:: IJEBD ::
(International Journal of Entrepreneurship and Business Development)
Volume 07 Number 05 September 2024

ISSN : 2597-4785 (ONLINE)
ISSN : 2597-4750 (PRINTED)

Cyber Risk Management Disclosure: The Impact of Firm Size, Profitability, and Intangible Asset

Mira Sofiani[1], Diani Putri Ramadhanty[1], Siti Jubaedah[2]
Accounting Study Program, Faculty of Economics and Business, Swadaya Gunung Jati University, Cirebon, Indonesia[1]
Department of Accounting, Swadaya Gunung Jati University, Cirebon, Indonesia[2]
Corresponding Author: mira.sofianii@gmail.com, dianip467@gmail.com, siti.jubaedah@ugj.ac.id

ABSTRACT

Purpose: This research aims to determine the impact of firm size, profitability, and intangible assets on cyber risk management disclosure.

Design/methodology/approach: This research is a causality study with quantitative methods and uses secondary data derived from annual reports of telecommunications and financial services sector companies listed on the Indonesia Stock Exchange in 2018-2022. The sampling technique used purposive sampling and obtained 150 annual reports which were analyzed using multiple linear regression**.**

Findings: The results showed that company size and profitability have a positive and significant influence on Cyber Risk Management Disclosure, but Intangible Assets are not significant.

Practical implications: According to the research outcomes, it is suggested for the development of government policies and regulations that encourage companies to increase cyber risk management disclosures in annual reports, as well as companies can understand the factors that influence cyber risk management disclosures so that companies can increase transparency and reduce cyber risk, besides that it can help investors make wiser investment decisions by having an understanding of cyber risk management faced by companies**.**

Originality/value: This research contributes to the development of an accounting conceptual framework on the concept of disclosure, especially voluntary disclosure and practical contributions for governments, companies, and investors**.**

Paper type: Research paper

Keyword: *Cyber Risk Management Disclosure, Firm Size, Intangible Asset and Profitability*
Received : May 13th
Revised : August 18th
Published : September 30th

I. INTRODUCTION

The use of technology in various areas of life has been triggered by the Covid-19 pandemic (McKinsey & Company, 2020). Digital technology has affected almost every economic sector in the world, most global companies allocate most of their financial resources for the implementation of digital transformation initiatives (Kunjana, 2017). Awareness of protecting digital assets is an important concern for companies because cyber attacks can affect company performance and reputation (Kelrey & Muzaki, 2019). Intentional or unintentional cyber events can result in the loss of confidentiality, availability, and integrity of digital information. Increasing IT security costs cannot significantly reduce cyber threats. The weakest point of cyber threats lies in people. The human tendency to be careless, hasty, disinformation, and vulnerable to *phishing* attacks. The above conditions have given rise to a new field of study whose focus is cyber risk. Cyber risk is a multidisciplinary topic that has recently received scientific attention due to its diversity and the rapid development of cyber security and cyber threats. Cyber risk is defined by combining two factors: technological and financial (Strupczewski, 2021).

ISSN : 2597-4785 (ONLINE)
ISSN : 2597-4750 (PRINTED)

The cyber attack case in the form of *ransomware* that hit PT Bank Syariah Indonesia Tbk. on May 8-11, 2023 made banking services unusable. Inaccessible services include direct services at branch offices, automated teller machines (ATMs), and *mobile banking* services (Afifah, 2023). According to a survey conducted by Kaspersky (2019), Indonesia ranked second in the top with 192,591 cases of cyberattacks in Southeast Asia during the Covid-19 pandemic (CNN, 2020). Cyberattacks do not only attack Indonesia. According to an EMC report in 2013, cyberattacks caused global financial losses of $5.9 billion or around 80 trillion rupiah (Radiansyah, 2016).

Cyber attacks have an indirect impact on stock prices and company performance (Solikhawati & Samsuri, 2023). Making voluntary disclosures is one way that can be used to reduce company risk. In this way, the quality of the company's financial statements will be better because the information submitted includes information about the company's risks and finances (Sulistyaningsih & Gunawan, 2018). Risk disclosure is a way for companies to communicate to users of annual reports about things that can threaten the company. However, risk management disclosure is still done voluntarily (Wijanarko & Rosita, 2023). Risk management is considered very important to implement because of the many risk threats received by the company (Suwaldiman & Fajrina, 2022). Disclosure of risk management in the annual report is used as a reference for consideration by investors when making investment decisions, this shows how important information transparency is in the company's annual report (Sarwono, *et al*., 2018). Therefore, disclosure of cyber risk management is important because the information has a value that can make the market react. In addition, cyber risk disclosure can be one of the tools to build a positive image of the company that will increase company profits (Jubaedah & Setiawan, 2023). However, the level of cyber risk disclosure in Indonesia is still low. And scientific articles that define cyber risk are not easy to find (Strupczewski, 2021). This makes this research relevant and important to do.

This research uses independent variables of firm size, profitability, and intangible assets. Research on risk management disclosure has been conducted by previous researchers and obtained different results. Research conducted by Sarwono & Hapsari, *et al* (2018) shows that company size has a significant positive effect on risk management disclosure, while profitability has no effect on risk management disclosure. Research by Wahyuni & Nurbaiti, *et al* (2020) shows that company size has an effect on risk management disclosure. And Sudharto & Salim's research (2021) reveals that company size has a positive and insignificant effect on disclosure risk, while profitability has a positive and significant effect on disclosure risk. To the best of the researchers' knowledge, previous research that discusses intangible assets on risk management disclosure is still difficult to find.

The research mentioned above are all related to risk management disclosure however, none have disclosed more company-specific cyber risk management information. Research conducted by Sari, *et al* (2023) has compiled a cyber risk management disclosure index. This index is used to provide an overview of the disclosures expected by stakeholders in the annual report. The results of the research resulted in the composition of a cyber risk management disclosure index of 16 (sixteen) items with a weight on each disclosure item. The index compiled by Sari, *et al* (2023) is used as a reference in this research. This research is a form of development from the research of Sari, *et al* (2023) by using signaling theory and adding variables of firm size, profitability, and intangible assets. This research will focus on the telecommunications and financial services sectors listed on the Indonesia Stock Exchange (IDX) in 2018-2022 as research objects. And aims to analyze how the influence of firm size, profitability, and intangible assets on cyber risk management disclosure.

This research contributes theoretically to the development of the accounting conceptual framework on the concept of disclosure, especially voluntary disclosure. The results of this research are expected to make a practical contribution to the government, companies, and investors. The results of this research can be used as a basis for developing government policies and regulations that encourage companies to increase cyber risk management disclosures in annual reports. The results of this research can help companies to understand the factors that influence cyber risk management disclosure, so that companies can increase transparency and reduce cyber risk. And investors can utilize the results of this research to make wiser investment decisions by having an understanding of the cyber risk management faced by the company.

A. Literature Review

In solving research problems and formulating hypotheses, the theoretical basis used by this research is signal theory. Ross (1977) developed signal theory to explain the motivation of companies to convey financial statement information to external parties, such as investors or shareholders. This theory assumes an information imbalance between company management who knows the company's condition and prospects better than external parties who have less or inaccurate information. The presentation of positive or interesting information can send signals or clues that the company has a high value or performance, so that it can increase stock prices or investment interest. Meanwhile, the presentation of negative or less attractive information can send signals or clues that the company has low value or performance, so that it can reduce stock prices or investment interest. Signal Theory states that companies that voluntarily provide a lot of information try to minimize information imbalances by conveying their effectiveness and real conditions through the provision of additional data to uninformed parties.

ISSN : 2597-4785 (ONLINE)
ISSN : 2597-4750 (PRINTED)

This shows that even high-performing entities utilize detailed information as a tool to signal to the market, in accordance with the findings revealed by (Arena *et al*, 2020), and (Gaol & Harjanto, 2019).

Disclosure is the presentation of information with sufficient explanation and can show the credibility of a company. The information presented must be clear, accurate, and reliable to describe the company's condition, both financial and non-financial. There are two types of disclosure according to the stipulated provisions, namely mandatory disclosure and voluntary disclosure. Mandatory disclosure is the minimum disclosure required by authorized institutions. Voluntary disclosure is a disclosure made by the company voluntarily without being required by an authorized institution (Neliana, 2018). According to Suwardjono (2014), signaling theory underlies voluntary disclosure. Signaling theory provides information signals needed by investors to consider and decide on their choices in investing in a company. According to this theory, management always tries to disclose private information that will be favored by investors and shareholders. A high level of voluntary disclosure will provide the best information, and users of financial statements need this information for decision making (Astuti, *et al*, 2021).

In every business, facing risks is inevitable. Risk is a condition that is uncertain, can bring losses, and is often encountered in various business activities. A company's financial statements usually include a special section describing the various risks faced by the company. This is known as risk disclosure. Although there are no sanctions for companies that do not disclose all existing risks, this disclosure remains a highly recommended practice (Sudharto & Salim, 2021). Risk management disclosure is one of the voluntary disclosures provided by companies in annual reports. Risk management disclosures made by companies can give investors more confidence in the company because with this, investors understand the extent to which the company is able to manage the risks they are facing or will face (Suwaldiman & Fajrina, 2022). Cybersecurity has become a new dimension in risk management (Li *et al*., 2018). The measurement of cyber risk management disclosure refers to an index designed to assess the transparency and effectiveness of companies in managing cyber risks. This index usually consists of a series of indicators that measure various aspects of cyber risk management, such as risk identification and assessment, risk control and mitigation, and monitoring and reporting (Briliyant & Ashari, 2018). This indicator can be used by companies to measure their ability to manage cyber risk thoroughly, providing a better understanding of the level of readiness and responsibility related to cybersecurity. This indicator can also be used as a basis for improvement and development of more effective strategies in facing cybersecurity challenges. The measurement of cyber risk management disclosure in this study refers to the index compiled by Sari, Suhardjanto, Probohudono *et al* (2023) with sixteen disclosure items.

B. Hypothesis Development

1. The Effect of Firm Size on Cyber Risk Management Disclosure

Firm size is an important factor in determining how detailed risks are disclosed, according to various previous studies. This size, often referred to as 'firm size', is a measure that indicates how big or small a company is. There are various methods to measure firm size, such as total assets or total employees. Depending on the size, companies can be categorized as small, medium, or large companies (Sudharto & Salim, 2021). Large company sizes have optimal supervision, this makes companies disclose more risk management (Wahyuni & Nurbaiti et al, 2020). This study shows that the larger the company size, the more likely it is to disclose cyber risk management. This research is supported by Wahyuni et al. (2020), Sudharto & Salim (2021) which show that company size has a significant positive effect on risk management disclosure.

H1: Firm size has a positive and significant influence on cyber risk management disclosure.

2. The Effect of Profitability on Cyber Risk Management Disclosure

Profitability is a measure of the company's success in generating profits from its total operating costs. This is a benchmark for parties inside and outside the company to evaluate how effective the company is in generating profits and managing its resources. The level of profitability of a company can show the company's ability to manage its resources (Sudharto & Salim, 2021). The company's high level of profitability will encourage managers to provide more detailed information, because the company wants to convince investors of the profitability generated and encourage management compensation. This positive and more detailed information encourages management to make voluntary disclosures by providing additional information in the annual report disclosure (Neliana, 2018). Information in voluntary disclosure can be used by investors to assess the company's performance in generating profits. So that the higher the level of company profitability, the more likely it is to disclose cyber risk management. When companies have high profits, they are more free to disclose cyber risk management, because disclosure requires high costs, so companies that have high profits will be more able to allocate additional resources to strengthen their information security systems. The profitability ratio used in this study is Return on Asset (ROA), which is the ratio of net profit after tax to total assets. Previous research has different results, research conducted by Sarwono & Hapsari, et al (2018) shows that profitability has no effect on

ISSN : 2597-4785 (ONLINE)
ISSN : 2597-4750 (PRINTED)

risk management disclosure. Meanwhile, research by Sudharto & Salim (2021) revealed that profitability has a positive and significant effect on risk disclosure.

H2: Profitability has a positive and significant influence on cyber risk management disclosure.

3. The Effect of Intangible Assets on Cyber Risk Management Disclosure

PSAK 19 (Revised 2018) defines intangible assets as assets that are formless, and can be identified without a physical form but, can be distinguished from other assets. Intangible assets also cannot be measured in money. PSAK 19 regulates how companies value their intangible assets. There are three ways companies can acquire intangible assets: (1) Buying from others. (2) Combining business with other companies. (3) Creating your own. (IAI 2018). Intangible assets are the center of information gaps that arise from uncertain economic activities and forward-looking company activities (Rosdini, 2016). Intangible assets are included in the category of non-current and intangible assets that provide economic and legal rights to their owners, such as intellectual copyrights, patents, franchises, and trademarks (Ramadhan et al, 2018). According to Warren et al. (2018), intangible assets owned by a company can be very diverse, depending on the sector in which the company operates. Examples of intangible assets that can be owned by a company include franchises, databases, patents, licenses, trademarks, customer relationships, and so on. For technology-based companies that have better intangible assets, disclosing intangible asset information informatively can increase positive appreciation from stakeholders in assessing management performance, which has a positive impact on market value and the continuity of the company's business relationships (Muyasaroh, 2020). Companies that have intangible assets tend to disclose information about the risks they face, including cyber risk management. To the best of the researchers knowledge, previous research that discusses intangible assets on risk management disclosure is still difficult to find.

H3: Intangible assets have a positive and significant influence on cyber risk management disclosure.

II. METHODS

This research is a causality study with quantitative methods and uses secondary data sourced from annual reports of telecommunications and financial services sector companies listed on the Indonesia Stock Exchange in 2018-2022. The sampling technique using purposive sampling obtained 150 annual reports which were analyzed using multiple linear regression**.**

The data source in this research is secondary data and is obtained from the IDX website, namely (www.idx.co.id) and the official website of each company if the annual report is not attached to the IDX website. Then, the data will be processed using SPSS (Statistical Package for the Social Sciences) software version 25.

The following table contains the operationalization of all variables used in this research. Cyber risk management disclosure is the dependent variable used in this research. The independent variables used in this research are firm size, profitability, and intangible assets.

Table 1 Variable Operationalization

Variable	*Description*	*Measurement*
Cyber Risk Management Disclosure (CRMD)	*The extent of information disclosure regarding cyber risk carried out by the company.*	*Using an indicator of 16 cyber risk items measured using a dummy score, where 1 for companies that disclose, 0 if not. (Sari, Suhardjanto, Probohudono. et al, 2023)*
Firm Size (SIZE)	*The company size scale is seen from the size of the company's total assets.*	*Ln = (Total Assets)* *(Hapsari & Prasetyo, 2020)*
Profitability (PROF)	*A scale that measures the amount of profitability generated by the company.*	$PROF = \frac{Net\ Income}{Total\ Assets}$ *(Hapsari & Prasetyo, 2020)*

ISSN : 2597-4785 (ONLINE)
ISSN : 2597-4750 (PRINTED)

Intangible Assets (INTA)	*Scale that measures the amount of intangible assets owned by the company*	*Intangible Assets = Acquisition value - Depreciation* *(David, Codwel, et al, 2017)*

The linear regression equation used in this research is.

$CRMD = \alpha + \beta_1 SIZE + \beta_2 PROF + \beta_3 INTA + e$

Where CRMD is the Cyber Risk Management Disclosure, SIZE is the Firm Size, PROF is the Profitability, INTA is the Intangible Assets, and e is an error term.

III. RESULTS AND DISCUSSION

A. Results

1. Descriptive Statistic

Based on the results of descriptive statistics in this study, it can be concluded as follows:

Table 2 Descriptive Statistic

Variable	*N*	*Minimum*	*Maximum*	*Mean*	*Std. Dev*
SIZE	*150*	*22.6867*	*35.2282*	*30.768707*	*2.3341288*
PROF	*150*	*.0006*	*38.6026*	*.742863*	*4.5676177*
INTA	*150*	*.0001*	*.2110*	*.0088780*	*.0252120*
CRMD	*150*	*3*	*15*	*9.72*	*3.2208840*

Notes: CRMD = cyber risk management disclosure, SIZE = firm size, PROF = profitability, INTA = intangible assets.
Source: Authors own processed

The first independent variable is firm size. Based on the results of descriptive statistics in table 2, it shows that the average value is 30.76. The lowest value is 22.68 owned by Clipan Finance Indonesia Tbk in 2021, while the highest value is 35.22 owned by PT Bank Mandiri (Persero) Tbk in 2022.

The next independent variable is profitability, based on financial statement data issued by the IDX, it shows that the average level of ROA of telecommunications and financial services companies for the 2018-2022 period is 0.74. The lowest value is at 0.0006 owned by PT Bank Ganesha Tbk in 2020, while the highest value is at 38.60 owned by Clipan Finance Indonesia Tbk in 2022.

The next independent variable is intangible assets. Based on the results of descriptive statistical analysis in table 2, it shows that the average value is 0.0088. The lowest value is at 0.0001 owned by PT Indoritel Makmur Internasional Tbk in 2020, while the highest value is at 0.21 owned by Asuransi Multi Artha Guna Tbk in 2018.

The dependent variable in this study is cyber risk management disclosure. Based on descriptive statistics, it shows that the average value is 9.72. The lowest value is at 3 owned by Paninvest Tbk, while the highest value is at 15 owned by PT Telkom Indonesia (Persero) Tbk.

2. Classical Assumption Test

Based on the test results, it is found that all classical assumptions have been met. The normality test shows a significance of 0.389 <0.05, indicating that the data distribution is normal and in accordance with the assumption of normality. This confirms that the research data meets the necessary normality criteria. Furthermore, the heteroscedasticity test results show that the significance value of each variable exceeds 0.05, indicating no heteroscedasticity in the regression equation, so the regression model can be considered for prediction purposes. In addition, the Variance Inflation Factor (VIF) test showed values less than 10 for all independent variables, which means there is no indication of multicollinearity among the independent variables. The autocorrelation test results yielded a Durbin Watson value of 1.919, which meets the criteria of dU < dW < 4-du, there is no

ISSN : 2597-4785 (ONLINE)
ISSN : 2597-4750 (PRINTED)

autocorrelation in the data. Thus, it can be concluded that the basic assumptions of this regression model are well met.

3. Multiple Linear Regression

The results of multiple linear regression using SPSS assistance, obtained the results as in table 3. The regression results in table 3 show that the form of the relationship between the dependent variable and the independent variables can be described in the multiple regression equation as follows:

$$CRMD = \alpha + \beta_1 SIZE + \beta_2 PROF + \beta_3 INTA + e$$
$$= -8.200 + 0.576 SIZE + 0.236 PROF + 9.479 INTA + e$$

Table 3 Multiple Linear Regression

Variable	*Unstandardized B*	*Std. Error*	*Standardized Coefficients Beta*	*t-Statistic*	*Sig.*
constant	*-8,200*	*3,833*		*-2,139*	*,034*
SIZE	*,576*	*,123*	*,417*	*4,665*	*,000*
PROF	*,236*	*,063*	*,334*	*3,735*	*,000*
INTA	*9.479*	*9,784*	*,074*	*,969*	*,334*

Notes: CRMD = cyber risk management disclosure, SIZE = firm size, PROF = profitability, INTA = intangible assets.
Source: Authors own processed

4. Model analysis

From the results of the analysis it is known that the Adjusted R Square value is 12.8%, then the independent variable consists of Company Size (X1), Profitability (X2), Intangible Assets (X3), which means that the ability to explain the variation in the dependent variable is very limited, namely only 12.8%. While the remaining 87.2% is explained by other variables outside the research variables. Each independent variable is able to explain an average of 4.27% for each variable, which is a pretty good value because the actual independent variables are very many and varied. Based on the results of the F statistical test, with a significance value for equation 1 of 0.00, which shows a value much smaller than 0.05, it can be concluded that the research model has a significant fit or this model is suitable for further research.

Table 4 Hypothesis Testing Results

Variable	*Coefficient*	*Prob a=0.5*
CRMD	*-8,200*	*0,034*
SIZE	*0,576*	*0,000*
PROF	*0,236*	*0,000*
INTA	*9,479*	*0,334*
Adjusted R Square	*0,145*	
F- Statistic	*8,280*	
Prob (F-statistic)	*0,000*	

ISSN : 2597-4785 (ONLINE)
ISSN : 2597-4750 (PRINTED)

N	*150*

Notes: indicates significance level at 5%, CRMD = cyber risk management disclosure, SIZE = firm size, PROF = profitability, INTA = intangible assets.
Source: Authors own processed

B. Discussion

In this subchapter, the results of the hypothesis testing that has been carried out are explained. The discussion of this research hypothesis will be explained as follows:

1. The Effect of Firm Size on Cyber Risk Management Disclosure

Table 4 variables show that Firm Size (X1) has a coefficient of 0.576 and a significance value of 0.000. Based on the coefficient value and significance above, it can be concluded that firm size has a significant positive effect on Cyber Risk Management Disclosure and H0 is rejected.

The rejection of H0 indicates that companies with large assets tend to face greater risks as their asset value grows. This phenomenon is based on the fact that the larger the company, the more complex its corporate governance. As a result, large companies tend to have more information related to corporate governance and operations. With more information available, especially related to cyber risk management, large companies have a greater responsibility to disclose such information to stakeholders. Therefore, it can be concluded that firm size has a significant impact on the level of cyber risk management disclosure made by the company. The results of this research are in line with Wahyuni *et al.* (2020), Sudharto & Salim (2021) which state that firm size has a positive effect on risk management disclosure.

2. The Effect of Profitability on Cyber Risk Management Disclosure

Table 4 variables shows that Profitability (X2) has a coefficient of 0.236 and a significance value of 0.000. Based on the coefficient value and significance above, it can be concluded that profitability has a significant positive effect on Cyber Risk Management Disclosure and H0 is rejected.

The rejection of H0 indicates that companies with high profits will disclose more cyber risk management, while companies with low profits will disclose less. When companies have high profits, they are more free to make cyber risk management disclosures, because disclosure requires high costs, so companies that have high profits will be more able to allocate additional resources to strengthen their information security systems. This can increase customer and investor confidence in the company, which can have a positive impact on the company's overall reputation and performance. However, low-profit companies may find it difficult to allocate additional resources for cyber management, so they are likely to have lower disclosure levels. Therefore, it is important for low-profit companies to prioritize investment in information security to protect their data and reputation. The results of this research are in line with Sudharto & Salim (2012) but different from Sarwono & Hapsari, *et al* (2018) which state that profitability has no effect on risk management disclosure.

3. The Effect of Intangible Assets on Cyber Risk Management Disclosure

Table 4 shows that the Intangible Asset variable (X3) has a coefficient of 9.479 and has a significance value of 0.334. Based on the coefficient value and significance, it can be concluded that there is a negative relationship between intangible assets and the level of cyber risk management disclosure. However, this research found that the coefficient value shows a negative trend, although the initial hypothesis shows a positive direction. Therefore, based on these results, there is not enough evidence to reject the null hypothesis (H0).

The acceptance of H0 indicates that there is not enough evidence to reject the null hypothesis that there is no influence between intangible assets and the level of cyber risk management disclosure. So in this context, there is not enough reason to believe that intangible assets, such as technology or copyrights, significantly affect the level of cyber risk management disclosure in companies. Based on the results of the analysis conducted, it can be concluded that the intangible assets in question have no impact on cyber risk management disclosure. To the best of the researchers' knowledge, previous studies that discuss intangible assets on risk management disclosure are still difficult to find. Therefore, it is necessary to conduct further research with more in-depth methods and using a larger sample to test the relationship between the two variables. This further research will help in providing a more complete understanding of the role of intangible assets in cyber risk management disclosure in the corporate context.

ISSN : 2597-4785 (ONLINE)
ISSN : 2597-4750 (PRINTED)

IV. CONCLUSION

This research examines the effect of firm size, profitability and intangible assets on cyber risk management disclosure. Based on the research results it can be concluded that: (1) Hypothesis testing results show that Firm Size affects Cyber Risk Management Disclosure. This is possible because companies with larger sizes tend to have more resources and capacity to manage risks, including cyber risks. (2) The results of hypothesis testing show that Profitability affects Cyber Risk Management Disclosure. This is possible because the level of profitability of companies can affect their priorities and management strategies related to cyber risk. (3) The results of hypothesis testing show that Intangible Assets have no effect on Cyber Risk Management Disclosure. This is because intangible assets have not been able to pressure companies to disclose more information in terms of risk management.

This research contributes to the development of an accounting conceptual framework on the concept of disclosure, especially voluntary disclosure and practical contributions for governments, companies, and investors. As a basis for the development of government policies and regulations that encourage companies to increase cyber risk management disclosures in annual reports, as well as companies can understand the factors that influence cyber risk management disclosures so that companies can increase transparency and reduce cyber risk, besides that it can help investors make wiser investment decisions by having an understanding of cyber risk management faced by companies.

The limitations in this research are that the reference sources that examine the disclosure of cyber risk management in Indonesia are still limited, the items of cyber risk management disclosure extracted in the annual report do not show the quality of information conveyed by the company.

It is suggested that future research can use other grand theories so as to get a different perspective on cyber risk management disclosure and can use a wider research sample to cover other sector companies such as the transportasion sector, insurance, and other sectors so that the contribution of research is getting better, plus a more recent research period so that it can describe the current situation.

REFERENCES

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. https://doi.org/10.54371/jiip.v6i11.3176

Arena, C., Petrides, Y., & Vourvachis, P. (2020). Determinants of CSR disclosure in Mexico. *International Journal of Banking, Accounting and Finance*, *11*(3), 303–341. https://doi.org/10.1504/IJBAAF.2020.107943

Ashari, R. A. (2018). Rencana Penerapan Cyber-Risk Management Menggunakan NIST CSF dan COBIT 5. *Jurnal Sistem Informasi*, *14*(2), 83–89. https://doi.org/10.21609/jsi.v14i2.702

Astuti, S. T., Susbiyani, A., Kamelia, I., & Afroh, F. (2021). Systematic Literature Review: Pengaruh Tingkat Pengungkapan Sukarela Terhadap Nilai Perusahaan. *Universitas Muhammadiyah Jember*, *49*, 1–14.

CNN. (2020). *RI Jadi Target Serangan Siber Terbesar Ke-2 di ASEAN Kala WFH*.

Gaol, F. A. L., & Harjanto, K. (2019). Impact of selected factors towards corporate social responsibility (CSR) disclosure: Evidence from indonesia. *Polish Journal of Management Studies*, *20*(1), 181–191. https://doi.org/10.17512/pjms.2019.20.1.16

Hapsari, C. A., & Prasetyo, A. B. (2020). Analyze Factors That Affect Carbon Emission Disclosure (Case Study in Non-Financial Firms Listed on Indonesia Stock Exchange in 2014-2016). *Accounting Analysis Journal*, *9*(2), 74–80. https://doi.org/10.15294/aaj.v9i2.38262

Jubaedah, S., & Setiawan, D. (2023). The effect of ownership structure on social and environmental disclosure in Indonesia. *Diponegoro International Journal of Business*, *6*(1), 24–35. https://doi.org/10.14710/dijb.6.1.2023.24-35

Kelrey, A. R., & Muzaki, A. (2019). Pengaruh Ethical Hacking Bagi Keamanan Data Perusahaan. *Cyber Security Dan Forensik Digital*, *2*(2), 77–81. https://doi.org/10.14421/csecurity.2019.2.2.1625

Kunjana, G. (2017). *Revolusi Digital*. https://investor.id/editorial/revolusi-digital

Li, H., No, W. G., & Wang, T. (2018). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems*, *30*(xxxx), 40–55. https://doi.org/10.1016/j.accinf.2018.06.003

McKinsey&Company. (2020). COVID-19-Facts-and-Insights-July-6. *Global Health and Crisis Response*, 1–54.

Muyasaroh, A. (2020). Analisis Tingkat Dan Kualitas Pengungkapan Aset Tak Berwujud Pada Perusahaan Berbasis Ilmu Pengetahuan Atau Teknologi Di Indonesia. *ABIS: Accounting and Business Information Systems Journal*, *7*(4). https://doi.org/10.22146/abis.v7i4.58864

ISSN : 2597-4785 (ONLINE)
ISSN : 2597-4750 (PRINTED)

Neliana, T. (2018). Pengungkapan Sukarela Laporan Tahunan dan Faktor-faktor yang Mempengaruhi. *Jurnal Akuntansi Dan Keuangan*, *7*. https://doi.org/https://doi.org/10.36080/jak.v7i1.586

Radiansyah, I., Rusdjan, C., & Priyadi, Y. (2016). Analisis Ancaman Phishing Dalam Layanan Online Banking. *Journal of Innovation in Business and Economics*, *7*(1). https://doi.org/https://doi.org/10.22219/jibe.v7i1.3083

Ramadhan, A., Utaminingtas, T. H., & Armeliza, D. (2018). *Analisis Pengaruh Profitabilitas, Intangible Asset, dan Manajemen Risiko terhadap Nilai Perusahaan (Studi Pada Perusahaan Property dan Real Estate yang terdaftar di BEI Periode 2015 - 2017)*.

Rosdini, D. (2016). Relevansi Nilai Aset Tak Berwujud. *Jurnal Akuntansi*, *8*(1), 65–85.

Sari, Y. P., Suhardjanto, D., Probohudono, A. N., & Honggowati, S. (2023). *Cyber Risk Management Disclosure of State-Owned Enterprises*. *15*(2), 180–190.

Sarwono, A. A., Hapsari, D. W. H. D. W., & Nurbaiti, A. (2018). Pengaruh Profitabilitas, Leverage Dan Ukuran Perusahaan Terhadap Pengungkapan Manajemen Risiko. *Angewandte Chemie International Edition, 6(11), 951–952.*, *3*(1), 10–27. https://medium.com/@arifwicaksanaa/pengertian-use-case-a7e576e1b6bf

Solikhawati, A., & Samsuri, A. (2023). Evaluasi Bank Syariah Indonesia Pasca Serangan Siber: Pergerakan Saham dan Kinerja Keuangan. *Jurnal Ilmiah Ekonomi Islam*, *9*(03), 4201–4208. http://dx.doi.org/10.29040/jiei.v9i3.10309

Strupczewski, G. (2021). Defining cyber risk. *Safety Science*, *135*(February 2020), 105143. https://doi.org/10.1016/j.ssci.2020.105143

Sulistyaningsih, S., & Gunawan, B. (2018). Analisis Faktor-faktor yang Memengaruhi Risk Management Disclosure (Studi Empiris Pada Perusahaan Manufaktur yang Terdaftar di Bursa Efek Indonesia Tahun 2012-2014). *Riset Akuntansi Dan Keuangan Indonesia*, *1*(1), 1–11. https://doi.org/10.23917/reaksi.v1i1.1973

Susanto Salim, & Sudharto, S. V. (2022). Efek Firm Size, Profitability, Gearing Ratio, Dan Public Ownership Terhadap Risk Disclosure. *Jurnal Ekonomi*, *26*(11), 125–143. https://doi.org/10.24912/je.v26i11.770

Suwaldiman, S., & Fajrina, A. N. (2022). Pengungkapan Manajemen Risiko: Perusahaan BUMN versus Non-BUMN. *Jurnal Ekonomi Dan Statistik Indonesia*, *2*(1), 124–133. https://doi.org/10.11594/jesi.02.01.14

Wahyuni, S., Nurbaiti, A., & Zultilisna, D. (2020). The effect of audit quality, audit committee size, independent board of commissioners, and company sizes on disclosure of corporate risk management (study on non-bank financial service institutions companies listed on the Indonesia stock exchange in the 2. *E-Proceeding of Management*, *7*(2), 3025–3032. https://openlibrarypublications.telkomuniversity.ac.id/index.php/management/article/view/13259

Wicaksono, A. P., Setiawan, D., Anni Aryani, Y., & Hartoko, S. (2024). The effect of ownership structure on water disclosure in Indonesian companies. *Journal of Open Innovation: Technology, Market, and Complexity*, *10*(1), 24–35. https://doi.org/10.1016/j.joitmc.2023.100185

Wijanarko, N. A. (2023). *Analisis Faktor - Faktor yang Mempengaruhi Risk Management Disclosure Perusahaan Manufaktur yang Terdaftar di Bursa Efek Indonesia 2015 – 2018*. *1*(1). https://doi.org/https://doi.org/10.59024/jise.v1i1.129