Sustainability and Social Impact

Research Article

Analysis of Stock Prices and Transaction Volumes of BRIS Before and After the Ransomware Attack

Khoirunnisa, Ahmad Dahlan Malik, Wahyu Agung Handono, Elsi Mersilia Hanesti

Received: 3 June 2025
Accepted: 10 September 2025
Published: 11 November 2025

Keywords:
Ransomware, Stock Prices, Transaction Volume, Indonesian Islamic Bank, BRIS.

ABSTRACT

Bank Syariah Indonesia (BSI) is currently the largest Islamic bank in Indonesia. However, BSI recently experienced disruptions in several services, including mobile banking, due to a ransomware attack that essentially locks access to data, thereby disrupting business operations. This phenomenon also led to a decline in BSI's stock, coded BRIS. The purpose of this study is to determine the differences in stock prices and transaction volumes before and after the ransomware attack. This research employs a quantitative method with a comparative research approach. The data sources for this study are secondary data obtained from the websites www.finance.yahoo.com and www.idx.co.id. The analysis techniques used include descriptive statistical analysis, normality tests, and hypothesis testing. The results of the hypothesis tests using the Paired Sample T-Test for stock prices and the Wilcoxon Signed Ranks Test for transaction volumes indicate significant differences in stock prices and transaction volumes before and after the ransomware attack that occurred in 2023.

INTRODUCTION

Banking is an industry related to banking activities, including the provision of financial services encompassing fund collection, investment management, lending, and other financial transactions. Conventional and Islamic banking are two types of financial banking institutions in Indonesia [10]. The Minister of State-Owned Enterprises (BUMN) representing the government stated that Indonesia must become a global center for Islamic finance and economics. To achieve this goal, the establishment of large-scale Islamic banks with strong assets and capital is necessary [15].

This step is realized through the establishment of Bank Syariah Indonesia (BSI). As the largest Islamic bank in Indonesia, BSI has significant potential [2], in the last two years, BSI has successfully attracted 19 million customers, making it the fifth-largest bank in Indonesia. Additionally, ranks BSI first as the bank with the most customers in Indonesia [4]. Besides being the Islamic bank with the most users in Indonesia, the merger conducted by BUMN has affected the shares owned by BSI. On the Indonesia Stock Exchange (IDX), BSI's shares are listed under the code BRIS. This merger has the potential to increase the value of BSI's shares.

Therefore, investors need to consider this information before deciding to invest in BSI's shares.

With BSI's current growth, it is expected to foster public trust in using Islamic banks for various financial-related activities. However, there are factors that diminish the level of trust among the Indonesian public, particularly BSI customers, in using the Islamic banking system, primarily due to a ransomware attack a few months ago that caused disruptions in several services, including mobile banking. According to a report [14], BSI's services experienced system disruptions from May 8 to May 11, 2023, preventing

customers from conducting financial transactions, both offline and online. This type of ransomware attack differs from hackers attempting to access an account. Ransomware perpetrators aim to encrypt critical data, backups, and systems to disrupt business operations.

Essentially, ransomware works by locking access, thereby disrupting business operations, but the information within is not stolen; rather, access to the information management system is compromised. This attack also resulted in a decline in the stock of Bank Syariah Indonesia BRIS, which fell to the Auto Reject Bottom (ARB) during the first trading session on Tuesday, May 16, 2023, at the level of 1,600. This represents a decline of 120 points from the previous closing level of 1,720 [12]. This incident indicates that events affecting a company can significantly influence its stock value. In other words, a company's performance and image can also serve as indicators of its prospects, thus affecting investment decisions. The objective of this research is to analyse the differences by comparing the stock prices of BRIS and the transaction volumes of BRIS before and after the ransomware attack that occurred in 2023.

Ransomware is a form of malicious software (malware) that has the potential to cause damage, created to encrypt data on computer systems or other devices [5]. Additionally, this software will demand a ransom from the victim to unlock their data. Ransomware poses a serious threat as it can lead to financial losses and disrupt business operations. With its ability to lock systems, the impact of ransomware can be very detrimental. Ransomware attacks, when viewed from an Islamic perspective, resemble theft and a means of taking someone else's property, both of which are explicitly prohibited in Islamic teachings. If data or other items are taken without the owner's permission, it is considered theft in Islam. Preventive measures are necessary to anticipate ransomware attacks that can be carried out by organizations or individuals [5], including:

a. Regularly backing up data to external storage or other secure locations.
b. Ensuring that software and operating systems are always updated to the latest versions.
c. Using reliable security solutions, such as installing trusted software.
d. Avoiding clicks on suspicious or unknown emails and links.
e. Using strong and unique passwords, combining letters, numbers, and specific characters.
f. Appropriately limiting user and user group access.
g. Activating firewalls on devices and antivirus software to restrict potentially harmful or suspicious websites.

By implementing preventive measures against ransomware attacks, organizations or individuals can at least minimize the risk of such attacks.

Stocks are defined as instruments in the financial market that serve as representations of ownership in a company [8]. Meanwhile, according to Fatwa DSN-MUI No. 135/DSN-MUI/V/2020, stocks that meet the requirements and conditions based on Islamic principles are referred to as sharia stocks. The requirements and conditions for sharia stocks include that the company exchanging stocks does not engage in haram businesses, the transactions involved do not contain elements of riba, and the company's financial ratios include interest-based debt not exceeding 45 percent of assets, and non-halal interest income not exceeding 10 percent of business revenue and others [7].

Stock prices result from the interaction between the bid price from buyers and the ask price or offer price from sellers [6]. This price is formed from the activities of investors selling and buying stocks. The total shares traded over a period is referred to as the stock transaction volume. The size of the stock transaction volume reflects investor interest in engaging in the buying and selling activities of the company's shares. Increased supply and demand for stocks will result in more volatile stock price movements. An increase in stock transaction volume indicates that the public is increasingly interested in those stocks, impacting stock fluctuations (Amelia, 2023).

RESULTS & DISCUSSION

Research Results

A. Stock Prices of BRIS

Table 4.1 Hypothesis Test for Stock Prices of BRIS

Paired Samples Test

		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference Lower	Upper			
Pair 1	stock price before ransomware attack - stock price after ransomware attack	-45,600	104,733	14,811	-75,365	-15,835	-3,079	49	,003

Source: Data processed by the researcher, 2025.

In Table 4.1, the significance value shows a significance level of 0.003. The significance level is 0.003 < 0.05. Thus, this significance value proves that H1 is accepted and H01 is rejected, indicating that there is a significant difference in BRIS stock prices before and after the ransomware attack that occurred in 2023.

B. Transaction Volume

Table 4.2 Hypothesis Test for Transaction Volume of BRIS Stocks

Ranks

		N	Mean Rank	Sum of Ranks
Stock Transaction Volume Before Ransomeware Attack - Stock Transaction Volume After	Negative Ranks	7[a]	20,93	146,50
	Positive Ranks	41[b]	25,11	1029,50
	Ties	2[c]		
	Total	50		

Test Statistics[a]

	Stock Transaction Volume Before Ransomeware Attack - Stock Transaction Volume After Ransomware Attack
Z	-4,529[b]
Asymp. Sig. (2-tailed)	,000

Source: Data processed by the researcher, 2025.

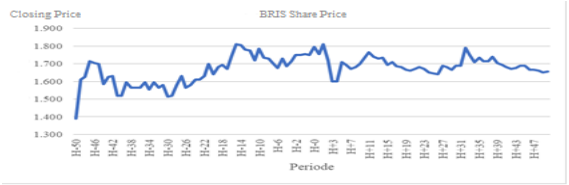
From the normality test conducted earlier, the transaction volume of stocks shows significance < 0.05, thus the hypothesis test for transaction volume uses the Wilcoxon Signed Ranks Test. The significance value of 0.000 is shown in Table 4.6, which is <0.05. Therefore, this result proves that H2 is accepted and H02 is rejected, indicating a significant difference between the transaction volume of BRIS stocks before and after the ransomware attack that occurred in 2023.

Discussion

A. Differences in BRIS Stock Prices Before and After the Ransomware Attack in 2023

To see the extent of the ransomware attack's impact on BRIS stock prices, we can refer to Graph 4.3, where the stock price data of BRIS is obtained from daily closing prices over the 50 days before and 50 days after the ransomware attack that occurred in 2023 through the Yahoo Finance website.

Graph 4.3 Analysis of BRIS Stock Prices



Source: Data processed, 2025.

In the graph above, it can be stated that BRIS stock prices before the ransomware attack showed a positive trend and reached a peak. Descriptive analysis also supports this finding, with the highest stock price before the ransomware attack reaching Rp. 1,810. Factors that may have contributed to this positive trend include BSI's strong financial performance, which showed stable growth, with a net profit of Rp 1.46 trillion in the first quarter of 2023 [11].

Meanwhile, stock prices after the ransomware attack tended to decline. Although there was a temporary increase during the attack, the stock price fell sharply on the third day after the ransomware attack, even reaching the level of Rp 1,600. This decline was triggered by panic selling from investors wanting to exit BRIS due to concerns about the impact of the attack. The market's reaction to the ransomware attack is understandable, as such attacks can create uncertainty and concerns about the company's performance and stability. However, not all investors engaged in selling; many long-term investors chose to delay selling BRIS shares until the situation became clearer. This reflects investor caution in making investment decisions, especially in uncertain situations like ransomware attacks.

The impact of the ransomware attack not only harms customers and shareholders but can also damage public trust in the BSI company. This is also evidenced by the results of the tests in the research results section, where the comparison test of BRIS stock prices before and after the ransomware attack using the Paired Sample T-Test showed a significance result of 0.003. Knowing that the significance of 0.003 is less than 0.05 means H1 is accepted and H01 is rejected, this test result proves that there is a significant difference in BRIS stock prices due to the ransomware attack that occurred in 2023.

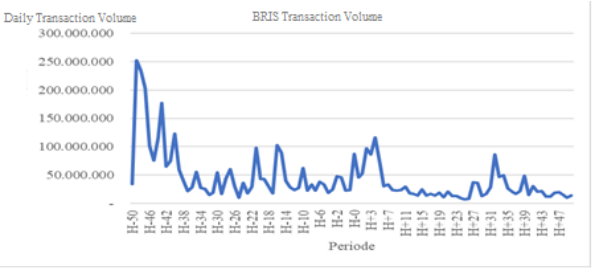
In addressing the ransomware attack affecting BSI, the company has shown a quick and responsive response in clarifying the situation. This step is crucial to alleviate investor concerns and prevent greater panic in the market. By assuring the public that customer data is safe and operations are not disrupted, BSI has successfully rebuilt trust and the company's reputation in facing this crisis. The actions taken by BSI to restore public trust are a form of risk management and developing mitigation plans [9].

B. Differences in BRIS Transaction Volume Before and After the Ransomware Attack in 2023

The transaction volume of stocks is the total shares traded over a period. The size of the stock transaction volume reflects investor interest in engaging in buying and selling activities and can provide an overview of the market's interest level in a company's shares [1]. In this study, the ransomware attack also impacted the transaction volume of BRIS stocks. The analysis of the transaction volume of BRIS stocks was conducted by presenting the daily trading

volume data for 50 days before and after the ransomware attack that occurred in 2023 through the website www.finance.yahoo.com. Graph 4.4 in this study shows the analysis results of the transaction volume of BRIS stocks before and after the ransomware attack.

Graph 4.4 Analysis of BRIS Stock Transaction Volume



| Source: Data processed using MS Excel – 2019, 2025.

In the graph, it shows that before the ransomware attack, the transaction volume of BRIS stocks was relatively stable. Trading activity was driven by long-term investors and speculators taking advantage of the positive price trend of BRIS stocks. Long-term investors tend to consider the company's long-term prospects, including fundamentals, past performance, and future growth potential. On the other hand, speculators exploit stock price fluctuations for short-term gains [3]. Both contributed to the stable transaction volume before the ransomware attack occurred. Meanwhile, the transaction volume of BRIS stocks after the ransomware attacks experienced significant changes, with an increase on the third day post-attack, but a drastic decline the following day. The initial high transaction volume may have been caused by a strong market reaction to the ransomware attack event. Investors reacted quickly to the news by buying and selling stocks, creating a surge in transaction volume. This contrasts with the stock price, which experienced a decline on the third day post-attack; this may occur because the decline in BRIS stock prices could attract investors wanting to buy shares at a lower price, while those wanting to sell were concerned about the future impact of the ransomware attack on BSI.

However, after the following day, the transaction volume of BRIS stocks dropped drastically, possibly due to information about BSI starting to circulate in the market and the impact of the ransomware attack becoming measurable. Investors may have already made decisions to buy, sell, or hold BRIS shares. This was also balanced by the stabilization of BRIS stock prices after the decline occurred the previous day, which could influence transaction volume. Investors may assess that stock prices have reached a fair point and begin to reconsider buying or holding their positions. This could lead to a decrease in trading activity and transaction volume. From Graph 4.2, it is evident that changes in stock transaction volume are influenced by the ransomware attack that occurred in 2023. This is evidenced by the results of the tests on the daily transaction volume of BRIS stocks, using the Wilcoxon Signed Ranks Test, which yielded a significance result of 0.000. Knowing that the significance of 0.000 is less than 0.05 means H2 is accepted and H02 is rejected, this test result proves that there is a significant difference in the transaction volume of BRIS stocks due to the ransomware attack that occurred in 2023.

With the ransomware attack affecting BSI, the company needs to implement preventive measures to ensure such attacks do not happen again, as mentioned in Surah Al-Hasyr verse 18, which relates to the ransomware attack on BSI, emphasizing the importance for the company to always be vigilant and prepare for the future. In the context of ransomware attacks, companies need to be aware of the potential for attacks and take preventive measures to minimize their impact. By protecting their systems and data from these ransomware attacks, companies are responsible for safeguarding their data and assets from such attacks. This can be achieved by implementing strong security systems and educating employees about cybersecurity. If these measures are taken, the company has "considered what it has prepared for tomorrow," which means preparing to anticipate or prevent the adverse effects of ransomware attacks. Strengthening security systems, including regular data backups, ensuring that software and operating systems are always updated to the latest versions, avoiding suspicious links, using strong passwords, limiting access rights for users and appropriate user groups, and activating firewalls and antivirus software on devices [5].

The ransomware attack has prompted BSI to enhance and strengthen its security systems, including the implementation of the latest and most advanced data security systems. This step includes the use of data encryption, firewalls, and intrusion detection systems to protect their infrastructure from cyberattacks. BSI has also conducted regular data security audits to ensure that security systems are always up-to-date and effective in facing evolving threats. These audits help identify potential vulnerabilities and take necessary corrective actions. Additionally, to improve operational security, BSI has implemented a stronger data backup system to ensure that customer data remains safe and can be quickly restored in the event of a ransomware attack or other unforeseen incidents. Employee training is also conducted by BSI to enhance their awareness and capabilities in facing cyberattacks. Employees are trained to recognize signs of cyberattacks, respond

quickly to attacks, and implement appropriate security practices in their daily tasks.

BSI has also maintained transparency and communication with customers regarding the steps taken to enhance security, as well as providing online platforms for customers to obtain information and assistance related to cybersecurity. BSI collaborates with the Financial Services Authority (OJK) and cybersecurity experts to enhance security systems and prevent ransomware or other cyberattacks in the future. This collaboration allows BSI to gain insights and advice from industry experts and strengthen cooperation among parties involved in protecting financial infrastructure from cyberattacks [11]. Through these efforts, BSI has demonstrated its commitment to protecting customer data and maintaining public trust. The steps taken by BSI reflect the company's seriousness in addressing cyber threats and yielding positive results in enhancing BSI's security systems.

METHODS

In this study, the objects of research are the stock prices of BRIS and the transaction volumes of BRIS. This research is quantitative with a comparative research method that compares similarities and differences between two or more characteristics and facts of the objects [13]. This study uses secondary data, namely daily closing stock prices of BRIS and the total shares traded of BRIS each day, within a range of 50 days before and 50 days after the ransomware attack that occurred in 2023. The data were obtained from the websites www.finance.yahoo.com and www.idx.co.id. The data analysis techniques include descriptive statistical analysis, normality tests, and hypothesis testing.

AUTHORS INFORMATION

Corresponding Author

Ahmad Dahlan Malik − Department of Islamic Economics, International University of Semen Indonesia, Gresik, Indonesia;
orcid.orgorcid.org/0000-0003-0067-733X; Phone: 085732126165;
Email: ahmad.malik@uisi.ac.id

Authors

Khoirunnisa− Department of Islamic Economics, International University of Semen Indonesia, Gresik, Indonesia

Wahyu Agung Handono − Department of Islamic Economics, International University of Semen Indonesia, Gresik, Indonesia

Elsi Mersilia Hanesti − Department of Islamic Economics, International University of Semen Indonesia, Gresik, Indonesia

ACKNOWLEDMENT

The completion of this research paper would not have been possible without the support and guidance of Khoirunnisa, Ahmad Dahlan Malik, Wahyu Agung Handono, Elsi Mersilia Hanesti, and International University of Semen Indonesia. Their dedication and overwhelming attitude towards helping is solely responsible for completing this research paper. The encouragement and insightful feedback were instrumental in accomplishing this task.

REFERENCES

[1] Amelia, R.S. (2023). Analisis Perbandingan Return Saham, Harga Saham Dan Volume Perdagangan Saham Bris Sebelum Dan Sesudah Merger. Al-Bay' : Journal of Sharia Economic and Business. Vol. 2, No. 02, hal 181-192.

[2] BSI. (2023). Gandeng FEB UI Perkuat Literasi Keuangan Syariah BSI Targetkan 20 Juta Nasabah Tahun Ini. Diakses dari https://www.bankbsi.co.id/news-update/berita/gandeng-feb-ui-perkuat-literasi-keuangan-syariah-bsi-targetkan-20-juta-nasabah-tahun-ini#:~:text=Per%20Mei%202023%2C%20jumlah%20nasabah,kali%20berdiri%20pada%20tahun%202021.

[3] Finance Detik. (2023). Arti Spekulasi Umum dan Dalam Ekonomi, Contoh Bedanya dengan Investasi. Diakses 10 Februari 2024, dari https://finance.detik.com/bursa-dan-valas/d-6835791/arti-spekulasi-umum-dan-dalam-ekonomi-contoh-bedanya-dengan-investasi

[4] Goodstats.id. (2023). Bank Syariah Paling Banyak Digunakan di Indonesia. Diakses dari https://goodstats.id/infographic/bank-syariah-paling-banyak-digunakan-di-indonesia-ZMcn3.

[5] Hartono, B. (2023). Ransomware: Memahami Ancaman Keamanan Digital. Amartaraya Solusi Utama, Jakarta: Bincang Sains dan Teknologi (BST), Vol.2, No.02, hal 55 – 62.

[6] Hartono, J. (2022). Portofolio Dan Analisis Investasi: Pendekatan Modul (Edisi 2). ANDI Yogyakarta.

[7] IDX Islamic. (2024). Saham Syariah. Diakses dari https://idxislamic.idx.co.id/edukasi-pasar-modal-syariah/saham-syariah/

[8] Indonesia Stock Exchange. (2023). Informasi Umum Saham. Diakses 13 November 2023, dari https://www.idx.co.id/id/produk/saham.

[9] Infobanknews. (2023). Pernah Terkena Serangan Siber Hingga Berhari-hari, BSI Makin Kuat Hadapi Risiko Baru di Era Digitalisasi. Diakses pada tanggal 20 Januari 2024, dari https://infobanknews.com/pernah-terkena-serangan-siber-hingga-berhari-hari-bsi-makin-kuat-hadapi-risiko-baru-di-era-digitalisasi/

[10] Jahja, A.S., & Muhammad, I. (2012). Analisis Perbandingan Kinerja Keuangan Perbankan Syariah dengan Perbankan Konvensional. Institut Perbanas Jakarta: Episteme, Vol. 7, No. 2, hal 337 – 360.
[11] Kontan Keuangan. (2023). Menengok Kasus BSI Dan Masalah Peretasan Di Perbankan. Diakses pada tanggal 10 Februari 2024, dari https://keuangan.kontan.co.id/news/menengok-kasus-bsi-dan-masalah-peretasan-di-perbankan.
[12] Mediaindonesia. (2023). Data Nasabah Bocor, Saham Bank Syariah (BRIS) Langsung Anjlok Sentuh ARB. Diakses dari https://mediaindonesia.com/ekonomi/581729/data-nasabah-bocor-saham-bank-syariah-bris-langsung-anjlok-sentuh-arb
[13] Munzaroh, S.A. & Sa'diyah, M. (2023). Analisis Perbandingan Harga Saham dan Volume Transaksi Pada Perusahaan Telekomunikasi di Jakarta Islamic Indeks. Universitas Islam Nahdlatul Ulama Jepara: Journal of Indonesia Sharia Economics (JIOSE), Vol. 2, No.1, hal 17 – 32.
[14] Tekno Kompas. (2023). Kronologi Layanan BSI Eror Down Berhari – hari dan "Dipalak" Hacker Ransomware Ratusan Miliar. Diakses dari https://tekno.kompas.com/read/2023/05/17/09010077/kronologi-layanan-bsi-eror-down-berhari-hari-dan-dipalak-hacker-ransomware?page=all
[15] Widiarma, I. (2022). Analisis Kinerja Perusahaan dan Transaksi Investor Saham Bank Syariah Pasca Merger Terhadap IHSG. Sekolah Tinggi Ilmu Ekonomi Indonesia Surabaya: Jurnal Al – Ijtimaiyyah, Vol.8, No.1, hal 154 – 174.

AUTHOR CONTRIBUTIONS

The completion of this research paper would not have been possible without the support and guidance of Khoirunnisa as data analyst, Ahmad Dahlan Malik as correspondent author, Wahyu Agung Handono as reviewer, Elsi Mersilia Hanesti as reviewer, and International University of Semen Indonesia. Their dedication and overwhelming attitude towards helping is solely responsible for completing this research paper. The encouragement and insightful feedback were instrumental in accomplishing this task.

COMPETING INTERESTS

Khoirunnisa, Ahmad Dahlan Malik, Wahyu Agung Handono, and Elsi Mersilia Hanesti as finance expertise.

ETHICS STATEMENT

We will uphold high standards of personal conduct and honesty in all of our professional relationships and pursuits. We will treat individuals with whom we work and those we serve with respect and consideration. We shall take appropriate professional care in all aspects of our job. We shall fulfil our professional obligations dependably, keeping an eye on the compliance components of our profession, which are so vital to our service position.