

The effect of cyber attacks on stock performance Bank Syariah Indonesia

Zahra Fatikhatun Nisa, Yuli Tri Cahyono

Accounting Department, Faculty of Economy and Business, Muhammadiyah University of Surakarta

e-mail: b200200518@student.ums.ac.id, ytic115@ums.ac.id

Abstract

This research aims to assess the stock performance of PT Bank Syariah Indonesia (BSI) prior to and during a cyber crime incident targeting its central server on May 8th, 2023. The stock performance of BSI shares on the capital market is forecast based on abnormal returns and trading volume activities. Quantitative research is being conducted using the event study approach. The research sample includes data for BSI shares registered on the capital market under the issuer's code BRIS. Researchers processed and analyzed the data using the Wilcoxon Signed Rank Test, facilitated by the IBM SPSS 25 software. The research findings indicate that the occurrence of the cyber crime event had no impact on the abnormal returns and trading volume activity of BSI shares. Therefore, there was no significant difference in the performance of the two stock variables, both before and after the incident. The event can be used as evaluation material for BSI to keep update and hardening its cyber security system, as well as to ensure transparency of information with investors. Investors can also get some learning to be calm and actively looking for information about the stock and company conditions related to their shares in order to avoid losses when they are facing with similar events.

Keywords: Cyber Crime, Stock Performance, Abnormal Returns, and Trading Volume Activity.

INTRODUCTION

The capital market is an economic tool that is influenced by numerous environmental factors, including both economic and non-economic impacts (Hidayat, 2013). Environmental impacts encompass a range of events that impact the entity in question. These occurrences can provide information for investors, whether they are internal or external to the issuer. Various stakeholders require event data to make lucrative investment decisions.

One of the events that occurred was when there was a cyber crime attack on the PT Bank Syariah Indonesia Tbk (BSI) server on May 8th, 2023. This incident caused BSI to experience disruption to its services. All customers cannot make transactions via ATM or BSI Mobile such as transfers, cash withdrawals, Hajj payments, funding, etc. There is issue of theft of customers and employee data in the BSI storage system and distributed on the dark web by unauthorized parties (www.kompas.tv, 2023). As a result, this causes disappointment, loss of trust, and negative views from customers towards the bank (finance.detik.com, 2023). Sentiment over the data leak influenced BSI share movements. In trading on Tuesday, May 16th, 2023, right after the hacker issued a claim regarding the leak of customer data on the dark web, BSI shares opened at IDR 1,720. However, at 01.00 pm, the shares fell to IDR 1,600, it's down 120 points or -6.98%. This achievement was the lowest during April-May 2023 (finance.yahoo.com, 2023).

This implies that cyber crime attacks have detrimental implications for the general populace. Inaccurate information will have an impact on the conditions of the capital market, particularly the performance of BSI shares. Investors typically regard an unfavorable perception of an occurrence as unfavorable information, resulting in a negative response from the market and a corresponding negative abnormal return (Tandelilin, 2010). Moreover, the trading volume activity provides a clear indication of the performance of BSI shares. Investors utilize stock trading volume to evaluate an announcement as either a positive or negative indication. Therefore, investors regard this factor as crucial when making investment selections in a company.

Hence, researchers are interested in conducting research related to events that occur in a company and their impact on its stock performance. This research is different from previous research which examined old events such as Islamic bank mergers researched by Ariyani and Pratama (2022), the increase in fuel prices researched by Setyawan (2006), the DKI Jakarta regional head election researched by Purba and Handayani (2017), and the Covid-19 disease outbreak was studied by Mulyadi et al (2020). Researchers want to conduct research on an event that is still very recent in 2023, so this research has never been conducted before. Researchers want to study the impact of cyber crime attacks on the abnormal return and trading volume activities of BSI stock. Researchers seek to determine the impact of this cyber crime attack on the performance of BSI shares. Researchers also want to know whether there is a difference in the performance of BSI shares before and after the event occurred.

LITERATURE REVIEW AND HYPOTHESIS DEVELOPMENT

Literature Review

Signalling Theory

Signalling theory describes the company management's view of the company's development regarding matters that can influence the response of investors and potential investors regarding the company (Brigham and Houston, 2006). Signal theory explains the ways in which companies provide signals to users of their financial statements (Tandellin, 2010). This signal consists of information pertaining to the approaches or strategies that firm management will employ to fulfill the expectations of stakeholders. This information is highly significant as it serves as an indicator that might potentially impact investors' decision-making process when selecting companies to invest in. Investors will respond positively to good news as reflected in rising share prices, positive abnormal returns, and actively traded shares and otherwise.

Agency Theory

Agency theory elucidates the dynamic between the principal, who grants a contract, and the agent, who receives the contract. The principal bestows the agent with the autonomy to make decisions that govern the relevant organization (Supriyono, 2018). Agents must possess the capacity to embrace and assume accountability for the future repercussions that accompany their freedom. The agent is accountable to the principal for the repercussions resulting from an event. Hence, it is imperative for agents to consistently generate favorable company performance, ensuring that the information disseminated is positive for the principal and leads to a stable or even enhanced share performance.

Hacking

The internet in general is a small network of computers that form a larger network with a different network structure (Maskun, 2013). This network can later be used as an opening for individuals to hack. Hacking is an activity carried out to gain access to data illegally via digital devices, such as computers, cellphones, tablets, and others (Wijaya and Umara, 2022). Hacking is carried out by individuals or people known as hackers. Hackers have in-depth knowledge of computers, networks, programming, or other hardware so they can damage the cyber security defenses of their target devices. Hacking can happen to many parties. Banking is a sector that is often targeted by hackers to steal customer or employee data, steal financial information, and even take important information hostage to obtain certain rewards.

Cyber Crime

Cybercrime encompasses various illicit activities conducted over computer networks, exploiting the advantages of digital technology (Wahid and Labib, 2010). Illegal cyber activities encompass activities such as breaching websites to disrupt their normal functioning, encountering data breaches and other forms of damages resulting from hacking, as well as engaging in extortion. The catalysts for this

action were the unrestricted nature of the internet network, a vulnerable network security mechanism, and ignorance. The offender may face sanctions and be deemed accountable for their actions.

Abnormal Return

Abnormal return refers to the disparity between the actual return and the expected return (Jogiyanto, 2013). Expected return, also known as normal return, is the anticipated return that needs to be estimated. The realized return, also known as actual return, is the percentage change in price between a specific time period, calculated by subtracting the prior price from the present price and dividing it by the previous price. Investors can achieve exceptional profits by leveraging the knowledge provided in an announcement of a significant event that has the potential to impact the financial market (Jogiyanto, 2003). Cyber crime assaults may lead to variations in abnormal return responses in the stock market for BSI shares. This case presents data that suggests a correlation between positive signals and an increase in stock prices, as well as a correlation between negative signals and a decrease in stock prices.

Trading Volume Activity

Trading volume activity serves as an indicator for observing stock trading activities (Husnan, 2005). Trading volume is a quantitative indicator that represents the total number of shares exchanged during a specific period of time (Jogiyanto, 2010). A high trading volume signifies active and widespread investor interest in the stock. Information possesses instructive value when the occurrence of an event causes a change in the number of shares exchanged as compared to other instances. Announcements pertaining to earnings, dividends, funding, investment, employment, marketing, production, sales, mergers, and other relevant matters concerning an issuer can significantly impact trade volume activities (Foster, 1986). A cyber crime attack refers to an incident where negative opinions from the public are disseminated with the intention of impacting the trading volume of a company's shares.

Capital Market

The capital market serves as a platform for individuals or entities seeking to engage in securities transactions, such as the buying and selling of shares or bonds (Fahmi, 2012). In order to attract investors, it is imperative for the capital market to possess both liquidity and efficiency. A liquid market refers to a situation where the buying and selling of shares and other financial instruments takes place with great speed and efficiency. When the company's share price accurately reflects all relevant information about the company, the market is considered efficient (Tandelilin, 2010). The information can originate from either an economic or non-economic event. Various stakeholders require information from an event announcement in order to make prudent investment decisions that yield profits.

Hypothesis Development

The Effect of Cyber Crime Attacks on Abnormal Returns

Abnormal returns can manifest before the dissemination of information or subsequent to its publication (Samsul, 2015). Investors evaluate the disparity in abnormal returns for an event by comparing the actual return achieved with the projected return. This assessment helps them determine whether the announcement or event provides information that can impact their investment choices. Information indicates the direction of stock prices, whether they will increase or decrease. According to Layyinaturrobbaniyah and Christopher (2019), a good signal leads to an increase in stock prices, while a negative signal results in a decrease in stock prices. Adnyani and Gayatri (2018), Puspita and Yuliari (2019), and Suci (2021) conducted research, which revealed that abnormal returns are influenced by the information sent through events. Consequently, there are discernible disparities in abnormal returns prior to and following the occurrence of such events. Based on that, the following hypothesis can be formulated:

H_1 : Cyber crime attacks have an impact on abnormal stock returns of BSI

H_2 : There is a difference in the abnormal return of shares of BSI before and after the cyber crime attack

The Effect of Cyber Crime Attacks on Trading Volume Activity

Stock trading volume measures the ease of buying or selling a stock. Observing variations in the number of shares being traded on the stock exchange allows investors to gauge their reaction to information (Ariyani and Pratama, 2022). Stock trading volume serves as a standard for analyzing information and assessing the influence of an event. If the share trading volume accurately encompasses all the necessary information for investors, then contrasting it with the average share trading volume activity yields a substantial disparity, which subsequently affects the issuer's share trading volume. Ainurrachma and Mawardi (2022), Suryani and Noviari (2023), and Ernawati et al (2019) conducted research that identified disparities in trade volume activity prior to and following the occurrence of an event. Cyber crime attacks elicit a pessimistic response from investors in the financial sector. If this affects the issuer's shares, there will be a corresponding alteration in the trading volume of its shares. Therefore, the hypothesis that can be formulated are:

H_3 : Cyber crime attacks affect the stock trading volume activity of BSI

H_4 : There is a difference in the trading volume activity of shares of BSI before and after the cyber attack.

The framework of thought in this research can be realized with the following picture:

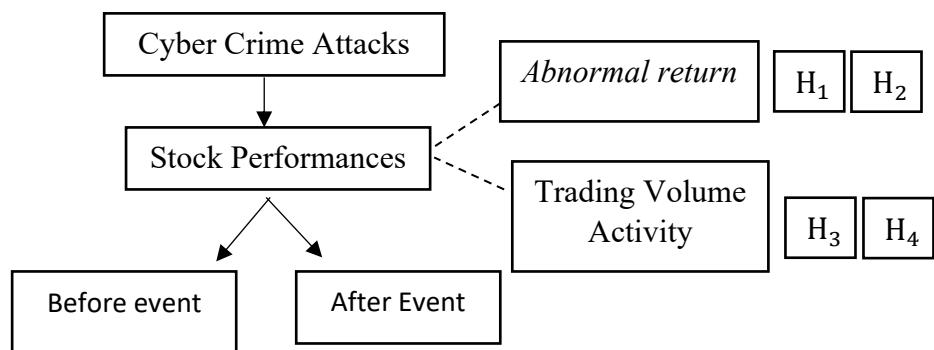


Figure 1. Research model

METHODS

This type of research is quantitative, using the event study method. The research focused on monitoring the performance of BSI shares with the issuer code BRIS in the capital market before and after the cyber crime attacks that occurred on May 8th, 2023. Data collection in the research used documentation methods. The research uses secondary data in the form of BSI stock data sourced from the BSI database (ir.bankbsi.co.id), the Indonesian Stock Exchange (IDX) (www.idx.co.id), and Yahoo Finance (www.finance.yahoo.com). Researchers processed and analyzed the data using the descriptive test and Wilcoxon Signed Rank Test for hypothesis test, facilitated by the IBM SPSS 25 software. The research time period was carried out for 40 days, that is, 20 days before and 20 days after the cyber crime attack occurred. The researchers examined whether the cyber crime attack event affected the performance of BSI shares through abnormal return and share trading volume activity. Then the researchers also wanted to know whether there was a significant difference in stock performance before and after the event occurred.

OPERATIONAL RESEARCH VARIABLES

The operational definitions of the variables used in the research are described as follows:

Cyber Crime

Cyber crime encompasses various illicit activities conducted over computer networks, exploiting the advantages offered by digital technology (Wahid & Labib, 2010). Saputra (2022) provides a comprehensive overview of many cyber crimes, including but not limited to the unauthorized access and compromise of critical data belonging to victims, the infiltration of social media platforms by malicious hackers, and the illicit acquisition of the victim's financial account balance. This study focuses on the cyber crime incident that transpired at BSI on May 8th, 2023, which serves as the variable. The occurrence of this cyber crime resulted in a disruption to the financial services of BSI, as well as the unauthorized disclosure of customer and staff data.

Abnormal Return

According Jogyanto (2013) describes abnormal return as the discrepancy observed between the actual return and the expected or normal return. The normal return, also referred to as the expected return, is the anticipated rate of return that necessitates estimation. The positive return difference arises when the actual return exceeds the projected return. Investors experience negative returns when their realized return falls below their anticipated return. The formula for abnormal returns is (Jogyanto, 2015):

$$AR_{i,t} = R_{i,t} - E[R_{i,t}]$$

Information:

$AR_{i,t}$: abnormal return on security i in event period t

$R_{i,t}$: actual return on security i in event period t

$E[R_{i,t}]$: expected return on security i in event period t

The actual return can be formulated as follows (Jogyanto, 2015):

$$R_{i,t} = \frac{P_{i,t} - P_{i,t-1}}{P_{i,t-1}}$$

Information:

$R_{i,t}$: actual return of stock i in event period t

$P_{i,t}$: stock price on security i in event period t

$P_{i,t-1}$: stock price on security i in event period t-1

Expected return can be calculated using a market-adjusted model, the formula is as follows (Jogyanto, 2015):

$$E[R_{i,t}] = R_{Mt}$$

$$R_{Mt} = \frac{IHSG_t - IHSG_{t-1}}{IHSG_{t-1}}$$

Information:

$E[R_{i,t}]$: expected return of stock i in event period t

R_{Mt} : stock market return in event period t

$IHSG_t$: composite stock price index in event period t

$IHSG_{t-1}$: composite stock price index in event period t-1

Trading Volume Activity

The measure of stock trading volume activity involves the examination of the number of shares traded over a specific period in relation to the total number of shares available for trading in the market. The formula for trading volume activity of a stock is as follows (Jogiyanto, 2015):

$$TVA = \frac{\sum \text{shares of company } i \text{ traded at a certain time}}{\sum \text{shares of company } i \text{ outstanding on the market at a certain time}}$$

Information:

TVA: Trading Volume Activity

RESULTS AND DISCUSSIONS

Descriptive Statistics

The results of descriptive statistical analysis are shown in Table 1.

Table 1. Result of Descriptive Statistics Analysis

Variable	Minimum	Maximum	Mean	Std. Deviation
AR before	-0,03084	0,04988	0,0021120	0,02572878
AR after	-0,06453	0,06313	-0,0008625	0,02857828
TVA before	0,13794	0,82578	0,3143138	0,17916384
TVA after	0,10526	0,92588	0,3359471	0,25325181

Table 1 presents the outcomes of descriptive statistical analyses conducted on the performance of BSI stock over a 40-day research period. The objective was to ascertain the minimum, maximum, mean, and standard deviation values of abnormal returns and trading volume activity prior to and following the occurrence of a cyber crime attack incident. The abnormal returns seen before the event exhibit a minimum value of -0.03084, a maximum value of 0.04988, a mean value of 0.0021120, and a standard deviation of 0.02572878. In comparison to the pre-event period, the abnormal return subsequent to a cyber crime incident exhibits a minimum value of -0.06453, a maximum value of 0.06313, a mean value of -0.0008625, and a standard deviation of 0.02857828. In addition, the trade volume activity preceding the event exhibited a minimum value of 0.13794, a maximum value of 0.82578, a mean value of 0.3143138, and a standard deviation value of 0.17916384. In conclusion, the trade volume activity following a cyber crime attack exhibits a minimum value of 0.10526, a maximum value of 0.92588, a mean value of 0.3359471, and a standard deviation of 0.25325181.

Hypothesis Test

The data in this study is considered not normally distributed because there are less than 30 samples, so a normality test is not needed. The method used to test hypotheses related to abnormal returns and trading volume activity used the Wilcoxon Signed Rank Test. In event study research, this technique is used to compare data before and after treatment. Researchers have conducted this test and the results are shown in Table 2.

Table 2. Result of Wilcoxon Signed Rank Test

Variable	Z	Asymp. Sig(2-tailed)
AR after – AR before	-0,224	0,823

TVA after – TVA before	-0,187	0,852
------------------------	--------	-------

According to the findings presented in Table 2, the statistical analysis reveals that the p-value associated with aberrant returns prior to and following the event is 0.823. When comparing this figure to a probability value of 5% or 0.05, it is observed that the value of Asymp. Sig(2-tailed) is more than 0.05. The findings of this study indicate that the alternative hypotheses (H_1 and H_2) are not supported. The absence of any impact on the irregular returns of BSI shares indicates that the cyber crime attack targeting BSI's core server did not have any discernible effect. Therefore, there is a lack of statistically significant disparity in abnormal returns prior to and following the occurrence of the event. Similar to abnormal returns, the statistical significance of trading volume activity prior to and following a cyber crime attack is determined to be 0.852. The determined probability value is 0.05 or 5%, indicating that the trade volume activity has a two-tailed asymptotic significance value > 0.05 . This shows that in this study H_3 and H_4 were rejected. This means that disruption due to cyber crime attacks does not affect BSI share trading volume activities. Therefore, there is no significant difference in trading volume activity either before or after the event occurred.

Discussions

The Effect of Cyber Crime Attacks on Abnormal Returns

The results of testing the abnormal return variable using the Wilcoxon Signed Rank Test can be seen in table 2. Based on this table, the value of Asymp. Sig(2-tailed) $0.823 > 0.05$, so H_1 and H_2 are rejected in this research. The aforementioned observation indicates that the occurrence of the cyber crime attack event did not have a substantial impact on abnormal returns. Consequently, there was no discernible disparity in abnormal returns on BSI shares both before and after the event. The findings of this study align with prior research conducted by Ariyani and Pratama (2022), Purba and Handayani (2017), and Setyawan (2006), which similarly found no discernible disparities in abnormal returns before or after the occurrence of an event.

Since there haven't been any big changes or differences in BSI stock abnormal returns, it seems that spreading information about cyber crime attacks hasn't been able to cause unexpected changes in stock trading activity outside of normal trading patterns. Multiple variables can exert an influence on the outcomes of this investigation. Investors perceived the cyber crime attack as a significant indicator, but their response was not overly reactionary due to their propensity to address past incidents involving BSI. When an incident transpires, investors tend to prioritize the analysis of BSI's response strategies to mitigate the impact of the attack. Consequently, they exhibit a deliberate approach in their decision-making about the purchase or sale of their shares, resulting in minimal deviations in abnormal returns. Another contributing factor is the limited duration of observation in this particular study, spanning 20 days prior to and 20 days following the occurrence of the cyber crime attack. As a result, researchers did not observe any discernible disparity in abnormal returns. Extending the duration of the observation period could lead to variations in the outcomes acquired.

The results of this research can be a breath of fresh air for the company because its stock performance is still as stable as before the attack and the returns received by investors have not experienced significant changes. However, company also needs to improve their cyber security systems so that this incident does not happen again in the future. The company also needs to provide transparent information on a regular basis to investors to prevent distorted communication and loss of trust in the issuer. Then this incident can also be a lesson for investors to remain calm when they are facing bad company conditions. A calm action accompanied by efforts to continuously monitor share price developments and seek further information regarding BSI's countermeasures allows them to avoid other losses. If investors immediately withdraw their shares, they will only get very little return or even no profit at all. Therefore, it is assumed that shares as a long-term investment must be owned by investors, so that they will not make decisions that could harm themselves in shares investing.

The Effect of Cyber Crime Attacks on Trading Volume Activity

Based on table 2, trading volume activity shows the value of Asymp. Sig(2-tailed) 0.852 > 0.05 of the probability value, so that H_3 and H_4 are rejected. The findings indicate that the occurrence of cyber crime assaults did not have a substantial impact on the level of stock trading volume activity. Consequently, there was no discernible disparity in trading volume activity on BSI shares, both prior to and subsequent to the incident. Ariyani and Pratama (2022), Purba and Handayani (2017), Suci (2021), and Setyawan (2006), had already found similar results: there is no clear difference in the amount of stock trading activity before and after an event. This study adds to those findings. Cyber crime attack incidents do not impact trading volume activity, indicating that investors' decision-making process and subsequent reactions to their investment choices remain unaffected by the information disseminated through these events.

The implementation of this measure serves to mitigate the occurrence of panic buying or panic selling, hence exerting an influence on the volume of shares exchanged among investors. One additional aspect that exerted influence on the outcomes of this research was the prompt response of BSI in addressing the attack, which therefore fostered sustained investor confidence in their respective investments. Hence, investors perceive this occurrence as having a neutral impact, devoid of positive or negative implications. The observed trade volume activity does not exhibit a reaction to external influences, therefore indicating that this variable continues to fluctuate. Moreover, there is no statistically significant disparity between the periods before and after the occurrence of the event. BSI's quick response to dealing with the main server disruption should be appreciated because this can prevent major losses, customer and employee data can be recovered and saved from unauthorized parties.

If the company continues to quickly resolve bank system malfunctions, reinforce its cyber security, improve its banking performance, and does not increase its share price, then its share trading volume could stabilize or even increase. This can happen because investors increasingly believe in BSI's performance, so they prefer to continue investing in the issuer. Furthermore, the neutral action shown by investors in responding to this incident also deserves appreciation. They remain calm and are in no rush to withdraw or sell the shares they own. It means that investors will continue to hold the BSI shares they own. Panic selling when an attack occurs can also bring more losses to investors. Investors must also filter the issuer's information regarding share conditions and the mitigation steps taken by the company periodically so as not to be trapped by fake news. Therefore, every investor must have an action of calm, patience, and actively seeking information when they facing with the same event.

CONCLUSIONS

Based on the results of research, it can be concluded that the cyber crime attacks that occurred at PT Bank Syariah Indonesia, Tbk did not affect and caused a significant disparity to the performance of its shares. It means that the cyber crime attack event did not make a significant difference to BSI share abnormal return and trading volume activity either before or after the incident occurred. The research undertaken by Ariyani and Pratama (2022), Setyawan (2006), Purba and Handayani (2017) aligns with the findings of this study, indicating no discernible disparities in abnormal returns and trading volume activity prior to or following the occurrence of an event.

This event can be a lesson for BSI to evaluate their performance, which are that they can always update and hardening their cyber security system periodically, quick act to handle all of the malfunctioning bank systems that can happen later, make company information transparent to investors and the general public, and improve banking performance. Investors remain confident of the capital they have planted or even choose to buy more BSI shares after seeing the quick response BSI has made to counter this cyber crime attack. Therefore, BSI's stock performance remained stable as before the event occurred. Then for investors, this event can also be used as a lesson to always be calm and active in seeking information regarding the company and the condition of its shares from

trusted sources. Being trapped by fake news means that investors will make the wrong investment decisions if they encounter similar events.

This study is subject to various constraints, as it solely relies on two factors, namely abnormal returns and stock trading volume activity, to depict stock performance in the capital market. This research also used only cyber-crime attacks as a benchmark for assessing the variables that impact stock performance inside the capital market. This research is deficient in its ability to elucidate the elements that can exert an influence on stock performance, as well as the variables that provide a comprehensive description of stock performance. The duration of the research period was rather brief, spanning only 40 days. Consequently, there is no H_a was accepted in this study. Hence, in order to further research, it is advisable to select events of greater significance in shaping financial circumstances or impacting stock performance within the capital market. Additionally, incorporating factors that effectively depict stock performance and extending the duration of the research period would be beneficial.

REFERENCES

- Adnyani, I. P. and Gayatri. (2018). Analisis Reaksi Pasar Terhadap Pengumuman Akuisisi Pada Perusahaan Akuisitor Yang Terdaftar di BEI. *E-Jurnal akuntansi Universitas Udayana*. Vol. 23 (3): 1870-1899.
- Ainurrachma, M. and Mawardi, I. (2022). Reaksi Pasar Saham terhadap Merger Bank Syariah Milik Negara. *Jurnal Ekonomi Syariah Teori dan Terapan*. Vol. 9(1): 92-105.
- Ariyani, D. A., dan Pratama, V.Y. 2022. "Reaksi Pasar Atas Peristiwa Merger Bank Syariah BUMN (Studi Peristiwa BRI Syariah)". *Journal of Sharia Finance and Banking*. Vol. 2(2).
- Brigham, E.F., and Houston, J.F. (2006). *Financial management*. Edition 8. Jakarta: Erlangga.
- Ernawati et al. (2019). Studi Komparatif : Reaksi Pasar Modal Dan Pasar Modal Syariah Terhadap Kemenangan Jokowi 2019 (Jokowi's Effect). *Jurnal Manajemen Dan Bisnis*. Vol. 2(2): 8-16.
- Fahmi, I. (2012). *Analisis Kinerja Keuangan*. Bandung: Alfabeta.
- finance.detik.com.
- finance.yahoo.com.
- Foster, George. (1986). *Financial Statement Analysis*. Second Edition. Singapore: Prentice-hall.
- Hidayat, A. S. (2013). "Reaksi Pasar Modal Indonesia Terhadap Kenaikan Harga Bahan Bakar Minyak (BBM) 22 Juni 2013 (Studi Peristiwa pada Perusahaan yang Terdaftar di Indeks LQ-45, Perusahaan Sektor Manufaktur dan Perusahaan Sektor Pertambangan)". *Skripsi Universitas Gadjah Mada*.
- Husnan, Suad. (2005). *Dasar-Dasar Teori Portofolio dan Analisis Sekuritas*. Edisi keempat. Yogyakarta: UPP AMP YKPN.
- ir.bankbsi.co.id.
- <https://news.republika.co.id>.
- <https://www.idx.co.id>.
- Jogiyanto, H. (2003). *Teori Portofolio dan Analisis Investasi*. Edisi 5. Yogyakarta:BPFE.
- Jogiyanto, H. (2010). *Teori Portofolio dan Analisis Investasi*. Edisi 7. Yogyakarta:BPFE.
- Jogiyanto, Hartono. (2013). *Teori Portofolio dan Analisis Investasi*. Edisi 8. Yogyakarta: BPFE.
- Jogiyanto, Hartono. (2015). *Teori Portofolio dan Analisis Investasi*. Edisi 10. Yogyakarta: BPPE.
- Layyinaturrobbaniyah, and Christopher, D. (2019). Indonesian Capital Market Reactions for the Election of Donald Trump As United States President (Empirical Study on Multinational

- Companies Listed on the Indonesia Stock Exchange). *Journal of Management and Business.*18(1):32–41.
- Maskun. (2013). *Kejahatan Siber Cyber Crime*. Jakarta: Kencana.
- Mulyadi et al. (2020). Analisis Kinerja Saham LQ45 Sebelum Dan Selama Pandemi *Coronavirus Disease* (Covid-19) Di Indonesia. *Jurnal Interprof.* Vol. 6(2): 156-167
- Purba, F., dan Handayani, S.R. (2017). “Analisis Perbedaan Reaksi Pasar Modal Indonesia Sebelum Dan Sesudah Peristiwa Non Ekonomi (Studi pada Peristiwa Politik Pilkada DKI Jakarta 2017 Putaran Kedua”}. *Journal Administrasi Bisnis*. Vol. 51(1).
- Puspita, N. V. and Yuliari, K. (2019). Analisis Pengaruh Stock Split Terhadap Harga Saham, Abnormal Return Dan Risiko Sistematik Saham Perusahaan (Studi Pada Perusahaan Yang Terdaftar Di Bei 2016-2018). *Jurnal Ekonika : Jurnal Ekonomi Universitas Kadiri*. Vol 4(1): 95-110.
- Saputra, S. (2022). Analisis Pembuktian Hukum Perkara Tindak Pidana Penggelapan Melalui Elektronik Sistem (Studi Perkara Nomor 118/Pid. B/2021/PN Cbn) . Universitas Islam Sultan Agung .
- Setyawan, S. T. A. (2006). Analisis Reaksi Pasar Modal Terhadap Kenaikan Harga BBM. Skripsi: Universitas Diponegoro, Semarang.
- Samsul, Muhammad. (2015). *Pasar Modal dan Manajemen Portofolio*. Edisi 2. Jakarta: Erlangga.
- Suci, M. P. (2021). “Analisis Reaksi Pasar Modal Terhadap Peristiwa Merger Bank Syariah (event study pada saham bank BRI Syariah)”. *Jurnal ekonomi, Manajemen, Bisnis, dan Sosial (EMBISS)*. 1(4).
- Supriyono, R.A. (2018). *Akuntansi Keperilakuan*. Yogyakarta: UGM Press.
- Suryani, N. M. A. M., & Noviari, N. (2023). Reaksi Pasar Modal terhadap Pengumuman Kebijakan Incentif Pajak Penjualan atas Barang Mewah. E-Jurnal Akuntansi, 33(2), 302-310
- Tandelilin, E. (2010). *Portfolio and Investment*. Yogyakarta: Kanisius.
- Wahid, A., dan Labib, M. (2010). *Kejahatan Mayantara*. Bandung: Refika Aditama.
- Wijaya, T. H. D. dan Umara, N. S. (2022). "Penerapan sanksi sosial sebagai alternatif pemidanaan terhadap pelaku tindak pidana kejahatan siber (cyber crime)". *Al-Qisth Law Review*, 5 No. 2 : 371-404.
- www.kompas.tv.