LAA MAISYIR
Jurnal Ekonomi Islam
p-ISSN: 2476-9371 e-ISSN: 2580-9512

http://journal.uin-alauddin.ac.id/index.php/lamaisyir
Publisher: Fakultas Ekonomi dan Bisnis Islam UIN Alauddin Makassar

The Impact of Cyber Attack to the Performance of Indonesia's Sharia Bank Stocks in 2023

Hamdan Ardiansyah[1], Arie Noviana[2], Aip Zaenal Mutaqin[3]
Universitas Pendidikan Indonesia[1], IAI Persis Bandung[2], STAI Persis Garut[3]
e-mail: hamdanardiansyah@upi.edu[1], arienoviana@iaipibandung[2], aipzm@staipersisgarut.ac.id[3]

Received: 14 October 2024; Revised: 20 Desember 2024; Published: 24 Desember 2024

Abstrak

Serangan siber pada sektor keuangan, termasuk Bank Syariah, menjadi ancaman serius yang dapat memengaruhi stabilitas dan kinerja pasar. Termasuk Bank Syariah Indonesia, sebagai bank syariah terbesar di Indonesia risiko tersebut yang akan berdampak terhadap kinerja saham. Penelitian ini bertujuan untuk menganalisis dampak serangan siber terhadap kinerja saham Bank Syariah Indonesia, sebelum dan sesudah insiden serangan siber**.** Metode yang digunakan adalah analisis kuantitatif dengan uji komparatif. Data yang digunakan merupakan data sekunder yang diperoleh dari IDX/Bursa Efek Indonesia dan Yahoo Finance. Sampel diambil dari data return saham BSI dengan kode saham BRIS pada tahun 2023 sebelum dan setelah terjadinya serangan siber. Pengujian data menggunakan uji normalitas dan uji beda dengan menggunakan uji *Wilcoxon*. Hasil penelitian menunjukan bahwa nilai signifikansi diatas 0,05 yakni 0,852 menunjukkan bahwa return saham sebelum dan sesudah terjadinya serangan siber tidak mengalami perbedaan yang signifikan. Hal tersebut menandakan bahwa return saham BSI stabil meski terjadi serangan siber, dimana pasar cenderung fokus pada kinerja fundamental dan prospek panjang saham BSI. Sehingga terjadinya serangan siber tidak mempengaruhi return saham yang merupakan bagian dari kinerja saham.

Kata kunci: Serangan Siber, Kinerja Saham, Bank Syariah Indonesia

Abstract

Cyberattacks on the financial sector, including Islamic banks, are a serious threat that can affect market stability and performance. Including Bank Syariah Indonesia (BSI), the largest Islamic bank in Indonesia, this risk will impact stock performance. This study aims to analyze the impact of cyberattacks on the stock performance of Bank Syariah Indonesia before and after cyberattack incidents. The method used is quantitative analysis with comparative tests. The data used is secondary data obtained from IDX/Indonesia Stock Exchange and Yahoo Finance. The stock performance sample taken is BSI's stock return data with the BRIS stock code in 2023 before and after the cyberattack. The data testing technique in this study uses a normality test and a difference test using the Wilcoxon test. The significance value above 0.05, which is 0.852, shows that stock returns before and after the cyberattack did not experience significant differences. This indicates that BSI stock returns are stable despite the cyberattack, where the market tends to focus on the fundamental performance and long-term prospects of BSI shares so that the occurrence of cyberattacks does not affect stock returns, which are part of stock performance.

Keywords: *Cyberattack, Stock Performance, Bank Syariah Indonesia*

INTRODUCTION

Cyber attacks have become increasingly common and complex in the modern technological era. Financial institutions, including Islamic banks, are not immune to this risk. Bank Syariah Indonesia (BSI), one of the largest Islamic banks in Indonesia, experienced a significant cyber attack in mid-2023 (Faizal dkk., 2023). This is its technological infrastructure, image, and customer trust. In line with research findings that explain that customer trust is seriously affected by incidents, indicating concerns about the security of banking services (Maulana & Fitriana, 2023). Not only that, the existence of this cyber case, seen from the perspective of Perception of Security and Trust, simultaneously impacts Customer Loyalty at Bank Syariah Indonesia (Zamzami Akromi Lubis & Fauzi Arif Lubis, 2024).

The movement of BRIS shares owned by Bank Syariah Indonesia experienced fluctuations during the last 10 days on May 8, 2023, which was finally closed due to the panic effect of investors after the news of the cyber attack. Meanwhile, the movement of BSI's financial performance has a fairly strong financial basis, as seen from the KPMM, ROA, ROE, and BOPO ratios, which are good because they are above the standard ratio. However, the FDR ratio has decreased in value, meaning the bank highly depends on time deposits (Solikhawati & Samsuri, 2023).

Information technology has become an integral part of the banking industry operations in the increasingly developing digital era. This digital transformation provides convenience in service and presents new challenges, one of which is the threat of cyber attacks. Cyber attacks in the financial sector, including banking, can potentially disrupt operations, damage reputation, and reduce customer trust.

The impact of these attacks can extend to the stock market, where stock price fluctuations are often influenced by investor perceptions of the Company's risk and stability (Restika & Sonita, 2023). Security risks such as phishing, malware, and service disruptions can harm customers and threaten trust in banking institutions. BSI's customer protection analysis involves understanding security policies, responses to cyber attacks, and customer data protection policies (Putri dkk., 2023).

Economic indicators of a nation can be viewed from the development of the banking sector. As is known, Bank Syariah Indonesia (BSI) is one of the Islamic banks with the largest assets because it results from a merger of 3 Islamic banks, namely BRI Syariah, BNI Syariah, and Bank Syariah Mandiri.

Not only seen from the asset side, other things need to be considered, namely from the technology side. However, banking operations that depend on technology make them vulnerable to cyber-attacks (Irawan dkk., 2021). Cyberattacks can manifest in many forms, from ransomware that encrypts data to disrupting banking service systems. For example, a ransomware attack 2023 infected 1.5 terabytes of BSI data, including sensitive information such as account numbers, transaction history, and customer emails (Wijanarko dkk., 2023). This disruption not only causes inconvenience to customers but also can potentially drain additional costs for recovery and compensation.

Bank Syariah Indonesia (BSI), one of Indonesia's largest Islamic financial institutions, is not immune to this threat. Although the sharia principles upheld by BSI provide differentiation compared to conventional banks, the threat to cybersecurity remains a critical issue that must be faced (Fitriani dkk., 2023). A successful cyberattack can damage the bank's image, cause customer data leaks, and disrupt operations. This negative impact is felt by customers and investors, which can ultimately affect the performance of the bank's shares in the capital market (Afifah, 2023).

This study aims to analyze the impact of cyber attacks on the stock performance of Bank Syariah Indonesia. Through a case study of stock price comparison before and after the cyber attack incident, it is hoped that this study can provide a deeper understanding of the relationship between cyber security and stock price fluctuations. In addition, this study is also expected to provide insight for banking industry players and investors regarding the importance of strengthening cyber security systems to minimize financial risks that may arise due to cyber attacks in the future (Dermawan dkk., 2023).

This study will also examine investor sensitivity to cyber attack incidents in the banking industry, especially in Islamic banking. Ultimately, these findings are expected to be the basis for Islamic banks' consideration in improving their cyber security systems and maintaining public trust and the stability of their stock performance (Wijayani, 2017).

By conducting this analysis, we can understand how serious the potential risk of cyber attacks is for financial institutions and how investors react to such incidents. The results of this study can be used as an important reference for bank management, financial regulators, and investors themselves in anticipating and responding to the risk of cyber-attacks. Next, we will explain the detailed methods and research results to help understand the complexity of the interaction between cyber attacks and the stock performance of Bank

Syariah Indonesia. Thus, we can provide a more complete picture of the impact of cyber attacks on national economic stability and investor confidence in the Indonesian Islamic banking industry.

RESEARCH METHOD

This research approach is a quantitative study using a case study technique before and after the cyber attack on BSI. The method used in this study is comparative, which compares stock performance through stock returns from before and after the cyber attack. The variables in the data analysis of this study are BSI stock returns. Data collection in this study uses documentation techniques. This study uses secondary BSI stock movement data from the IDX and Yahoo Finance databases (Martono, 2010). Researchers process and analyze data using the stages of normality testing and comparative testing using the IBM SPSS 25 application (Pramesti, 2018). The research period is 72 days, 36 days before and after the cyberattack. Researchers analyze whether cyberattack crime attacks affect BSI stock performance through stock returns.

So, the framework of this research is depicted as follows:

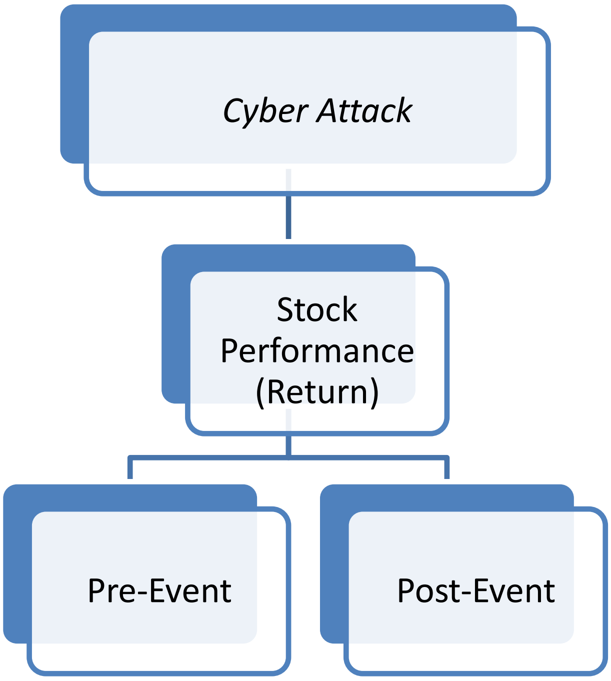

Figure 1. Research Framework

A hypothesis test is carried out using the Wilcoxon test to test whether there is a significant difference in stock price performance before and after the event.

RESULT AND DISCUSSION

Table 1. Descriptive Statistics

Variable	Mean	Std. Dev	Min	Max
Before	0.0031	0.2328	0.00	0.05
After	0.0006	0.02917	0.00	0.06

Source: Processed data

The BRIS stock return variable before the cyberattack event was 0.00 to 0.05, with a standard deviation before the cyberattack event of 0.2328 and a mean of 0.0031. Meanwhile, the BRIS stock return variable after the cyberattack event was in the range of 0.00 to 0.0, with a standard deviation before the cyberattack event of 0.02917 and a mean of 0.0009.

Table 2. Test of Normality

Tests of Normality

Return		Kolmogorov-Smirnov[a]			Shapiro-Wilk		
		Statistic	df	Sig.	Statistic	df	Sig.
Result	Before	,157	36	,025	,938	36	,043
	After	,206	36	,000	,825	36	,000

a. Lilliefors Significance Correction

This study conducted a normality test using the One-Sample Kolmogorov-Smirnov Test and Shapiro-Wilk. Then, for the results of the One-Sample Kolmogorov-Smirnov Test, the data distribution for the before and after conditions was not normally distributed. The statistical value of the Kolmogorov-Smirnov test shows that the largest absolute difference between the observed data distribution and the theoretical distribution is 0.157 before and 0.206 after. The significance test results produce a p-value of 0.025 for before and 0.000 for after, both of which are less than 0.05. The results of the Shapiro-Wilk test are also the same; the data distribution for the before and after conditions is not normally distributed. The statistical value of the Kolmogorov-Smirnov Shapiro Wilk test shows that the largest absolute difference between the observed data distribution and the theoretical distribution is 0.938 for before and 0.825 for after. The significance test results produced a p-value of 0.043 for before and 0.000 for after, both of which were smaller than 0.05. Because the normality test results stated that the data studied were not normally distributed, the data included nonparametric data. So, for further comparative testing using the Wilcoxon test.

Table 3. Wilcoxon Test

Test Statistics[a]

	Sesudah - Sebelum
Z	-.186[b]
Asymp. Sig. (2-tailed)	,852

a. Wilcoxon Signed Ranks Test

b. Based on positive ranks.

Based on the Wilcoxon test results shown in the table, it can be concluded that the average difference between the before and after conditions has a significance value (Sig. 2-tailed) of 0.852, which is much greater than the threshold of 0.05. There is no statistically significant difference between the before and after conditions. These results indicate that the changes are most likely due to chance factors or natural variation, and there is no strong evidence to show a real effect of cyberattacks. Bank Syariah Indonesia is a bank that was merged with BRI Syariah Bank, Bank Mandiri Syariah, and BNI Syariah, which was inaugurated on February 1, 2021. On May 8, 2023, all customers could not use BSI services. These services include direct services at branch offices, ATMs, and mobile service applications. The cyber attack that caused a decline in the share price of BRIS, owned by Bank Syariah Indonesia, is detrimental and worrying. Cybersecurity is a crucial issue in the banking world, and these attacks can affect investor confidence and the company's image (Bravely, 2023).

According to (Jin dkk., 2023), when a company experiences a cyber attack, management needs to be vigilant to improve internal control, reduce operational risk, and maintain reputation. Therefore, banks are likely to do less earnings management and enhance the quality of accounting information, depending on the cyber attack. However, when a bank becomes a victim of a cyber attack, the bank may lose customers or experience disruption to business operations. Banks have the potential to do more revenue management to mitigate the potential negative impact of cyber attacks on their revenues (Hogan dkk., 2023).

Based on the results of the Paired Samples Test shown in the figure, it can be concluded that the average difference between the before and after conditions is 0.00250 with a standard deviation of 0.03581. The 95% confidence interval of the difference ranges from -0.00962 to 0.01462, which includes the value of zero. The resulting t value is 0.419 with a degree of freedom (df) of 35.

The significance value (Sig. 2-tailed) is 0.678, much greater than the threshold of 0.05. Thus, there is no statistically significant difference between the before and after conditions. These results indicate that the changes are most likely due to chance factors or natural variation, and there is no strong evidence to show a real effect of cyberattacks.

A successful cyberattack can have a significant financial impact on a company. The costs of handling attacks, system recovery, security audits, and compensation that may have to be paid to affected customers can be a heavy burden for the company (Solikhawati & Samsuri, 2023). This could negatively impact the company's financial performance, and investors are concerned about a potential decline in revenue and profits.

Therefore, it is important for companies to have strong and responsive cybersecurity measures in place and the ability to respond to cyber-attacks quickly and effectively (Radiansyah dkk., 2016). This means that cybercrime attacks have detrimental implications for the general public. Inaccurate information will impact capital market conditions, especially BSI stock performance (Nisa & Cahyono, 2024). Transparency and good communication with investors and stakeholders are also important to build trust and minimize the negative impacts that may arise from cyber attacks.

We can see no significant price change at the beginning of the cessation of business services for consumers. However, if the service remains cessation and is exacerbated by news of cyber attacks and corporate data leaks (Bravely, 2023). An investor must conduct economic analysis to determine economic decisions because economic analysis tends to have a strong relationship between what happens in the macroeconomic environment and capital market performance (Cahyanti dkk., 2024).

We even see the performance of Islamic banks, which is quite good, indicating a strong financial foundation and the ability to overcome the problem. This shows that BSI has a good risk management system that has successfully isolated the impact of cyber attacks (Tristanto dkk., 2023)

Table 4. Profit and Loss Statement and Financial Ratios

Year	Income	EBITDA	Net Profit	NPM	EPS
2019	2.683.027.000.000	569.480.000.000	74.016.000.000	2,76 %	7
2020	3.564.727.000.000	887.632.000.000	248.054.000.000	6,96 %	52
2021	15.791.588.000.000	5.229.148.000.000	3.028.205.000.000	19,18 %	74
2022	18.328.517.000.000	6.957.581.000.000	4.260.182.000.000	23,18 %	104
2023	18.892.400.000.000	8.215.656.000.000	5.512.192.000.000	29,18 %	124

Source: Processed data

It can be seen that BSI's revenue increases every year; even over six years, its revenue has increased 6 times. Not only revenue but also the Company's profit has increased, as reflected in the EBITDA, Net Profit, and NPM ratios. Net Profit reflected in the NPM ratio has increased over the past six years. Whereas in 2019, it was 2.76%. In 2023, it had reached 29.18%. The results of the study showed that cyberattack events did not affect stock returns; these results were also reinforced by the EPS ratio, which is a ratio that compares the Company's net profit with the number of shares in the capital market. The EPS value has increased every year to reach 124.

Table 5. ROA and ROE

Year	Return on Asset	Return on Equity
2019	0,17 %	1,45 %
2020	0,43 %	4,56 %
2021	1,56 %	12,11 %
2022	1,76 %	12,71 %
2023	1,62 %	14,72 %

Table 5 shows the BSI ROA and ROE ratio data, which explains an annual increase in both ROA and ROE. ROA is a ratio that describes how efficient the Company is in managing resources that generate profit. At the same time, ROE is a ratio that describes how efficiently the Company utilizes its shareholders' capital to help prospective investors or investors make decisions to invest.

Table 6. BRI Dividends

Stock	BRIS
Status	FINAL
Payent Type	TUNAI
Dividen Per Share	IDR 9.23431
Total Dividen	IDR 426,018,167,788
Cum Date	Tue, 30 May 2023
Ex Date	Wed, 31 May 2023
Rec Date	Mon, 05 Jun 2023
Dist Date	Fri, 23 Jun 2023

Source: IDX Mobile

BSI has great potential to become one of the world's leading Islamic banks. The company's solid performance supports this, the Indonesian government's commitment to developing the halal industry and the fact that Indonesia has the world's largest Muslim population. Even when experiencing a cyberattack, BRIS could distribute dividends after its first dividend in 2018 of IDR 1.10 per share. After that, BRIS shares also distributed cash dividends of 10% of the company's net profit in 2022, or around IDR 426.02 billion, equivalent to IDR 9.24 per share.

CONCLUSION

Based on the results of the research that has been conducted, it can be concluded that the cyberattack incident that occurred at BSI did not affect stock performance as reflected in returns. This is evident from the comparative test using the Wilcoxon test, and the significance value is above 0.05, namely 0.852, which means that the BRIS stock return did not change before or after the cyberattack incident. This indicates that the BSI stock return is stable despite the cyberattack, where the market tends to focus on fundamental performance, as seen from the discussion above, and the long-term prospects of BSI shares. So that the cyberattack did not affect the performance of BSI shares as reflected in stock returns. The results of this study can help prospective investors make investment decisions, especially in BSI/BRIS shares. This study has limitations in sampling, namely, only 36 samples before and after the incident. So, questions for further research can be more on the number of samples taken.

REFERENCE

Afifah, D. (2023). Perlindungan Konsumen di Sektor Jasa Keuangan pada Kasus Serangan Siber Ransomware yang Menimpa Perbankan. *JIIP-Jurnal Ilmiah Ilmu Pendidikan*, *6*(11), 9318–9323.

Bravely, I. (2023). Analisis pergerakan harga saham setelah layanan terhenti (Studi kasus PT Bank Syariah Indonesia Tbk.). *Jurnal Mirai Management*, *8*(1), 231–236.

Cahyanti, I. S., Janwari, Y., Solehudin, E., & Jubaedah, D. (2024). The Effect of Interest Rates and Inflation on Islamic Stock Returns in Companies Listed on the Jakarta Islamic Index. *Airlangga International Journal of Islamic Economics and Finance*, *7*(01), 15–28. https://doi.org/10.20473/aijief.v7i01.55610

Dermawan, I., Baidawi, A., & Dewi, S. M. (2023). Serangan Cyber dan Kesiapan Keamanan Cyber Terhadap Bank Indonesia. *Jurnal Informasi Dan Teknologi*, 20–25.

Faizal, M. A., Faizatul, Z., Asiyah, B. N., & Subagyo, R. (2023). Analisis Risiko Teknologi Informasi Pada Bank Syariah: Identifikasi Ancaman Dan Tantangan Terkini. *Jurnal Asy-Syarikah: Jurnal Lembaga Keuangan, Ekonomi dan Bisnis Islam*, *5*(2), 87–100. https://doi.org/10.47435/asy-syarikah.v5i2.2022

Fitriani, R., Subagiyo, R., & Asiyah, B. N. (2023). Mitigating IT Risk of Bank Syariah Indonesia: A Study of Cyber Attack on May 8, 2023. *Al-Amwal : Jurnal Ekonomi Dan Perbankan Syari'ah*, *15*(1), 86. https://doi.org/10.24235/amwal.v15i1.14124

Hogan, K. M., Olson, G. T., Mills, J. D., & Zaleski, P. A. (2023). An Analysis of Cyber Breaches and Effects on Shareholder Wealth. *International Journal of the Economics of Business*, *30*(1), 51–78. https://doi.org/10.1080/13571516.2023.2168994

Irawan, H., Dianita, I., & Mulya, A. D. S. (2021). Peran bank syariah Indonesia dalam pembangunan ekonomi nasional. *Jurnal Asy-Syarikah: Jurnal Lembaga Keuangan, Ekonomi Dan Bisnis Islam*, *3*(2), 147–158.

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*, 103705. https://doi.org/10.1016/j.frl.2023.103705

Martono, N. (2010). *Metode penelitian kuantitatif: Analisis Isi dan Analisis Data Sekunder (sampel halaman gratis)*. RajaGrafindo Persada. https://books.google.com/books?hl=en&lr=&id=tUl1BgAAQBAJ&oi=fnd&pg=PR7&dq=Metode+Penelitian+Kuantitatif:+Analisis+Isi+dan+Analisis+Data+Sekunder&ots=FfnfKDZ22a&sig=j68_6gaNJ67Qm3sUuYNd_CKSC_4

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. *Rayah Al-Islam*, *7*(3), 1755–1768.

Nisa, Z. F., & Cahyono, Y. T. (2024). The effect of cyber attacks on stock performance Bank Syariah Indonesia. *InCAF Proceeding of International Conference On Accounting and Finance*, *2*, 359–368.

Pramesti, G. (2018). *Mahir Mengolah data Penelitian Dengan Spss 25. Elex media*.

Putri, D. F., Andriani, Sari, W. R., & Nabbila, F. L. (2023). Analisis Perlindungan Nasabah BSI Terhadap Kebocoran Data Dalam Menggunakan Digital Banking. *JURNAL ILMIAH EKONOMI DAN MANAJEMEN*, *1*(4), Article 4. https://doi.org/10.61722/jiem.v1i4.331

Radiansyah, I., Rusdjan, C., & Priyadi, Y. (2016). Analisis Ancaman Phishing Dalam Layanan Online Banking. *Journal of Innovation in Business and Economics*, *7*(1), 1–14.

Restika, R., & Sonita, E. (2023). Tantangan keamanan siber dalam manajemen likuiditas bank syariah: menjaga stabilitas keuangan di era digital. *Krigan: Journal of Management and Sharia Business*, *1*(2), 25. https://doi.org/10.30983/krigan.v1i2.7929

Solikhawati, A., & Samsuri, A. (2023a). Evaluasi Bank Syariah Indonesia Pasca Serangan Siber: Pergerakan Saham dan Kinerja. *Jurnal Ilmiah Ekonomi Islam*, *9*(3), 4201. https://doi.org/10.29040/jiei.v9i3.10309

Solikhawati, A., & Samsuri, A. (2023b). Evaluasi Bank Syariah Indonesia Pasca Serangan Siber: Pergerakan Saham dan Kinerja. *Jurnal Ilmiah Ekonomi Islam*, *9*(3), 4201. https://doi.org/10.29040/jiei.v9i3.10309

Tristanto, T. A., Nugraha, N., Waspada, I., Mayasari, M., & Kurniati, P. S. (2023). Sustainability performance impact of corporate performance in Indonesia banking. *Journal of Eastern European and Central Asian Research (JEECAR)*, *10*(4), 668–678.

Wijayani, D. R. (2017). Kepercayaan Masyarakat Menabung pada Bank Umum Syariah. *Muqtasid: Jurnal Ekonomi dan Perbankan Syariah*, *8*(1), 1. https://doi.org/10.18326/muqtasid.v8i1.1-12

Zamzami Akromi Lubis & Fauzi Arif Lubis. (2024). Pengaruh Persepsi Keamanan dan Kepercayaan Terhadap Loyalitas Nasabah: Studi Kasus Serangan Siber di Bank Syariah Indonesia. *El-Mal: Jurnal Kajian Ekonomi & Bisnis Islam*, *5*(10). https://doi.org/10.47467/elmal.v5i10.5280