Consistent with previous

CAMEL-based studies on Indonesian banking, NPM is therefore used as an indirect indicator of management effectiveness in generating operating profit from banking activities (Kannapadang, 2023; Ayusningtyas et al., 2024). The interpretation of NPM follows the benchmark criteria provided in Bank Indonesia Circular Letter No. 6/23/DPNP/2004, which have been widely adopted in CAMEL-based banking studies. In this study, these criteria are used as analytical benchmarks rather than as regulatory measures specifically prescribed for Islamic banking.

A limitation of this approach is that annual CAMEL indicators may be influenced by factors beyond the cyberattack, including macroeconomic conditions, financing growth, post-merger adjustments, and broader banking industry trends. In addition, because the cyberattack occurred in May 2023, the 2023 annual report captures approximately seven months of post-incident performance and recovery. Nevertheless, annual CAMEL indicators remain useful for assessing cumulative financial resilience because cyber incidents may affect capital adequacy, asset quality, earnings, and liquidity throughout the fiscal year (Jin et al., 2023; Aderinto & Faforiji, 2025; Martins & Moutinho, 2025; Sulong et al., 2025). Therefore, the findings should be interpreted as an assessment of financial resilience following the incident rather than evidence of a direct causal effect of the cyberattack.

Data Collection Procedures

Data were collected from secondary sources, including the audited financial statements and annual reports of Bank

Syariah Indonesia for 2022 (pre-attack period) and 2023 (post-attack period), obtained from the official websites of Bank Syariah Indonesia and the Indonesia Stock Exchange. Financial data used to calculate the CAMEL ratios were extracted from these reports, while supplementary information regarding cybersecurity governance, crisis mitigation measures, and information technology investment was obtained from the narrative disclosures contained in the annual reports.

Data Analysis

This study employs a comparative analysis of financial indicators between 2022, representing the pre-incident period, and 2023, representing the incident year in which the cyberattack occurred in May. Accordingly, the analysis evaluates financial resilience during the period surrounding the incident rather than a purely post-attack condition. The CAMEL framework is implemented to evaluate financial conditions, as it encapsulates the aggregate impacts of operational disruptions, including cyberattacks, on fundamental financial metrics such as capital adequacy, asset quality, profitability, and liquidity.

Ethical Approval

This research employs readily available secondary data and does not engage human subjects. Consequently, official ethical approval is unnecessary. All data are utilised responsibly and cited accurately to uphold academic integrity.

Results and Discussion

Table 4 presents the financial profile of Bank Syariah Indonesia during the pre-incident period (2022) and the incident year (2023). In 2022, total assets amounted to IDR 305,727,438 million, total equity was IDR 33,500,000 million, total financing reached IDR 67,452,903 million, and information technology investment totalled IDR 266 billion. In 2023, total assets increased to IDR 353,624,124 million, total equity rose to IDR 38,740,000 million, total financing reached IDR 85,588,153 million, and information technology investment increased to IDR 968 billion. Compared with 2022, total assets increased by 15.6%, total equity by 15.6%, total financing by 26.9%, and information technology investment by 263.0%.

The following section presents the results of the financial soundness ratios calculated using the CAMEL method of Bank Syariah Indonesia using the CAMEL method before and after the cyberattack.

Table 5 presents the CAMEL indicators of Bank Syariah Indonesia during the pre-incident period (2022) and the incident year (2023). In 2022, the bank recorded a Capital Adequacy Ratio (CAR) of 20.29%, Non-Performing Financing (NPF) of 2.42%, Net Profit Margin (NPM) of 22.0%, Return on Assets (ROA) of 1.98%, Cost-to-Income Ratio (CIR) of 75.88%, and Financing-to-Deposit Ratio (FDR) of 79.37%.

In the incident year (2023), CAR increased to 21.04%, NPF decreased to 2.08%, NPM rose to 27.80%, ROA increased to 2.35%, CIR declined to 71.27%, and FDR increased to 81.73%.

Based on the adopted CAMEL classification criteria, CAR, ROA, CIR, and FDR remained within the sound category in both reporting periods, while NPF remained moderately sound. Although NPM improved by 5.80 percentage points, it remained below the benchmark for a sound classification and therefore continued to be categorized as Fundamentally Unsound under the adopted assessment framework.

Compared with 2022, CAR increased by 0.75 percentage points, NPF declined by 0.34 percentage points, NPM increased by 5.80 percentage points, ROA rose by 0.37 percentage points, CIR improved by 4.61 percentage points, and FDR increased by 2.36 percentage points. Overall, the

Table 4. The fundamental financial data for Bank Syariah Indonesia

Item	Period	
	2022	2023
Total Asset (in Million Rupiah) *	305,727,438	353,624,124
Total Equity (in Million Rupiah) *	33,500,000	38,740,000
Total Financing (net) (in Million Rupiah) *	67,452,903	85,588,153
Information technology investment (in Million Rupiah) **	266,000	968,000

Source: Secondary Data

CAMEL indicators indicate that BSI's financial soundness did not deteriorate during the incident year, with improvements observed in most indicators relative to the pre-incident fiscal year. To facilitate comparison across indicators, Figure 1 below provides a visual summary of the CAMEL results for 2022 and 2023. While most indicators improved during the incident year, the figure also highlights the comparatively weaker performance of the Management component (NPM), which remained below the benchmark adopted for a sound classification.

The figure illustrates changes in the six CAMEL indicators between 2022 and 2023. Improvements were observed in CAR, NPM, ROA, and FDR, while NPF and CIR declined,

indicating improvements in asset quality and operational efficiency. The figure is intended to complement the tabular presentation in Table 4 and facilitate comparison across indicators.

As shown in Table 6, Bank Syariah Indonesia obtained an identical bank soundness score of 83 in both 2022 and 2023. Based on the Bank Indonesia classification criteria, a score between 81 and 100 indicates a highly sound bank. Therefore, the overall soundness classification remained unchanged during the study period.

Although the aggregate soundness score remained stable, several individual CAMEL indicators showed improvement. CAR, ROA, CIR, and FDR remained within the sound category, while NPF remained in the moderately sound category. NPM improved from 22.00% to 27.80%; however, it continued to be classified as Fundamentally Unsound because it remained below the minimum threshold specified in the adopted CAMEL assessment framework.

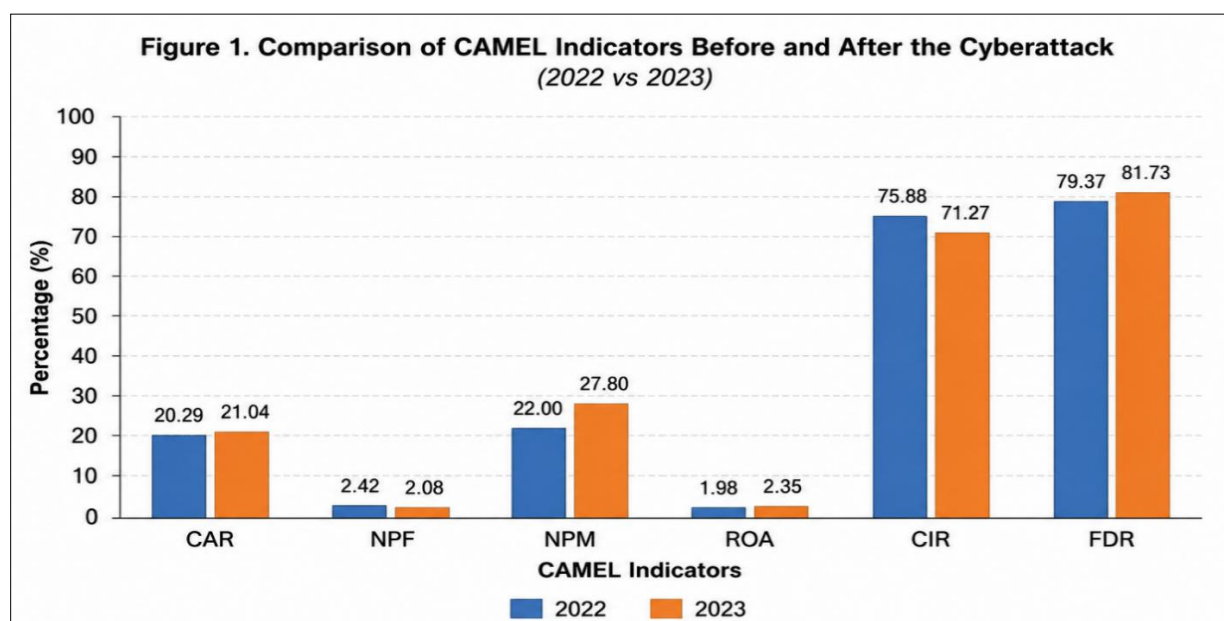
Given that the analysis is based on two annual observations, the findings should be interpreted as a descriptive comparison rather than a formal statistical test of differences. Overall, the results indicate that the bank maintained a highly sound classification during the incident year, while exhibiting improvements in several financial performance indicators.

This section discusses the findings in relation to previous studies on banking performance and cybersecurity incidents. Particular attention is given to the interpretation of financial resilience following the 2023 cyberattack, while also considering alternative explanations for the observed changes in financial indicators, including business growth,

Table 5. CAMEL pre-incident and incident year

Indicator(s)	Measurement(s)	Period			CAMEL*	
		2022	2023	Diff.	2022	2023
Capital	CAR	20.29	21.04	+0.75	Sound	Sound
Asset quality	NPF	2.42	2.08	-0.34	Moderate	Moderate
Management	NPM	22.00	27.80	+5.80	Fundamentally unsound	Fundamentally unsound
Earnings	ROA	1.98	2.35	+0.37	Sound	Sound
	CIR	75.88	71.27	-4.61	Sound	Sound
Liquidity	FDR	79.37	81.73	+2.36	Sound	Sound

*See Table 1, Source: Secondary Data

**Figure 1.** Comparison of CAMEL Indicators Before and After the Cyberattack (2022 vs 2023)

Source: Data analysed.

CAR = Capital Adequacy Ratio, NPF = Non-Performing Financing, NPM= Net Profit Margin,

ROA= Return on Assets, CIR = Cost-to-Income Ratio, FDR = Financing to Deposit Ratio

managerial policies, and broader economic conditions. The section further outlines the study's limitations and directions for future research.

Interpretation of Key Findings

The findings indicate that Bank Syariah Indonesia (BSI) maintained overall financial soundness during the incident year, with improvements observed in several CAMEL indicators, including capital adequacy (CAR), asset quality (NPF), profitability (ROA), and operational efficiency (CIR). The study also documents a substantial increase in information technology (IT) expenditure of approximately 263% during the same period. Although the annual report describes continued investment in digital infrastructure and technology development, the available annual financial data do not allow the observed financial performance or IT expenditure to be attributed directly to the cyber incident or subsequent recovery efforts. Instead, these findings provide descriptive evidence of financial resilience during the fiscal year in which the cyberattack occurred, while acknowledging that broader economic conditions, managerial decisions, and other organizational factors may also have influenced the observed outcomes. From the perspective of cyber-resilience theory Araujo et al. (2024), the observed financial stability is consistent with the characteristics of resilient organizations that are able to absorb and adapt to cyber-related disruptions. However, this interpretation should be regarded as theoretical rather than causal because the present study does not isolate the effects of cybersecurity governance, IT investment, or

other organizational responses. Accordingly, the findings suggest that the CAMEL framework provides a useful descriptive perspective for assessing annual financial resilience following a major cyber incident, although further research using higher-frequency or multi-case data is needed to examine causal relationships.

The findings suggest that, in the case of Bank Syariah Indonesia, the cyber incident was not accompanied by a deterioration in overall financial soundness during the incident year. However, this observation should be interpreted within the specific institutional and economic context of BSI and should not be generalized to other banking institutions. The study also documents a substantial increase in information technology investment during the same period. Although the annual report describes continued investment in digital infrastructure and cybersecurity, the available evidence does not establish whether these investments contributed directly to the observed financial resilience. Instead, the findings indicate that the maintenance of financial soundness coincided with continued technology investment during the incident year. From the perspective of cyber-resilience theory, this pattern is consistent with the proposition that organizational resilience involves technological, financial, and managerial preparedness. Nevertheless, the present study provides descriptive rather than causal evidence, and further research incorporating governance disclosures, incident-response information, or higher-frequency financial data is needed to examine these relationships more directly.

Table 6. Bank soundness score

Period	Measurement(s)	Value (s)	Category (A)	Weight % (B)	Score (A/B)*100
2022	CAR	20.29	Sound	5	(25/30) *100
	NPF	2.42	Moderate	4	
	NPM	22.00	Fundamentally unsound	1	
	ROA	1.98	Sound	5	
	CIR	75.88	Sound	5	
	FDR	79.37	Sound	5	
Total Soundness Score				25	83
2023	CAR	21.04	Sound	5	(25/30) *100
	NPF	2.08	Moderate	4	
	NPM	27.80	Fundamentally unsound	1	
	ROA	2.35	Sound	5	
	CIR	71.27	Sound	5	
	FDR	81.73	Sound	5	
Total Soundness Score				25	83

Source: Secondary Data (analysed)

Table 7. Key Findings from Reviewed Literature

No	Author(s)	Year	Study Focus	Key Findings	Moderating Factors	Geographic Context
1	Masood et al.	2016	CAMELS model & Islamic bank performance	The study found that Islamic banks based on financial ratios, providing a reliable framework for assessing bank soundness and supporting strategic decision-making	Financial structure, governance, market development	Pakistan
2	Mintrom & Thomas	2018	Decision-making theory & ERM	Effective decision-making requires rapid response and integration with risk management systems	Managerial capability	Global
3	Muhammad & Triharyono	2019	Bank performance before-during-after crisis	Islamic banks show variations in financial performance across pre-crisis, crisis, and post-crisis periods, indicating that external shocks influence financial stability but can be managed over time	Crisis intensity, bank resilience, macroeconomic conditions	Indonesia
4	Haapamäki & Sihvonen	2019	Cybersecurity framework	Cybersecurity involves investment, internal control, audit, and	Governance structure, audit effectiveness	Europe

No	Author(s)	Year	Study Focus	Key Findings	Moderating Factors	Geographic Context
				disclosure as integrated components		
5	Antczak	2020	Cybersecurity cost accounting	Cybersecurity expenses are strategic and include prevention and post-attack mitigation costs	Cost allocation strategy, management decisions	Europe
6	Razavi et al.	2023	Cybersecurity as intangible asset	Cybersecurity is a strategic intangible asset, especially in trust-based sectors like banking	Industry type (financial services)	Global
7	Erkan-Barlow et al.	2023	Cyberattacks & bank performance	Cyberattacks negatively impact bank profitability, deposits, and lending	Bank size, ownership structure	USA
8	Jooda et al.	2023	Cyber resilience and threat mitigation in financial institutions	CAMEL indicators reflect financial stability of banks	Regulatory environment	Global
9	Jin et al.	2023	Cyber risk & bank behaviour	Cyberattacks increase loan loss provisions and reduce earnings management	Internal control strength	Global
10	Abdilah & Fitriyah	2024	Bank health (CAMEL & RGEK)	CAMEL effectively measures financial health and reflects fluctuations in performance	ROA, efficiency ratios	Indonesia
11	Alsakini et al.	2024	Cybersecurity & financial reporting	Cybersecurity breaches significantly affect financial reporting quality across financial statements	Type of cyberattack, response speed	Jordan
12	Araujo et al.	2024	Cyber-resilience theory	Organizations that can anticipate, absorb, recover, and adapt to cyber threats are able to maintain operational continuity and financial stability	IT capability, governance, adaptive capacity	Global
13	Al Hammadi et al.	2024	Fintech adoption and risk management in Islamic banking	Fintech adoption and IT capabilities improve risk management effectiveness, while digital transformation alone has no significant impact.	Regulatory environment and IT security	United Arab Emirates (UAE)
14	Aderinto & Faforiji	2025	Cybersecurity & profitability	Cyberattacks reduce EPS and overall profitability	Financial resilience capacity	Global
15	Sulong et al.	2025	Cyber risk & risk-taking	Cyber risk increases bank risk-taking behaviour and affects financial strategy	Competition, IT investment, deposit volatility	Global
16	Martins & Moutinho	2025	Cyberattacks & market impact	Short-term cyber incidents can influence firm valuation, stakeholder expectations, and managerial decisions, with effects reflected in annual financial performance	Market sensitivity, response strategy	Global
17	Mollik & Majeed	2025	Cybersecurity challenges in digital Islamic banking	Islamic banks face cyber threats such as fraud, ransomware, and data breaches, requiring stronger cybersecurity governance and Shariah-based risk management.	Regulatory support and cybersecurity frameworks	Bangladesh
18	Putri	2025	Cybersecurity, digital regulation, and Shariah compliance in Islamic digital economy	Cybersecurity and Shariah compliance must be integrated to maintain public trust and digital financial integrity.	Digital regulation and Shariah governance	Indonesia

No	Author(s)	Year	Study Focus	Key Findings	Moderating Factors	Geographic Context
19	Alifah et al.	2025	Cybersecurity and operational risk in Islamic banking	Cyber risks may lead to operational failures and Shariah non-compliance, affecting customer trust and financial stability.	Governance systems and cybersecurity frameworks	Indonesia
20	Ridzwan et al.	2026	Role of Islamic finance in economic resilience	Islamic finance promotes economic stability through risk-sharing, ethical finance, zakat, waqf, sukuk, and FinTech integration during economic crises.	Regulatory support, institutional development, and financial technology	Malaysia
21	Wati et al.	2026	Cyberattack risk mitigation in Islamic banks during digital transformation	The rapid digital transformation of Islamic banks increases exposure to phishing, ransomware, DDoS, and data breaches, requiring integrated cybersecurity mitigation aligned with ethical of sharia principles.	Cybersecurity governance, digital literacy, and AI-based security systems	Indonesia
22	Nipa et al.	2026	Islamic FinTech for disaster risk financing and economic resilience	Islamic FinTech improves financial inclusion, transparency, and disaster recovery through blockchain, mobile platforms, and Islamic social finance instruments.	Regulatory barriers, digital literacy, and technological infrastructure	Southeast Asia, Middle East, and Africa
23	Fuszder et al.	2026	Cybersecurity risk and bank competition	Cybersecurity risk significantly influences bank competition, affecting banking stability, operational performance, and competitive behaviour within financial institutions.	Cybersecurity exposure and banking market structure	United States
24	Rohim et al.	2026	Role of Islamic fintech in reducing economic vulnerability	Islamic fintech improves financial inclusion, expands halal financing access, and strengthens household economic resilience among vulnerable Muslim communities through digital financial services.	Digital literacy, effective regulation, and institutional collaboration	Indonesia

Comparison with Previous Studies

The findings are broadly consistent with, and extend, previous research. While [Masood et al. \(2016\)](#) did not examine cybersecurity incidents, their study demonstrated that the CAMELS framework is a reliable tool for evaluating Islamic bank performance. This supports the methodological use of CAMELS in the present study, although the findings regarding financial resilience following a cyberattack are specific to the BSI case. This study also confirms the findings of [Haapamäki & Sihvonen \(2019\)](#) and [Antczak \(2020\)](#) that cybersecurity must be seen as a fundamental element of governance and corporate strategy. The substantial increase in IT investment at BSI coincided with the maintenance of annual financial soundness during the incident year, providing a relevant contextual observation for interpreting the bank's financial resilience without implying a causal effect of cybersecurity spending. These findings are further supported by [Al Hammadi et al. \(2024\)](#), who found that fintech adoption and technological capabilities positively improve risk management effectiveness in Islamic banks, emphasizing the importance of cybersecurity readiness and IT capability in maintaining institutional resilience. Similarly, [Putri \(2025\)](#) argued that cybersecurity should be integrated with Shariah governance because digital security is not only a technical issue but also part of Islamic ethical responsibility and trust preservation. [Wati et al. \(2026\)](#) also emphasized that cyber risk mitigation in Islamic banks requires integrated strategies that uphold Islamic ethical values, including maintaining trust, protecting customer assets, and ensuring public benefit and financial security. In addition, [Alifah et al. \(2025\)](#) explained that cyberattacks and operational risks in Islamic banking may disrupt Shariah compliance and customer trust, highlighting the importance of adaptive governance and integrated cybersecurity frameworks in

maintaining institutional stability. Furthermore, [Jooda et al. \(2023\)](#) emphasized that financial institutions increasingly face sophisticated cyber threats such as ransomware, social engineering, and advanced persistent attacks, making cyber resilience and strategic risk management essential for long-term operational sustainability.

Moreover, [Muhammad & Triharyono \(2019\)](#) showed that Islamic banks experience fluctuations in performance across pre-, during-, and post-crisis periods, suggesting that financial shocks—such as cyberattacks—can be absorbed and managed over time depending on institutional resilience. This argument is consistent with [Mollik & Majeed \(2025\)](#), who highlighted that digital Islamic banking increasingly faces threats such as phishing, ransomware, and data breaches, thereby requiring stronger cybersecurity governance and institutional preparedness. In line with this, [Ridzwan et al. \(2026\)](#) explained that Islamic finance institutions with stronger governance structures, ethical financial practices, and technological adaptation tend to demonstrate greater economic resilience during periods of uncertainty and crisis. [Ramadhanty et al. \(2022\)](#) similarly found that Islamic finance in Indonesia remained resilient during the COVID-19 pandemic due to its flexible structure, diverse Islamic contract models, and government support, while adaptability and technological readiness strengthened long-term sustainability. Furthermore, [Nipa et al., \(2026\)](#) found that technology integration, including blockchain and digital financial systems, enhances transparency, operational efficiency, and institutional resilience, supporting the argument that strategic technological investment may strengthen organizational recovery capacity after operational disruptions. [Fuszder et al. \(2026\)](#) also emphasized that cybersecurity risk significantly influences banking competition, operational stability, and institutional performance, indicating that cybersecurity capability has

become a strategic determinant of long-term competitiveness in the banking sector.

Nonetheless, the findings differ from those reported by Erkan-Barlow et al. (2023) and Aderinto & Faforiji (2025), who found that cyberattacks were associated with declines in profitability, liquidity, and overall financial performance. Several factors may explain this difference. First, the previous studies examined different banking environments and institutional contexts, whereas the present study focuses on a single Islamic bank in Indonesia. Second, those studies primarily assessed the direct financial consequences of cyber incidents using broader banking samples, while this study evaluates financial resilience through the CAMEL framework during the incident year. Third, BSI experienced continued growth in assets, financing, and equity during the study period, which may have mitigated the financial impact of the cyberattack. Therefore, the contrasting findings should be interpreted in light of differences in context, methodology, and measurement rather than as contradictory evidence. The observed IT investment and financial improvements coincided with the incident year but cannot be directly attributed to the cyberattack. These differences may be attributable to several factors, such as institutional preparedness, response speed, governance effectiveness, and investment capability. Moreover, whereas Alsakini et al. (2024) underscored the detrimental influence of cybersecurity breaches on the quality of financial reporting, the findings may suggest that effective mitigation measures could help reduce these consequences mitigation techniques might alleviate these negative consequences. This perspective is also strengthened by Wati et al. (2026), who argued that layered cybersecurity systems, AI-based anomaly detection, and digital governance can significantly reduce operational risks and maintain public trust in Islamic banking institutions.

The findings validate recent studies Jin et al. (2023); Sulong et al. (2025), indicating that cyber risk affects management decision-making and risk-taking behaviour. This study demonstrates that heightened IT investment and enhanced efficiency suggest that the cyberattack elicited adaptive reactions, which were later shown in annual financial performance as measured by the CAMEL framework. These findings also align with Putri (2025) and Rohim et al. (2026), who emphasized that digital transformation and Islamic fintech development require adaptive governance, effective regulation, digital literacy, and strong cybersecurity systems to maintain institutional sustainability, financial inclusion, and customer trust in the digital Islamic financial ecosystem.

Limitations and Cautions

This study, while providing valuable insights, has several limitations. First, the use of a single case study limits the transferability of the findings to other banking institutions or geographical contexts, as banks may differ in their governance structures, financial capacity, risk management practices, and exposure to cybersecurity threats. Second, the analysis relies on annual financial data and CAMEL indicators, which provide a cumulative assessment of financial performance but may not capture short-term operational disruptions, customer reactions, or immediate market responses following a cyberattack. In addition, annual CAMEL ratios cannot fully isolate the effects of the cyberattack from other factors, such as business growth, macroeconomic conditions, industry trends, or management policies during the same period. Third, this study relies primarily on secondary data and does not include direct measures of cyberattack-related losses, customer trust, service disruption duration, deposit withdrawal behaviour, or internal decision-making processes. Consequently, the findings should be interpreted as an assessment of financial resilience during

the incident year rather than a comprehensive evaluation of all organizational consequences of the cyberattack.

Recommendations for Future Research

Future research should extend this analysis by comparing multiple Islamic and conventional banks to improve the generalizability of the findings. The use of high-frequency financial data, such as monthly or quarterly indicators, would enable a more precise assessment of financial performance during and immediately after cyber incidents. In addition, future studies should examine customer trust, deposit behaviour, and cyber-related costs to provide a more comprehensive understanding of the financial and behavioural consequences of cyberattacks. Combining these measures with governance disclosures or qualitative evidence, such as management interviews, could further clarify the organizational responses associated with financial resilience following cyber incidents.

Conclusion

This study assessed the financial resilience of BSI during the 2023 cyberattack incident year using the CAMEL framework. The findings show that BSI maintained a highly sound classification, with improvements observed in several financial indicators, including capital adequacy, asset quality, profitability, and operational efficiency. However, the overall bank soundness score remained unchanged, and the Management component (NPM) continued to be classified as Fundamentally Unsound under the adopted CAMEL criteria.

As a single-case study based on annual financial data, the findings should be interpreted as a descriptive assessment of financial resilience rather than evidence of the direct impact of the cyberattack. The results suggest that the BSI case was accompanied by stable financial performance during the incident year, although other factors such as business growth, management policies, and broader economic conditions may also have influenced the observed outcomes.

Practically, the findings highlight the importance of maintaining strong capital, liquidity, governance, and technology capabilities to support organizational resilience in the face of cybersecurity disruptions. For Islamic banks and regulators, strengthening cybersecurity governance and continuous monitoring of operational and financial resilience remain essential. Future research should examine multiple banking institutions and use higher-frequency data to better understand the relationship between cybersecurity incidents and financial performance.

Author contributions

All authors have contributed significantly to this research and manuscript preparation. Aminah Aminah acted as the research coordinator, formulated the research problem, and developed the literature review. Tri Damayanti was responsible for data analysis and contributed to drafting the manuscript, particularly the discussion and conclusion sections. Henny Murtini and Yenni Priatna Sari contributed to data collection and the development of the research methodology. All authors reviewed and approved the final version of the manuscript.

Acknowledgements

The authors would like to express their gratitude to all parties who indirectly supported this research. Special thanks to institutions providing access to financial reports and data sources, particularly through official platforms such as the Indonesia Stock Exchange and BSI. Appreciation is also given to colleagues and peers who provided valuable insights and feedback during the research process.

References

- Abdilah, M., & Fitriyah. (2024). Health of Islamic Commercial Banks in Indonesia: Camel and Rgec Methods. *Proceeding International Conference of Islamic Economics & Business (ICONES)*, 391–404.
- Aderinto, A. A., & Fafarji, A. C. (2025). Cybersecurity Threats and Financial Performance of Listed Commercial Banks in Nigeria. *Asian Journal of Advanced Research and Reports*, 19(4), 381–394. <https://doi.org/10.9734/ajarr/2025/v19i4990>
- Al Hammadi, M., Jimber-Del Rio, J. A., Ochoa-Rico, M. S., Montero, O. A., & Vergara-Romero, A. (2024). Risk Management in Islamic Banking: The Impact of Financial Technologies through Empirical Insights from the UAE. *Risks*, 12(2), 1–15. <https://doi.org/10.3390/risks12020017>
- Alifah, R. N., Subagiyo, R., & Aswad, M. (2025). Cybersecurity and Operational Risk in Islamic Banking: Enhancing Governance and Shariah Compliance in The Digital Age. *Proceedings of The Iqtishaduna International Conference 2025*, 209–212.
- Alsakini, S. A. K., Alawawdeh, H. A., & Alsayed, S. (2024). The Impact of Cybersecurity on the Quality of Financial Statements. *Applied Mathematics and Information Sciences*, 18(1), 169–181. <https://doi.org/10.18576/amis/180117>
- Anand, K., Duley, C., & Gai, P. (2026). Cybersecurity and Financial Stability. *Review of Finance*, 30(3), 1109–1150. <https://doi.org/10.1093/rof/rfaf079>
- Antczak, J. (2020). Cybersecurity Costs in an Enterprise Unit. *Edukacja Ekonomistów i Menedżerów*, 55(1), 82–94. <https://doi.org/10.33119/eeim.2020.55.6>
- Araujo, M. S. de, Machado, B. A. S., & Passos, F. U. (2024). Resilience in the Context of Cyber Security: A Review of the Fundamental Concepts and Relevance. *Applied Sciences (Switzerland)*, 14(5). <https://doi.org/10.3390/app14052116>
- Ayusningtyas, A. F., Yendra, Y., & Marihi, L. O. (2024). Analysis of Bank Health Levels Using the Camel Method at BUMN Commercial Banks Listed. *Advances in Management & Financial Reporting*, 2(3), 135–148. <https://doi.org/10.60079/amfr.v2i3.256>
- Bank Syariah Indonesia. (2023). *Laporan Publikasi Keuangan Triwulan III*. <https://ir.bankbsi.co.id/misc/Laporan-Keuangan/Tahun-Laporan-2023/Laporan-Publikasi-Triwulan-Sep-ID.pdf>
- Erkan-Barlow, A., Ngo, T., Goel, R., & Streeter, D. (2023). An In-Depth Analysis of The Impact of Cyberattacks on The Profitability of Commercial Banks in The United States. *Journal of Global Business Insights*, 8(2), 120–135. <https://doi.org/10.5038/2640-6489.8.2.1246>
- Fatikhathun Nisa, Z., & Tri Cahyono, Y. (2024). The Effect of Cyber Attacks on Stock Performance Bank Syariah Indonesia. *Proceeding International Conference on Accounting and Finance*, 2, 359–368.
- Fuszder, Md. H. R., Abdullah, M., Sulong, Z., & Abakah, E. J. A. (2026). Cybersecurity Risk and Bank Competition. *Journal of International Financial Markets, Institutions and Money*, 109. <https://doi.org/10.1016/j.intfin.2026.102313>
- Gulyas, O., & Kiss, G. (2023). Impact of cyber-Attacks on The Financial Institutions. *Procedia Computer Science*, 219, 84–90. <https://doi.org/10.1016/j.procs.2023.01.267>
- Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in Accounting Research. *Managerial Auditing Journal*, 34(7), 808–834. <https://doi.org/10.1108/MAJ-09-2018-2004>
- Jin, J., Li, N., Liu, S., & Khalid Nainar, S. M. (2023). Cyber Attacks, Discretionary Loan Loss Provisions, and Banks' Earnings Management. *Finance Research Letters*, 54(February). <https://doi.org/10.1016/j.frl.2023.103705>
- Jooda, T. O., Samson, A. T. O., & Adeyemi Adewunmi. (2023). Strengthening Cyber Resilience in Financial Institutions: A Strategic Approach to Threat Mitigation and Risk Management. *World Journal of Advanced Research and Reviews*, 20(3), 2217–2247. <https://doi.org/10.30574/wjarr.2023.20.3.2460>
- Kannapadang, D. (2023). Analysis of the Camel Method for Assessing the Financial Health Condition of PT. Bank Negara Indonesia (Persero) Tbk, During the Covid-19 Pandemic. *Jurnal Ekonomi*, 12(03), 2023. <http://ejournal.seaninstitute.or.id/index.php/Ekonomi>
- Martins, A. M., & Moutinho, N. (2025). Stock-Term Market Impact of Major Cyber-Attacks: Evidence for The Ten Most Exposed Insurance Firms to Cyber Risk. *Finance Research Letters*, 71(January), 1–8. <https://doi.org/10.1016/j.frl.2024.106361>
- Masood, O., Ghauri, S. M. K., & Aktan, B. (2016). Predicting Islamic Banks Performance through CAMELS Rating Model. *Banks and Bank Systems*, 11(3), 37–43. [https://doi.org/10.21511/bbs.11\(3\).2016.04](https://doi.org/10.21511/bbs.11(3).2016.04)
- Mintrom, M., & Thomas, M. (2018). Policy Entrepreneurs and Collaborative Action: Pursuit of The Sustainable Development Goals. *International Journal of Entrepreneurial Venturing*, 10(2), 153–171. <https://doi.org/10.1504/IJUEV.2018.092710>
- Mollik, E., & Majeed, F. (2025). Cybersecurity Challenges in Digital Islamic Banking Established in Bangladesh: Risk Management Perspective. *European Journal of Economic and Financial Research*, 8(8), 51–80. <https://doi.org/10.46827/ejefr.v8i8.1912>
- Muhammad, R., & Triharyono, C. (2019). Analysis of Islamic Banking Financial Performance Before, During and After Global Financial Crisis. *Jurnal Ekonomi & Keuangan Islam*, 5(2), 80–86. <https://doi.org/10.20885/jeki.vol5.iss2.art5>
- Nipa, N. N., Zahid, Z., & Amin, R. (2026). Harnessing Islamic FinTech for Disaster Risk Financing: Innovative Strategies for Economic Resilience and Sustainable Development. *Journal of Islamic Economics Lariba*, 12(1), 259–284.
- OJK. (2023). *Operasional Bank Syariah Indonesia Kembali Normal Masyarakat Diminta Tenang*. Otoritas Jasa Keuangan. <https://ojk.go.id/id/berita-dan-kegiatan/siaran-pers/Pages/Operasional-Bank-Syariah-Indonesia-Kembali-Normal-Masyarakat-Diminta-Tenang.aspx>
- Putri, C. K. (2025). Cybersecurity, Digital Regulation, and Shariah Compliance Challenges in Islamic Digital Economy. *Annual International Conference on Islamic Economics and Business*, 278–284.
- Ramadhanty, S. A., Wijaya, L. I., & Mahadwartha, P. A. (2022). How Islamic Finance is Resilient During the Pandemic. *Journal of Business and Banking*, 12(1), 1. <https://doi.org/10.14414/jbb.v12i1.2934>
- Ramli, A. M., Suseno, S., Mayana, R. F., Rajamanickam, R., & Rohmana, R. D. (2026). The Urgency of Regulating Artificial Intelligence in Relation to Cybersecurity and Cyber Resilience. *Cogent Social Sciences*, 12(1). <https://doi.org/10.1080/23311886.2026.2632977>
- Razavi, H., Jamali, M. R., Emsaki, M., Ahmadi, A., & Hajiaghehi-Keshteli, M. (2023). Quantifying the Financial Impact of Cyber Security Attacks on Banks: A Big Data Analytics Approach. *IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, 533–538. <https://doi.org/10.1109/CCECE58730.2023.10288963>
- Reuters. (2023). *Indonesia's Biggest Islamic Bank Says Customer Data Safe Amid Reports of Breach*. Reuters. <https://www.reuters.com/business/finance/indonesias-biggest-islamic-bank-says-customer-data-safe-amid-reports-breach-2023-05-16/>
- Ridzwan, Elyn Mohd; Nor Aman, N. H., & Muhammad, S. (2026). Understanding The Role of Islamic Finance in Economic Resilience. *International Journal of Research and Innovation in Social Science (IJRISS)*, 10(19), 41–57. <https://doi.org/10.47772/IJRISS>
- Rohim, Muhtarom, Ilyas, I., & Moyo, K. (2026). The Role of Islamic Financial Technology in Reducing Economic Vulnerability in Indonesian Muslim Communities. *Al-Waarits*, 3(1), 82–93.
- Sulong, Z., Fuszder, Md. H. R., Abdullah, M., & Abakah, E. J. A. (2025). Cybersecurity Risk and Bank Risk-Taking. *Journal of Behavioral and Experimental Finance*, 47, 1–8. <https://doi.org/10.1016/j.jbef.2025.101080>
- Timur, Y. P., Ridlwan, A. A., Fikriyah, K., Susilowati, F. D., Canggih, C., & Nurafini, F. (2024). How should Bank Syariah Indonesia Respond to Cyber-attacks? Churn, Sentiments, and Emotions Analysis with Machine Learning. *Journal of Islamic Economics Lariba*, 10(1), 439–470. <https://doi.org/10.20885/jielariba.vol10.iss1.art24>
- Wati, H., Aswad, M., Subagiyo, R., & Asiyah, B. N. (2026). Cyber Attack Risk Mitigation in the Digital Transformation of Islamic Banks in Indonesia. *International Conference on Islam, Law, and Society (INCOILS) Conference Proceedings 2025*, 1(1), 20–33. <https://incoils.or.id/index.php/INCOILS/article/view/335>