

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

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

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 menunjukkan 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*

## PENDAHULUAN

Serangan siber telah menjadi fenomena yang semakin umum dan kompleks dalam era teknologi modern. Institusi keuangan, termasuk bank-bank syariah, tidak luput dari risiko ini. Bank Syariah Indonesia (BSI) sebagai salah satu bank syariah terbesar di Indonesia, telah mengalami serangan siber yang cukup signifikan pada pertengahan tahun 2023 (Faizal dkk., 2023). Hal ini tidak saja berdampak pada infrastruktur teknologinya, tetapi juga pada citra dan kepercayaan nasabah. Sejalan dengan hasil penelitian yang menjelaskan bahwa kepercayaan nasabah terpengaruh secara serius oleh insiden, mengindikasikan keprihatinan terhadap keamanan layanan perbankan (Maulana & Fitriana, 2023). Tidak hanya itu, adanya kasus siber ini dilihat dari sisi Persepsi Keamanan dan Kepercayaan secara simultan berpengaruh terhadap Loyalitas Nasabah Pada Bank Syariah Indonesia (Zamzami Akromi Lubis & Fauzi Arif Lubis, 2024).

Sementara itu, pergerakan saham BRIS milik Bank Syariah Indonesia mengalami fluktuasi selama 10 hari terakhir pada tanggal 8 Mei 2023 yang pada akhirnya ditutup karena efek panik dari investor pasca berita serangan siber. Sedangkan pergerakan kinerja keuangan BSI memiliki dasar keuangan yang cukup kuat dilihat dari rasio KPMM, ROA, ROE, dan BOPO yang dinilai baik karena di atas standar rasio. Namun, pada rasio FDR mengalami penurunan nilai yang berarti bank memiliki ketergantungan yang tinggi pada simpanan berjangka (Solikhawati & Samsuri, 2023).

Era digital yang semakin berkembang, teknologi informasi telah menjadi bagian integral dari operasional industri perbankan. Transformasi digital ini tidak hanya memberikan kemudahan dalam pelayanan, tetapi juga menghadirkan tantangan baru, salah satunya adalah ancaman serangan siber. Serangan siber di sektor keuangan, termasuk perbankan, berpotensi mengganggu operasional, merusak reputasi, dan menurunkan kepercayaan nasabah.

Dampak dari serangan ini dapat meluas hingga ke pasar saham, di mana fluktuasi harga saham seringkali dipengaruhi oleh persepsi investor terhadap risiko dan stabilitas Perusahaan (Restika & Sonita, 2023). Terdapat risiko keamanan seperti phishing, malware, dan gangguan layanan, yang dapat merugikan nasabah dan mengancam kepercayaan terhadap institusi perbankan. Analisis perlindungan nasabah BSI melibatkan pemahaman terhadap kebijakan keamanan, respons terhadap serangan siber, dan kebijakan perlindungan data nasabah (Putri dkk., 2023).

Indikator ekonomi suatu bangsa dapat ditinjau dari perkembangan sektor perbankan. Seperti yang diketahui Bank Syariah Indonesia (BSI) merupakan salah satu bank syariah dengan aset terbesar karena merupakan hasil merger dari 3 bank syariah yakni BRI Syariah, BNI Syariah dan Bank Syariah Mandiri. Tidak hanya dilihat dari sisi aset ada hal lain yang perlu diperhatikan yakni dari sisi teknologi. Namun, operasional perbankan yang bergantung pada teknologi membuatnya rentan terhadap serangan siber (Irawan dkk., 2021). Serangan siber dapat bermanifestasi dalam banyak bentuk, mulai dari ransomware yang mengenkripsi data sampai gangguan sistem layanan perbankan. Contohnya, serangan ransomware pada tahun 2023 telah berhasil menginfeksi 1,5 terabyte data BSI, termasuk informasi sensitif seperti nomor rekening, riwayat transaksi, dan email nasabah. (Wijanarko dkk., 2023) Gangguan ini tidak saja menyebabkan ketidaknyamanan bagi nasabah namun juga berpotensi menguras biaya tambahan untuk pemulihan dan kompensasi.

Bank Syariah Indonesia (BSI), sebagai salah satu lembaga keuangan syariah terbesar di Indonesia, tidak luput dari ancaman ini. Meskipun prinsip-prinsip syariah yang diusung oleh BSI memberikan diferensiasi dibandingkan dengan bank konvensional, ancaman terhadap keamanan siber tetap menjadi isu kritis yang harus dihadapi. (Fitriani dkk., 2023) Sebuah serangan siber yang berhasil dapat merusak citra bank, menyebabkan kebocoran data nasabah, dan mengganggu operasional. Dampak negatif ini tidak hanya dirasakan oleh nasabah, tetapi juga oleh para investor, yang pada akhirnya dapat mempengaruhi kinerja saham bank di pasar modal (Afifah, 2023).

Penelitian ini bertujuan untuk menganalisis dampak serangan siber terhadap kinerja saham Bank Syariah Indonesia. Melalui studi kasus perbandingan harga saham sebelum dan sesudah insiden serangan siber, diharapkan penelitian ini dapat memberikan pemahaman yang lebih mendalam mengenai hubungan antara keamanan siber dan fluktuasi harga saham. Selain itu, penelitian ini juga diharapkan dapat memberikan wawasan bagi para pelaku industri perbankan dan investor mengenai pentingnya penguatan sistem keamanan siber untuk meminimalisir risiko finansial yang dapat muncul akibat serangan siber di masa mendatang (Dermawan dkk., 2023).

Penelitian ini juga akan mengkaji seberapa besar tingkat sensitivitas investor terhadap insiden serangan siber yang terjadi di industri perbankan, khususnya pada perbankan syariah. Pada akhirnya, temuan ini diharapkan dapat menjadi dasar pertimbangan bagi bank syariah untuk meningkatkan

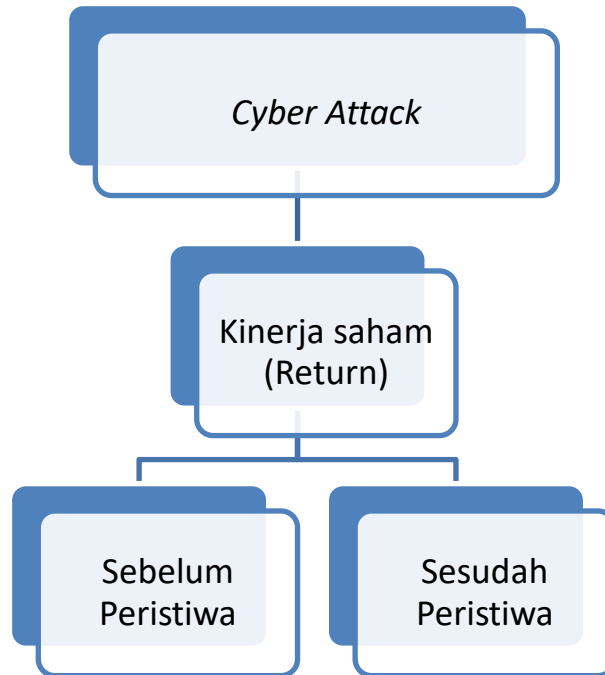
sistem keamanan siber dan menjaga kepercayaan publik serta stabilitas kinerja saham mereka. (Wijayani, 2017)

Melalui melakukan analisis ini, kita dapat memahami betapa seriusnya potensi risiko serangan siber bagi institusi keuangan dan bagaimana investor bereaksi terhadap insiden semacam itu. Hasil penelitian ini dapat digunakan sebagai referensi penting bagi manajemen bank, regulator keuangan, dan investor sendiri dalam mengantisipasi dan merespons risiko serangan siber. Selanjutnya, kita akan menjelaskan metode detail dan hasil penelitian untuk membantu memahami kompleksitas interaksi antara serangan siber dan kinerja saham Bank Syariah Indonesia. Dengan demikian, kita dapat memberikan gambaran yang lebih lengkap tentang dampak serangan siber terhadap stabilitas ekonominasional dan kepercayaan investor dalam industri perbankan syariah Indonesia.

## METODE PENELITIAN

Pendekatan penelitian ini merupakan penelitian kuantitatif dengan menggunakan teknik penelitian studi kasus yakni sebelum dan sesudah terjadinya peristiwa serangan siber di BSI. Metode yang digunakan dalam penelitian ini adalah komparatif dengan membandingkan kinerja saham melalui return saham dari sebelum dan sesudah terjadinya serangan siber. Variabel dalam analisis data penelitian ini adalah return saham BSI. Pengumpulan data dalam penelitian ini menggunakan teknik dokumentasi. Penelitian ini menggunakan data sekunder berupa data pergerakan saham BSI yang diperoleh dari database IDX dan Yahoo Finance (Martono, 2010). Peneliti mengolah dan menganalisis data menggunakan tahapan uji normalitas dan uji komparatif menggunakan aplikasi IBM SPSS 25 (Pramessti, 2018). Periode penelitian adalah 72 hari, 36 hari sebelum dan sesudah serangan *cyberattack*. Peneliti menganalisis apakah serangan kejahatan *cyberattack* mempengaruhi kinerja saham BSI melalui return saham.

Sehingga kerangka dari penelitian ini tergambar sebagai berikut :



**Gambar 1. Kerangka Penelitian**

Menguji apakah terdapat perbedaan signifikan kinerja harga saham sebelum dan sesudah peristiwa terjadi, maka dilakukan uji hipotesis dengan menggunakan uji Wilcoxon.

## HASIL PENELITIAN DAN PEMBAHASAN

**Tabel 1. Statistik Deskriptif**

Variable	Mean	Std. Dev	Min	Max
Sebelum	0.0031	0.2328	0.00	0.05
Sesudah	0.0006	0.02917	0.00	0.06

Sumber: Data diolah

Variabel return saham BRIS sebelum terjadinya peristiwa *cyberattack* berada pada rentang nilai 0.00 sampai 0.05, dengan Standar deviasi sebelum terjadinya peristiwa *cyberattack* adalah 0.2328 dan Mean sebesar 0.0031. Sementara variabel return saham BRIS setelah terjadinya peristiwa *cyberattack* berada pada rentang 0.00 sampai 0.0, dengan Standar deviasi sebelum terjadinya peristiwa *cyberattack* adalah 0.02917 dan Mean sebesar 0.0009.

Tabel 2. Uji Normalitas

		Kolmogorov-Smirnov <sup>a</sup>			Shapiro-Wilk		
		Statistic	df	Sig.	Statistic	df	Sig.
Return	sebelum	,157	36	,025	,938	36	,043
	Sesudah	,206	36	,000	,825	36	,000

a. Lilliefors Significance Correction

Pada penelitian ini, dilakukan uji normalitas dengan menggunakan uji One-Sample Kolmogorov-Smirnov Test dan Shapiro Wilk. Kemudian untuk hasil uji One-Sample Kolmogorov-Smirnov Test, distribusi data untuk kondisi *sebelum* dan *sesudah* tidak berdistribusi normal. Nilai statistik uji Kolmogorov-Smirnov menunjukkan bahwa perbedaan absolut terbesar antara distribusi data yang diamati dan distribusi teoretis adalah 0,157 untuk *sebelum* dan 0,206 untuk *sesudah*. Hasil uji signifikansi menghasilkan p-value sebesar 0,025 untuk *sebelum* dan 0,000 untuk *sesudah*, keduanya lebih kecil dari 0,05.

Hasil uji Shapiro Wilk pun sama, distribusi data untuk kondisi *sebelum* dan *sesudah* tidak berdistribusi normal. Nilai statistik uji Kolmogorov-Smirnov Shapiro Wilk menunjukkan bahwa perbedaan absolut terbesar antara distribusi data yang diamati dan distribusi teoretis adalah 0,938 untuk *sebelum* dan 0,825 untuk *sesudah*. Hasil uji signifikansi menghasilkan p-value sebesar 0,043 untuk *sebelum* dan 0,000 untuk *sesudah*, keduanya lebih kecil dari 0,05. Karena hasil uji normalitas menyatakan bahwa data yang diteliti tidak berdistribusi normal, maka datanya termasuk data nonparametrik. Sehingga untuk pengujian komparatif selanjutnya menggunakan uji wilcoxon

Tabel 3. Uji Wilcoxon  
Test Statistics<sup>a</sup>

	Sesudah - Sebelum
Z	-.186 <sup>b</sup>
Asymp. Sig. (2-tailed)	,852

a. Wilcoxon Signed Ranks Test

b. Based on positive ranks.

Berdasarkan hasil uji Wilcoxon yang ditunjukkan pada tabel, dapat disimpulkan bahwa perbedaan rata-rata antara kondisi *sebelum* dan *sesudah* mempunyai Nilai signifikansi (Sig. 2-tailed) sebesar 0,852, yang jauh lebih besar dari ambang batas 0,05. Tidak ada perbedaan yang signifikan secara statistik antara kondisi *sebelum* dan *sesudah*. Hasil ini menunjukkan bahwa perubahan yang terjadi kemungkinan besar disebabkan oleh faktor kebetulan atau variasi alami, dan tidak ada bukti kuat yang menunjukkan adanya efek yang nyata dari *cyberattacks*.

Bank Syariah Indonesia merupakan bank hasil merger antara bank BRI Syariah, Bank Mandiri Syariah, dan BNI Syariah yang diresmikan pada tanggal 1 Februari 2021. Pada tanggal 8 Mei 2023 layanan BSI tidak bisa digunakan oleh seluruh nasabah. Layanan tersebut diantaranya: layanan langsung di kantor cabang, mesin ATM, dan aplikasi layanan mobile. Serangan siber yang menyebabkan penurunan harga saham BRIS milik Bank Syariah Indonesia merupakan hal yang merugikan dan mengkhawatirkan. Keamanan siber menjadi isu yang krusial dalam dunia perbankan, dan serangan tersebut dapat mempengaruhi kepercayaan investor serta citra perusahaan (Bravely, 2023)

Menurut (Jin dkk., 2023) bahwa ketika perusahaan mengalami serangan siber, manajemen perlu waspada untuk meningkatkan pengendalian internal, menurunkan risiko operasional, dan menjaga reputasi. Oleh karena itu, bank kemungkinan akan melakukan lebih sedikit manajemen laba dan meningkatkan kualitas informasi akuntansi, tergantung pada serangan siber. Meskipun demikian, ketika sebuah bank menjadi korban serangan siber, bank tersebut mungkin kehilangan nasabah atau mengalami gangguan operasional bisnis. Bank berpotensi melakukan lebih banyak manajemen pendapatan untuk memitigasi potensi dampak negatif serangan siber terhadap pendapatannya (Hogan dkk., 2023)

Berdasarkan hasil uji Paired Samples Test yang ditunjukkan pada gambar, dapat disimpulkan bahwa perbedaan rata-rata antara kondisi *sebelum* dan *sesudah* sebesar 0,00250 dengan standar deviasi 0,03581. Interval kepercayaan 95% dari perbedaan tersebut berkisar antara -0,00962 hingga 0,01462, yang mencakup nilai nol. Nilai t yang dihasilkan sebesar 0,419 dengan derajat kebebasan (df) sebanyak 35.

Nilai signifikansi (Sig. 2-tailed) sebesar 0,678, yang jauh lebih besar dari ambang batas 0,05. Dengan demikian, tidak ada perbedaan yang signifikan secara statistik antara kondisi *sebelum* dan *sesudah*. Hasil ini menunjukkan bahwa perubahan yang terjadi kemungkinan besar disebabkan oleh faktor

kebetulan atau variasi alami, dan tidak ada bukti kuat yang menunjukkan adanya efek yang nyata dari *cyberattack*.

Serangan siber yang berhasil dapat berdampak pada finansial yang signifikan bagi perusahaan. Biaya penanganan serangan, pemulihan sistem, audit keamanan, serta ganti rugi yang mungkin harus dibayarkan kepada pelanggan yang terkena dampak dapat menjadi beban yang berat bagi perusahaan (Solikhawati & Samsuri, 2023). Hal ini dapat berpengaruh negatif terhadap kinerja keuangan perusahaan, dan investor khawatir terjadi potensi penurunan pendapatan dan laba.

Oleh karena itu, penting bagi perusahaan untuk memiliki angkah-langkah keamanan siber yang kuat dan responsif, serta kemampuan untuk mengatasi serangan siber dengan cepat dan efektif (Radiansyah dkk., 2016). Hal ini berarti bahwa serangan kejahatan siber memiliki implikasi yang merugikan bagi masyarakat umum. Informasi yang tidak akurat akan berdampak pada kondisi pasar modal, khususnya kinerja saham BSI (Nisa & Cahyono, 2024). Transparansi dan komunikasi yang baik dengan investor dan pemangku kepentingan juga penting untuk membangun kepercayaan dan meminimalkan dampak negatif yang mungkin timbul akibat serangan siber.

Dapat kita lihat bahwa tidak terjadi perubahan harga yang signifikan di awal terhentinya layanan bisnis terhadap konsumen. Akan tetapi jika layanan tetap terhenti serta diperparah dengan berita serangan *cyber* dan kebocoran data perusahaan (Bravely, 2023). Seorang investor harus melakukan analisis ekonomi untuk menentukan keputusan ekonomi karena analisis ekonomi cenderung memiliki hubungan yang kuat antara apa yang terjadi di lingkungan ekonomi makro dengan kinerja pasar modal (Cahyanti dkk., 2024).

Bahkan kita lihat kinerja bank syariah yang cukup baik menunjukkan adanya dasar keuangan yang kuat dan kemampuan untuk mengatasi masalah tersebut. Hal ini menunjukkan bahwa BSI memiliki sistem manajemen risiko yang baik yang berhasil mengisolasi dampak serangan siber (Tristanto dkk., 2023)

**Tabel 4. Laporan Laba Rugi dan Rasio Keuangan**

Tahun	Pendapatan	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

Sumber : Data diolah



Dapat dilihat bahwa pendapatan dari BSI meningkat setiap tahun, bahkan selama enam tahun pendapatannya meningkat 6 kali. Tidak hanya pendapatan, laba Perusahaan pun sama meningkat yang tercermin dari rasio EBITDA, Net Profit dan NPM. Laba Bersih yang tercermin dalam rasio NPM menunjukkan kenaikan selama enam tahun terakhir Dimana pada tahun 2019 sebesar 2,76% di tahun 2023 sudah mencapai 29,18%. Hasil penelitian yang menunjukkan bahwa peristiwa *cyberattack* tidak mempengaruhi return saham, hasil tersebut diperkuat juga dengan rasio EPS yang merupakan rasio yang membandingkan laba bersih Perusahaan dengan jumlah saham di pasar modal. Nilai EPS mengalami kenaikan setiap tahunnya hingga mencapai 124.

**Tabel 5. ROA dan ROE**

Tahun	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 %

Berdasarkan Tabel 5 merupakan data rasio ROA dan ROE BSI yang menjelaskan bahwa terjadi peningkatan setiap tahunnya, baik ROA maupun ROE. ROA merupakan rasio yang menggambarkan seberapa efisien Perusahaan dalam mengelola sumber daya yang menghasilkan laba. Sementara ROE merupakan rasio yang menggambarkan seberapa efisien Perusahaan dalam memanfaatkan modal pemegang sahamnya. Sehingga dapat membantu calon investor atau investor dalam pengambilan Keputusan untuk berinvestasi.

**Tabel 6. Dividen BRI**

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

Sumber : IDX Mobile

BSI memiliki potensi besar untuk menjadi salah satu bank syariah terdepan didunia. Hal ini didukung oleh kinerja perseroan yang cukup solid,

adanya komitmen pemerintah Indonesia untuk mengembangkan industri halal, dan fakta bahwa Indonesia adalah negara dengan jumlah penduduk muslim terbesar didunia. Bahkan ketika mengalami *cyberattack* BRIS mampu membagikan deviden, setelah dividen pertamanya ditahun 2018 sebesar Rp1,10 persaham. Setelah itu, saham BRIS juga kembali membagikan dividen tunai sebesar 10% dari perolehan laba bersih perseroan pada tahun 2022, atau sekitar Rp. 426,02 miliar yang ekuivalen dengan Rp.9,24 perlembar saham.

### KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, maka dapat disimpulkan bahwa adanya peristiwa *cyberattack* yang terjadi di BSI tidak berpengaruh terhadap kinerja saham yang tercermin dalam return. Hal tersebut terbukti dari hasil uji komparatif dengan menggunakan uji Wilcoxon, nilai signifikansinya diatas 0,05 yakni 0,852 yang mempunyai arti bahwa return saham BRIS tidak mengalami perubahan baik sebelum atau pun setelah terjadinya peristiwa *cyberattack*. Hal tersebut menandakan bahwa return saham BSI stabil meski terjadi serangan siber, dimana pasar cenderung fokus pada kinerja fundamental yang dapat dilihat dari pembahasan diatas, serta prospek panjang saham BSI. Sehingga terjadinya serangan siber tidak mempengaruhi kinerja saham BSI yang tercermin dalam return saham. Hasil penelitian ini dapat membantu calon investor atau investor dalam pengambilan Keputusan berinvestasi khususnya pada saham BSI/BRIS. Penelitian ini terdapat keterbatasan dalam pengambilan sampel yang dilakukan, yakni hanya 36 sampel sebelum dan sesudah terjadinya peristiwa. Sehingga saran untuk penelitian selanjutnya bisa lebih banyak dalam jumlah pengambilan sampel.

## DAFTAR PUSTAKA

- 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=tU11BgAAQBAJ&oi=fnd&pg=PR7&dq=Metode+Penelitian+Kuantitatif:+Analisis+Isi+dan+>

Analisis+Data+Sekunder&ots=FfnfKDZ22a&sig=j68\_6gaNJ67Qm3sUu  
YNd\_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>