International Journal of Economics, Business and Management Research

Vol. 9, No.12; 2025

ISSN: 2456-7760

Cybersecurity Disclosure: Analysis on Banking Companies Listed on the Indonesia Stock Exchange

Erna Hidayah[1*]
Khansa Ananda[2]
[1,2]Accounting Department, Universitas Islam Indonesia
Ringroad Utara, Condongcatur, Depok, Sleman, Yogyakarta, Indonesia

doi.org/10.51505/IJEBMR.2025.91212 URL: https://doi.org/10.51505/IJEBMR.2025.91212

Received: Nov 15, 2025 Accepted: Nov 20, 2025 Online Published: Dec 13, 2025

Abstract
This study aims to analyze the determinants of cybersecurity disclosure in banking companies that go public on the Indonesia Stock Exchange in 2020-2024. The independent variables are company size, company value, gender diversity of the board of directors, financial expertise of the board of directors, and institutional ownership, while the dependent variable is cybersecurity disclosure. The number of observations was 232 banks out of 47 banks listed on the Indonesia Stock Exchange in 2020-2024. The data was analyzed using the EViews version 12 program. The results show that only the company size variable has a significant positive effect on cybersecurity disclosure. Meanwhile, company value, gender diversity of the board of directors, financial expertise of the board of directors, and institutional ownership have no effect. These findings suggest that larger companies tend to have greater capacity and drive to transparently disclose cybersecurity-related information.

Keywords: Cybersecurity disclosure, company size, company value, gender diversity, financial expertise, institutional ownership.

1. Introduction

Cybersecurity Disclosure (CSD) is the disclosure of information related to how a bank protects data, systems, and transactions from cyber threats. CSD provides stakeholders with an overview of how companies identify, manage, and mitigate the risk of cyberattacks that have the potential to disrupt operational activities (Chen at al., 2022). For banks that have gone public, this disclosure is important and mandatory, because: Banks store sensitive data (customer accounts, transactions, pins, biometrics, etc.), cyber attacks on banks have a systemic impact (disrupting financial stability), and investors need certainty that cyber risks are managed properly.

Research on risk disclosure, including ESG disclosure and sustainability disclosure, has grown rapidly in the Indonesian literature, but studies that specifically address cybersecurity disclosure are still very limited. The majority of previous research has focused more on risk disclosure in general, so that the cybersecurity aspect, which is now an important issue for the financial

Vol. 9, No.12; 2025

ISSN: 2456-7760

services industry, has not received adequate attention (Abdullah et al., 2017; Dissanayake et al., 2020). In addition, some findings related to common determinants of disclosure, such as company size, board structure, and company value, show mixed and inconsistent results between studies (Ahmed & Courtis, 1999; Alotaibi & Hussainey, 2016). This indicates the need for a more focused analysis on specific contexts, including in the banking sector that is highly vulnerable to cyber risks.

In a global context, several studies have begun to examine the determinants of CSD and found that company characteristics as well as corporate governance can affect the level of cybersecurity disclosure (Abdullah, 2024). However, these results are obtained from the context of countries with different levels of regulation and governance than Indonesia, so generalizations are still limited. Findings from the MENA region, for example, suggest that CSD has a positive effect on bank performance and that governance structures have a role to play in strengthening these relationships (Gerged & Agogo, 2024). However, there is no empirical evidence to test whether similar patterns also occur in Indonesian banks, which have different market characteristics, levels of digitalization, and regulatory structures. This inconsistency in the context confirms the existence of a gap in the domestic literature that has not been filled.

In Indonesia, research on CSD still focuses on narrow topics, such as the link between CSD and audit quality (Astuti, 2023). Meanwhile, other important dimensions such as the relationship between CSD and company value, investor perception, risk governance, and banking stability, have been largely untouched in empirical studies. With the increasing digitization of financial services and the complexity of cyber threats since 2020, there should be an urgency for banks to disclose cybersecurity information more comprehensively. However, there has been no study that captures how the CSD trend develops in banks listed on the Indonesia Stock Exchange (IDX) during 2020–2024, including what factors drive variations in disclosure rates.

In addition, the dynamics of OJK regulatory developments related to information technology risk management and the increasing cases of data leaks in the financial sector, raise the need to understand whether companies are responsive to these risks through increased transparency of cybersecurity disclosures. The misalignment between the increased risk and the lack of academic studies creates a clear gap, namely there is no empirical evidence that specifically examines the determinants of CSD in the Indonesian banking sector based on the most recent period. Thus, this study has high urgency and relevance to fill these gaps through empirical analysis focusing on banking companies listed on the IDX during 2020–2024.

2. Literature Review

2.1. Theoritical Review

2.1.1. Agency Theory

The agency theory by Jensen & Meckling (1976) explains the existence of a conflict of interest between the principal (shareholders) and the agent (management). Information asymmetry makes management potentially act in its own interests, not the interests of shareholders. Therefore, an

Vol. 9, No.12; 2025

ISSN: 2456-7760

effective corporate governance mechanism is needed to reduce these conflicts. Strengthening governance mechanisms and transparent information disclosure functions to reduce information asymmetry, reduce agency costs, and increase management accountability to shareholders (Chung et al., 2010; Habbash, 2016; Correa-Garcia et al., 2020; Sulimany et al., 2021; Adinegara & Sukamulja, 2021). Thus, agency theory emphasizes that CSD is an instrument to reduce information asymmetry and conflicts of interest, through the supervision of the board of directors and pressure from institutional shareholders.

2.1.2. Signaling Theory

The theory of signals proposed by Spence (1973), states that companies have an incentive to provide positive signals to the market and stakeholders through the disclosure of information. This signal aims to reduce information asymmetry between the company's internal parties (management) and external parties (investors, creditors, regulators, and the public). Transparent disclosure of information, both financial and non-financial data, serves as a positive signal for investors regarding the company's performance and prospects (Moloi, 2016; Abdullah et al., 2017; Susanto & Indrabudiman, 2023). The implementation of effective good corporate governance (GCG), including risk management and cybersecurity practices, can reduce information asymmetry, increase stakeholder trust, and demonstrate the company's readiness to face cyber threats (Ekasari & Kus Noegroho, 2020; Alashi & Badi, 2020; Huang et al., 2021; Pitafi & Cloud, 2024; Yamada, 2024). Thus, CSD serves as a signal of the company's credibility and commitment in maintaining business sustainability and reducing investor doubts amid increasing cyber risks.

2.2. Empirical Review

Alodat et al. (2024) examined the factors influencing Cyber Security Disclosure (CSD) in 225 non-financial companies listed on the London Stock Exchange (LSE) for the period 2011-2020 with 2,250 observations. The independent variables are the size of the board, the independence of the board, the gender diversity of the board, the frequency of board meetings. The results of the study showed that the size of the board, the independence of the board, and the frequency of board meetings had a positive effect, while the gender diversity of the board had no effect on CSD.

Smaili et al. (2023) examined the factors influencing Cyber Security Disclosure (CSD) in the 60 largest companies listed on the Toronto Stock Exchange (TSX) for the 2014-2018 period, with 300 observations. The independent variables are the board's performance, board independence, board size, and the board's financial expertise. The conclusion is that the size of the board has no effect on CSD.

Kurnia & Ardianto (2024) examined 47 banks listed on the Indonesia Stock Exchange (IDX) for the 2014-2021 period, with 376 observations. The independent variables are the proportion of women on the board of commissioners and directors, the critical number of women, the BLAU Index. The result is that women on the board of directors have a negative influence.

Vol. 9, No.12; 2025

ISSN: 2456-7760

Gao et al. (2020), examined 112 companies in the United States for the period 2007-2018. The independent variables are company size, profitability, intangible assets, previous cybersecurity incidents, executive changes, auditor changes. The result is that company size has a positive effect, profitability has no effect, intangible assets have a negative effect, and previous incidents have a positive effect on CSD.

Héroux & Fortin (2022) examined 250 companies listed on the Toronto Stock Exchange (TSX), with independent variables of board IT expertise, board tenure, board independence, female directors on the board of directors, age of the board, committee responsible for cybersecurity on the board of directors. The conclusion is that all independent variables have a positive effect on CSD.

2.3. Hypothesis Development

Company size describes the scale and operational capacity of a company (Itung & Lasdi, 2018; Astari et al., 2025). Based on signal theory, large companies have a tendency to provide positive signals to the market through broader transparency of information, including disclosure of cybersecurity practices. From the perspective of agency theory, large companies face operational complexity and higher agency costs, so management is encouraged to reduce information asymmetry through more comprehensive disclosure. Empirically, previous research has shown that company size has a positive effect on the breadth of disclosure, including cybersecurity disclosure (Dey et al., 2018; Dao & Hoang, 2020; Putra & Rachmawati, 2021; Al-Sartawi, 2022; Sofiani et al. 2024; Singh, 2025; Sari et al. 2024; Gao et al. 2020). Thus, the first hypothesis of this study is:

H1: Company size has a positive effect on cybersecurity disclosure

A company's value reflects the market's perception of the company's performance and prospects, which is usually reflected in the stock price (Sujoko & Soebiantoro, 2007). High-value companies tend to get more attention from investors and stakeholders, thus facing pressure to maintain transparency and disclose important information. According to signal theory, companies with high market value tend to maintain investors' reputations and trust through information transparency, including cybersecurity disclosures. From the perspective of agency theory, high-value companies face immense pressure from investors to maintain sustainability, so management is encouraged to minimize information asymmetry by increasing cybersecurity disclosure. Previous research has shown a positive relationship between company value and disclosure rates, including risk and cybersecurity issues (Dey et al., 2018; Dao & Hoang, 2020; Al-Sartawi, 2022). Therefore, the second hypothesis of this study is:

H2: Company value has a positive effect on cybersecurity disclosure.

Companies with more gender-diverse boards of directors are believed to have better oversight capabilities and more transparent decision-making, so they tend to disclose cybersecurity information more effectively. Signal theory explains that the presence of women on the board of

Vol. 9, No.12; 2025

ISSN: 2456-7760

directors is a signal of diversity and good governance for investors. Agency theory asserts that gender diversity strengthens oversight mechanisms, reduces agency conflicts, and encourages more transparent disclosure. Previous research has found that women's representation on boards of directors improves the quality of disclosure, including risk and sustainability aspects (García-Sánchez et al., 2019; Pucheta-Martínez & Gallego-Álvarez, 2020; Radu & Smaili, 2022; Mazumder & Hossain, 2023; Héroux & Fortin, 2022; Sari et al. 2024). Thus, the three hypotheses of this study are:

H3: Gender diversity of the board of directors has a positive effect on cybersecurity disclosure

The financial expertise of board members includes the ability to understand financial information and accurately assess risks, thereby increasing the effectiveness of management oversight and reducing agency issues (Fama & Jensen, 1983; Allini et al., 2016). Based on signal theory, boards with financial expertise are able to provide credibility signals regarding the quality of corporate governance through broader disclosure. From the point of view of agency theory, board members who have a financial background can carry out monitoring functions more effectively, thus encouraging management to increase information disclosure, including cybersecurity disclosure. Empirical research supports that the financial expertise of boards is positively related to the level of transparency and risk disclosure (Krishnan & Visvanathan, 2008; Ho et al., 2015; Dao & Hoang, 2020). Thus, the four hypotheses of this study are:

H4: The financial expertise of the board of directors has a positive effect on cybersecurity disclosure.

Institutional ownership reflects the proportion of a company's shares held by financial institutions such as pension funds, banks, insurance companies, mutual funds, and other investment institutions. According to signal theory, institutional ownership signals market confidence as institutional investors demand higher governance and transparency. In agency theory, institutional investors act as an effective external oversight mechanism, thus encouraging companies to reduce information asymmetry by increasing cybersecurity disclosure. Previous research has shown that institutional ownership has a positive effect on the quality of disclosure and transparency of companies (Shleifer & Vishny, 1997; Suto & Takehara, 2017; Al-Sartawi, 2022). Thus, the five hypotheses of this study are:

H5: Institutional ownership has a positive effect on cybersecurity disclosure

2.4. Research Model

Here is the research model:

Vol. 9, No.12; 2025

ISSN: 2456-7760

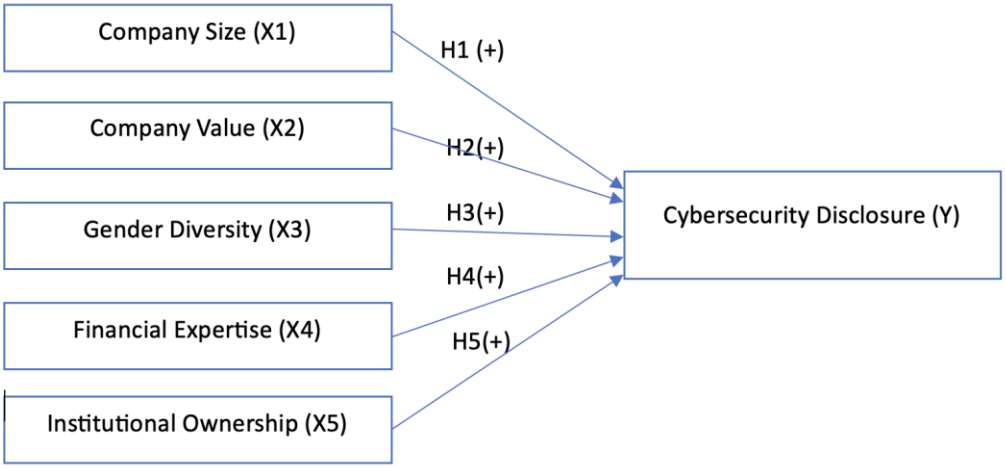

Figure 1. Research Model

3. Method

3.1. Population and Sample

The population in this study is all banking sector companies listed on the Indonesia Stock Exchange for the 2020-2024 period as many as 47 banks. The research period is 5 years so that there are a total sample of 235 companies. There are banks that have only gone public after 2020 and there are banks that have merged, so the total sample analyzed was 232 banks.

3.2. Data Collection Methods

The type of data used in this study is secondary data obtained from annual reports and sustainability reports that can be accessed through the company's official website and the IDX's official website (www.idx.co.id).

3.3. Operational Definitions and Variable Measurements

In this study, the dependent variables are Cybersecurity Disclosure and five independent variables, namely company size, company value, gender diversity of the board of directors, financial expertise of the board of directors, and institutional leadership.

Cybersecurity Disclosure (CSD)

The dependent variable in this study is cybersecurity disclosure (CSD), which is voluntary disclosure related to cybersecurity risks and management in the company's annual report or sustainability (Chen et al., 2022; Mazumder & Hossain, 2023). CSD is measured using keywords adapted from Gordon et al. (2010) and calculated with the following natural logarithms:

CSD = ln(number of words related to cybersecurity)

CSD measurement using keyword frequency is relevant, as it reflects the level of emphasis companies have on cybersecurity issues in the context of external communications. This

Vol. 9, No.12; 2025

ISSN: 2456-7760

approach is in line with Agency Theory (reducing asymmetric information) and Signaling Theory (sending management commitment signals). This method is also consistent with the practice of content analysis in accounting which is considered objective, measurable, and replicable.

Company Size (SIZE)

The size of a company reflects the scale of operations and the capacity of the company to carry out its business activities. This variable is measured using the company's total assets because it is considered more representative than the market capitalization or total sales (Itung & Lasdi, 2018; Smaili et al., 2023; Astari et al., 2025). Measurements are carried out with the natural logarithm of total assets as follows:

***SIZE* = ln (Total Assets)**

Company Values (VALUE)

A company's value indicates the market's perception of a company's performance and prospects, which can influence the pressure to disclose information. This variable is measured using the Price-to-Book Value (PBV) ratio, which is the comparison between the market price per share and the book value per share (Harmono, 2009; Fidhayatin & Dewi, 2012; Irawan & Kusuma, 2019). The measurement formula is as follows:

$$\textbf{VALUE} = \frac{\textbf{Price per share}}{\textbf{Book Value per share}}$$

Gender Diversity of the Board of Directors (GENDER)

The gender diversity of the board of directors was measured to assess the inclusivity and influence of women in the company's strategic decision-making. This variable is calculated based on the percentage of the number of female board members to the total board members (Rahmadani, 2023; Mazumder & Hossain, 2023). The measurement formula is as follows:

$$\textbf{GENDER} = \frac{\textbf{Number of female directors}}{\textbf{Number of directors}} \textbf{ x 100\%}$$

Financial Expertise of the Board of Directors (EXPERT)

This variable assesses the ability of board members who have a background or expertise in finance and or accounting to evaluate the company's financial risks and information (Allini et al., 2016; Alshirah et al., 2020). The measurement is carried out by calculating the proportion of members of the board of directors who have financial expertise compared to the total members of the board of directors as follows:

$$\textbf{EXPERT} = \frac{\textbf{Number of directors with financial expertise}}{\textbf{Number of directors}} \textbf{ x 100\%}$$

Vol. 9, No.12; 2025

ISSN: 2456-7760

Institutional Ownership (INST)

Institutional ownership describes the participation of financial institutions in the company's ownership structure and its role in management supervision (Ristiyana, 2017; Nilayanti & Suaryana, 2019; Marsinah, 2021). This variable is measured as the proportion of shares owned by the institution to the total outstanding shares as follows:

$$\textbf{INST} = \frac{\textbf{Number of institution shares}}{\textbf{Number of shares outstanding}}$$

4. Results

4.1. Descriptive Statistical Analysis

The results of the descriptive statistical analysis are presented in Table 1 below.

Table 1. Descriptive Statistical

Variable	Obs.	Mean	Min	Max	Std. Dev.
CSD (Y)	232	5.764	4.143	7.256	0.534
SIZE (X_1)	232	31.460	27.997	35.426	1.704
VALUE (X_2)	232	2.479	0.230	63.423	5.598
GENDER (X_3)	232	0.179	0.000	0.880	0.177
EXPERT (X_4)	232	0.986	0.400	1.000	0.059
INST (X_5)	232	0.856	0.046	1.000	0.179

Table 1 above describes the dependent and independent variables in this study. The number of observations is 232 banking companies that go public on the IDX for the 2020-2024 period.

4.2. Panel Data Regression Analysis

The analysis method in this study is panel data regression, which is a statistical technique that combines cross-section and time series data simultaneously. Before determining the panel regression model used, a model selection test was first carried out to determine the most suitable panel regression method.

4.2.1. Model Selection Test

The best panel data model was selected through three main tests, namely the Chow test, the Hausman test, and the Lagrange Multiplier (LM) test. According to Gujarati & Porter (2009), the Chow Test to choose between CEM and FEM, the Hausman Test to choose between FEM and REM, and the Lagrange Multiplier Test (LM Test) to choose CEM and REM.

Chow Test

The Chow test is used to determine whether *the Common Effect* (CEM) or *Fixed Effect* (FEM) model is more appropriate in estimating panel data.

Vol. 9, No.12; 2025

ISSN: 2456-7760

Table 2. Chow Test Results

Effects Test	Statistic	d.f.	Prob.
Cross-section F	11.0776	(46.180)	0.0000
Cross-section Chi-square	311.6031	46	0.0000

Based on the results of the Chow Test presented in Table 2, a *p-value* of 0.0000 (< 0.05) was obtained, so the most suitable model was FEM. The next test was carried out using the Hausman Test.

Hausman Test

The Hausman test is used to determine the most appropriate model between Fixed Effect (FEM) and *Random Effect* (REM) in estimating panel data.

Table 3. Hausman Test Results

Test Summary	Chi-Sq. Statistic	Chi-Sq. d.f.	Prob.
Cross-section random	1.9901	5	0.8505

Based on the results of the Hausman Test in Table 3, a p-value of 0.8505 (> 0.05) was obtained, so the model chosen was REM. Thus, the test continued using the Lagrange Multiplier Test (LM Test). On the other hand, if the p-value < 0.05, then the selected model is FEM and testing with LM Test is not required.

Uji Lagrange Multiplier

The Lagrange Multiplier Test (LM Test) is carried out when the results of the Chow Test and Hausman Test show a choice between the Pooled Least Square (PLS) and Random Effect (REM) models. The purpose of this test is to determine whether a more appropriate CEM or REM model is used in estimating panel data.

Table 4. Lagrange Multiplier Test Results

	Test Hypothesis		
	Cross-section	Time	Both
Breusch-Pagan	205.6429	0.7464	206.3894
	(0.0000)	(0.3876)	(0.0000)

Although the REM has been determined based on the results of the previous Chow Test and Hausman Test, the LM Test is still carried out as an additional test to strengthen the selection of the model. Based on the results of the LM Test presented in Table 4, a Breusch-Pagan p-value of 0.0000 (< 0.05) was obtained, which further confirms that REM is the right choice in estimating panel data in this study. Since REM uses the Generalized Least Squares (GLS) method that has

Vol. 9, No.12; 2025

ISSN: 2456-7760

taken into account individual variations at random, testing classic assumptions such as normality, heteroscedasticity, and autocorrelation is no longer necessary.

4.2.2. Hypothesis Test Results

Table 5. Hypothesis Test Results

Hypothesis	Description	Coefficient	Prob.	Result
H_1	Company size	0.240	0.000	Supported
H_2	Company value	-0.002	0.679	Not Supported
H_3	Gender diversity	-0.085	0.514	Not Supported
H_4	Finansial expertise	-0.763	0.058	Not Supported
H_5	Institutional ownership	0.185	0.149	Not Supported
F statistic = 0.000	Adj R-squared = 0.583			

In Table 5, it can be concluded that company size has a significant positive effect on CSD disclosure, while company value, gender diversity of the board of directors, financial expertise of the board of directors, and institutional ownership have no effect on CSD disclosure. The Adjusted R-squared value of 0.583 or 58.3% indicates that the regression model used has good predictive ability after considering the number of variables and observations.

5. Discussion

The results showed that of the five independent variables studied, only the company size variable had a significant positive effect on the level of Cybersecurity Disclosure (CSD) in public banking companies in Indonesia. Meanwhile, the variables of company value, gender diversity of the board of directors, financial expertise of the board of directors, and institutional ownership did not show a significant influence. These findings indicate that cybersecurity disclosure practices in the banking sector in Indonesia are more influenced by operational scale and regulatory demands than by the characteristics of the company's internal governance.

5.1. The Effect of Company Size on Cybersecurity Disclosure

The results of the analysis show that company size has a significant positive effect on CSD in banking companies in Indonesia for the 2020–2024 period, which means that the first hypothesis is supported. These results are also in line with previous research by Sofiani et al. (2024), Gao et al., (2020), Singh (2025), Jiang et al., (2022), Sari et al., (2024), Kurniasih & Sari (2013), and Itung & Lasdi (2018) which showed that large companies are more motivated to engage in strategic disclosures, including CSD. This is due to the availability of adequate resources, high market pressures, and demands for accountability. Thus, it can be concluded that company size is an important determinant in driving CSD practices in the banking sector.

Vol. 9, No.12; 2025

ISSN: 2456-7760

5.2. The Effect of Company Value on Cybersecurity Disclosure

For the second hypothesis, the results of the analysis show that the company value measured by PBV has no effect on the CSD so the second hypothesis is not supported. The lack of effect of corporate value on CSD shows that bank companies in Indonesia have not seen cybersecurity disclosure as a strategy to increase market perception or increase company value. In the perspective of Signaling Theory, companies with high scores should be encouraged to provide quality signals through better disclosure. However, these results indicate that cybersecurity signals are not yet considered as strategic signals that have a direct impact on market valuations. The results of this study support the findings of Chen et al.'s (2014) research which shows that company values do not always encourage openness on sensitive issues such as information security. However, these results differ from Gordon et al. (2010), Berkman et al. (2018), and Hidayat et al. (2021) which show a positive relationship between information disclosure and company value. Thus, market motivations such as company value have not been fully the main driver of information disclosure in the field of cybersecurity.

5.3. The Effect of Gender Diversity of the Board of Directors on Cybersecurity Disclosure

The third hypothesis shows that the gender diversity of the board of directors has no effect on the level of CSD, so this hypothesis is not supported. Agency Theory predicts that gender diversity on the board of directors can improve oversight, risk sensitivity, and quality of disclosure. However, the absence of the influence of gender diversity on CSD suggests that the presence of women on the board has not substantively influenced cyber risk transparency policies. This is likely to happen because cybersecurity issues are still considered a technical aspect, not a strategic governance issue discussed at the board level.

These findings are in line with the research of Alodat et al. (2024) and Shukla & Pandey (2023) which also found a non-significant effect, but differed from the results of Sari et al. (2024), Mazumder & Hossain (2023), Radu & Smaili (2022), and Héroux & Fortin (2022) which showed a positive influence, as well as Kurnia & Ardianto (2024) found a significant negative influence on CSD levels. Thus, these results indicate that gender diversity in the board of directors still does not provide a meaningful role to the practice of CSD in the Indonesian banking sector.

5.4. The Effect of the Financial Expertise of the Board of Directors on Cybersecurity Disclosure

In the fourth hypothesis, the results of the analysis show that the financial expertise of the board of directors has no effect on the level of CSD, which means that the fourth hypothesis is not supported. This means that the existence of board members with financial backgrounds has not made a real contribution in encouraging information disclosure related to cybersecurity. Agency Theory assumes that boards with financial expertise are able to improve the quality of oversight and encourage transparency. However, the results of this study show that financial competence does not automatically translate into increased cybersecurity disclosure. This can happen because cyber issues require IT technical competence, not financial competence.

Vol. 9, No.12; 2025

ISSN: 2456-7760

These results are different from the research of Smaili et al. (2023) which found that the financial expertise of board members of the board of directors had a positive effect on the increase in the amount of cyber risk information in the annual report, and Alshirah et al. (2020) which recorded the positive contribution of financial expertise to the quality of non-financial disclosures. Research by Allini et al. (2016) concluded that the financial expertise of the board of directors has a negative effect on risk disclosure in state-owned companies in Italy, due to the tendency of the conservative attitude of the directors in withholding strategic information that is considered sensitive. Thus, financial expertise on the board of directors has not yet become the dominant factor in influencing CSD practices.

5.5. The Effect of Institutional Ownership on Cybersecurity Disclosure

The results of the analysis showed that institutional ownership had no effect on the CSD level, so the fifth hypothesis was not supported. Within the framework of Agency Theory, institutional investors are expected to be able to encourage companies to increase transparency, including in terms of cyber risk disclosure. However, the findings of this study show that institutional shareholders have not paid special attention to the issue of cybersecurity disclosure so that it does not put significant pressure on management.

These findings are in line with the research of Anggraeni & Iradianty (2023), Gustyana & Putri (2022) and Prasetyo (2023) which found that institutional ownership has no effect on risk management disclosure and CSR disclosure. However, these results are different from Sari et al. (2024) who found a negative influence, Hardana & Syafruddin (2019) and Dihardjo & Hersugondo (2023) who found a positive influence. Thus, institutional ownership cannot be considered as a determining factor in encouraging CSD practices in the Indonesian banking sector.

6. Conclusion and Implication

6.1. Conclusion

Based on the results of the analysis and discussion that has been carried out, it can be concluded that the level of Cybersecurity Disclosure (CSD) in public banking companies in Indonesia is influenced by the size of the company. Meanwhile, the variables of company value, gender diversity of the board of directors, financial expertise of the board of directors, and institutional ownership did not have a significant effect on CSD. This shows that cybersecurity disclosure is more compliance-based and influenced by the company's operational characteristics. These findings confirm that banking management needs to view cybersecurity as an integral part of the institution's operational sustainability and reputation.

6.2. Implications

The important implication is that the banking industry needs to shift the disclosure paradigm from simply complying with regulations to being a tool to increase public trust, corporate value, and digital resilience. Given the increase in cyberattacks during the 2020–2024 period,

Vol. 9, No.12; 2025

ISSN: 2456-7760

cybersecurity transparency should be seen as an integral part of the operational sustainability and reputation of banking institutions.

6.3. Suggestions for Future Research

For future researchers, it is recommended to use a more in-depth CSD measurement approach, such as content analysis based on the weight of disclosure quality, machine learning text analysis, or an index based on international standards. In addition, researchers are further advised to include external variables such as audit quality, regulation, industrial risk level, and also expand the sample size by including other industry sectors outside of banking, such as financial technology companies (fintech) or sectors that have a high intensity of information system use. It is hoped that further research can provide a more comprehensive picture of Cybersecurity Disclosure practices in various types of industries.

References

Abdullah, A., Waemustafa, W., & Mat Isa, H. (2017). *Disclosure of Information in the Company's Annual Reports: A Bibliometric Analysis* (Vol. 2, Ser. 2, p. 66). CSRC Publishing. http://doi.org/10.2139/ssrn.3057542

Abdullah, W. N. (2024). A systematic literature review on cybersecurity disclosure determinants. *KnE Social Sciences*, 9(2), 256–282.

Adinegara, G. R., & Sukamulja, S. (2021). The Effect of Good Corporate Governance on the Market Value of Financial Sector Companies in Indonesia. *Jurnal Akuntansi dan Keuangan*, *23*(2), 83–94. https://doi.org/10.9744/jak.23.2.83-94

Ahmad, N. Z., & Septiani. A. (2017). Pengaruh Interlock Dewan Direksi Dan Interlock Auditor Eksternal Terhadap Pengungkapan Sukarela Pada Laporan Tahunan. *Diponegoro Journal of Accounting*, *6*(4), 201–215.

Ahmed, K., & Courtis, J. K. (1999). Associations between corporate characteristics and disclosure levels in annual reports: A meta-analysis. *British Accounting Review*, 31(1), 35–61.

Alashi, S. A., & Badi, D. H. (2020). The Role of Governance in Achieving Sustainable Cybersecurity for Business Corporations. *Journal of Information Security & Cybercrimes Research*, *3*(1), 97–112. https://doi.org/10.26735/EINT7997

Allini, A., Rossi, F. M., & Hussainey, K. (2016). The Board's Role in Risk Disclosure: An Exploratory Study of Italian Listed State-Owned Enterprises. *Public Money & Management*, *36*(2), 113–120. https://doi.org/10.1080/09540962.2016.1118935

Alodat, A. Y., Hao, Y., Nobanee, H., Ali, H., Mansour, M., & Amosh, H. Al. (2024). Board Characteristics and Cybersecurity Disclosure: Evidence from the UK. *Electronic Commerce Research*. https://doi.org/10.1007/s10660-024-09867-w

Alotaibi, K., & Hussainey, K. (2016). Determinants of CSR disclosure quantity and quality: Evidence from Saudi Arabia. *International Review of Financial Analysis*, 47, 247–261.

Alshirah, M. H., Rahman, A. A., & Mustapa, I. R. (2020). Board of Directors' Characteristics and Corporate Risk Disclosure: The Moderating Role of Family Ownership. *EuroMed Journal of Business*, *15*(2), 219–252. https://doi.org/10.1108/EMJB-09-2019-0115

Vol. 9, No.12; 2025

ISSN: 2456-7760

Anderson, R. C., Mansi, S., & Reeb, D. M. (2004). Board Characteristics, Accounting Report Integrity, and the Cost of Debt. *Journal of Accounting and Economics*, *37*(3), 315–342. https://doi.org/10.1016/j.jacceco.2004.01.004

Anggraeni, H., & Iradianty, A. (2023). Analisis Good Corporate Governances dan Pengungkapan Manajemen Risiko pada Perusahaan Farmasi. *Jurnal Orientasi Bisnis Dan Entrepreneurship*, *4*(1), 81–94. https://doi.org/10.33476/jobs.v4i1.3609

Ardianto, R., Ramdhani, R. F., Dewi, L. O. A., Prabowo, A., Saputri, Y. W., Lestari, A. S., & Hadi, N. (2024). Transformasi Digital dan Antisipasi Perubahan Ekonomi Global dalam Dunia Perbankan. *MARAS: Jurnal Penelitian Multidisiplin*, *2*(1), 80–88. https://doi.org/10.60126/maras.v2i1.114

Ariyanto, S. (2024). Analisis Framing Model Robert N. Entman tentang Serangan Ransomware Pada PT Bank Syariah Indonesia Tbk. *Jurnal CommLine*, *9*(1), 59–77. https://doi.org/10.36722/cl.v9i1.2899

Astari, N. M. P., Gama, A. W. S., & Astiti, N. P. Y. (2025). Pengaruh Stuktur Modal, Good Corporate Governance dan Ukuran Perusahaan terhadap Harga Saham Perusahaan Perbankan yang Terdaftar di BEI Tahun 2021-2023 dengan Profitabilitas Sebagai Pemediasi. *EMAS*, *6*(4), 843–859. https://doi.org/10.36733/emas.v6i4.6106

Astuti, F. R. (2023). Cybersecurity disclosure dan kualitas audit pada perusahaan perbankan Indonesia (Tesis tidak dipublikasikan). Universitas Pendidikan Indonesia.

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity Awareness and Market Valuations. *Journal of Accounting and Public Policy*. https://doi.org/10.1016/j.jaccpubpol.2018.10.003

Chen, J., Henry, E., & Jiang, X. (2022). Is Cybersecurity Risk Factor Disclosure Informative Evidence from Disclosures Following a Data Breach. *Journal of Business Ethics*, *187*(3), 199–224. https://doi.org/10.1007/s10551-022-05107-z

Chen, J. J., Tan, Y., & Gong, S. X. H. (2014). Do Higher Value Firms Voluntarily Disclose More Information? Evidence from China. *The British Accounting Review*, *47*, 18–32. https://doi.org/10.2139/ssrn.2205403

Chung, K. H., Elder, J., & Kim, J.-C. (2010). Corporate Governance and Liquidity. *Journal of Financial and Quantitative Analysis*, *45*(2), 265–291. https://doi.org/10.1017/S0022109010000104

Correa-Garcia, J. A., Garcia-Benau, M. A., & Garcia-Meca, E. (2020). Corporate governance and its implications for sustain-ability reporting quality in Latin American business groups. *Journal of Cleaner Production*, *260*(1), 121142. https://doi.org/10.1016/j.jclepro.2020.121142

CNN Indonesia. (2023, Mei 13). *Ransomware LockBit 3.0 klaim lumpuhkan BSI dan curi data pengguna*. https://www.cnnindonesia.com/teknologi/20230513093401-185-949046/ransomware-lockbit-30-klaim-lumpuhkan-bsi-dan-curi-data-pengguna

Dihardjo, J. F., & Hersugondo, H. (2023). Exploring the Impact of ESG Disclosure, Dividend Payout Ratio, and Institutional Ownership on Firm Value: A Moderated Analysis of Firm Size. *Jurnal Ekonomi Bisnis Dan Kewirausahaan*, *12*(2), 184–207. https://doi.org/10.26418/jebik.v12i2.64129

Vol. 9, No.12; 2025

ISSN: 2456-7760

Dissanayake, T., Dissanayake, D., & Davidson, R. (2020). Risk disclosure and firm characteristics: Evidence from emerging markets. *Journal of Accounting in Emerging Economies*, 10(3), 489–512.

Ekasari, J. C., & Kus Noegroho, Y. A. (2020). The Impact of Good Corporate Governance Implementation on Firm Value. *International Journal of Social Science and Business*, *4*(4), 553–560. https://doi.org/10.23887/ijssb.v4i4.29688

Eling, M. (2020). *Cyber risk research in business and actuarial science* (review). — ringkasan tinjauan literatur mengenai hasil yang beragam

Fajariah, Z. I., & Akbar, A. (2025). Dampak Transaksi Digital Banking Terhadap Penyusutan Penggunaan Mesin Atm Di Indonesia. *E-Proceeding of Management*, *12*(8), 2339–2347.

Fama, E. F., & Jensen, M. C. (1983). Agency Problems and Residual Claims. *Journal of Law & Economics*, *26*(2), 327–349. https://doi.org/10.2139/ssrn.94032

Fidhayatin, S. K., & Dewi, N. H. U. (2012). Analisis Nilai Perusahaan, Kinerja Perusahaan dan Kesempatan Bertumbuh Perusahaan terhadap Return Saha pada Perusahaan Manufaktur yang Listing di BEI. *The Indonesian Accounting Review*, *2*(2), 203–214.

Gao, L., Calderon, T. G., & Tang, F. (2020). Public Companies' Cybersecurity Risk Disclosures. *International Journal of Accounting Information Systems*, *38*, 100468. https://doi.org/10.1016/j.accinf.2020.100468

Gerged, A. M., & Agogo, D. (2024). Cybersecurity disclosure and bank performance: The moderating effect of corporate governance structures. *Future Business Journal*, 10(1), 1–18.

Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market Value of Voluntary Disclosures Concerning Information Security. *MIS Quarterly*, *34*(3), 567–594. https://doi.org/10.2307/25750692

Gustyana, J., & Wijaya, H. (2020). Pengaruh Kepemilikan Manajerial, Kepemilikan Institusional, dan Ukuran Perusahaan terhadap Kinerja Perusahaan Manufaktur. *Jurnal Multiparadigma Akuntansi*, *2*(4), 1718–1727. https://doi.org/10.24912/jpa.v2i4.9367

Gustyana, T. T., & Putri, R. S. A. (2022). Pengaruh Good Corporate Governance terhadap Pengungkapan Manajemen Risiko pada Perusahaan Telekomunikasi. *Jurnal Ilmiah MEA (Manajemen, Ekonomi, & Akuntansi)*, *6*(1), 951–960. https://doi.org/10.31955/mea.v6i1.1903

Habbash, M. (2016). Corporate Governance and Corporate Social Responsibility Disclosure: Evidence from Saudi Arabia. *Social Responsibility Journal*, *12*(4), 740–754. https://doi.org/10.1108/SRJ-07-2015-0088

Hardana, H., & Syafruddin, M. (2019). Analisis Pengungkapan Manajemen Risiko (Bukti Indonesia). *Diponegoro Journal of Accounting*, *8*(2), 1–15.

Harmono. (2009). *Manajemen Keuangan: Berbasis Balanced Scorecard*. Bumi Aksara.

Haryanto, A. T. (2024, Januari 31). *APJII: Jumlah pengguna internet Indonesia tembus 221 juta orang*. detikInet. https://inet.detik.com/cyberlife/d-7169749/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang

Héroux, S., & Fortin, A. (2022). Board of Directors' Attributes and Aspects of Cybersecurity Disclosure. *Journal of Management and Governance*, *28*(2), 359–404. https://doi.org/10.1007/s10997-022-09660-7

Vol. 9, No.12; 2025

ISSN: 2456-7760

Hidayat, W. W., Yuniati, T., Prasetyo, E. T., & Husadha, C. (2021). Pengaruh Kepemilikan Manajerial, Leverage dan CSR terhadap Nilai Perusahaan, Studi Kasus Perusahaan Jasa di Indonesia. *Jurnal Ilmiah Manajemen Ubhara*, *3*(1), 214-227. https://doi.org/10.31599/jmu.v3i1.893

Huang, K., Madnick, S., Choucri, N., & Zhang, F. (2021). A Systematic Framework to Understand Transnational Governance for Cybersecurity Risks from Digital Trade. *Global Policy*, *12*(5), 625–638. https://doi.org/10.1111/1758-5899.13014

Indonesia. (1998). *Undang-Undang Republik Indonesia Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan*.

Irawan, D., & Kusuma, N. (2019). Pengaruh Struktur Modal dan Ukuran Perusahaan terhadap Nilai Perusahaan. *Jurnal AKTUAL*, *17*(1), 66–81.

Itung, S., & Lasdi, L. (2018). Pengaruh Strategi Diversifikasi dan Kepemilikan Manajerial terhadap Kinerja Perusahaan yang Dimoderasi oleh Struktur Modal. *Jurnal Akuntansi Kontemporer*, *10*(2), 69–80. https://doi.org/10.33508/jako.v10i2.2219

Jensen, M. C., & Meckling, W. H. (1976). Theory of the Firm: Managerial Behavior, Agency Costs, and Ownership Structure. *Journal of Financial Economics*, *3*(4), 305–360. https://doi.org/10.1016/0304-405X(76)90026-X

Jiang, W., Legoria, J., Reichelt, K. J., & Walton, S. (2022). Firm Use of Cybersecurity Risk Disclosures. *Journal of Information Systems*, *36*(1), 151–180. https://doi.org/10.2308/ISYS-2020-067

Kelton, A. S., & Pennington R. R. (2020). Do voluntary disclosures mitigate the cybersecurity breach contagion effect? *Journal of Information Systems*, *34*(3), 133–157. https://doi.org/10.2308/isys-52628

Komite Nasional Kebijakan Governance. (2006). *Pedoman Umum Good Corporate Governance Indonesia*.

Kurnia, P., & Ardianto, A. (2024). Board Gender Diversity and Cyber Security Disclosure in the Indonesian Banking Industry: A Two-Tier Governance Context. *Corporate Governance*, *24*(7), 1614–1637. https://doi.org/10.1108/CG-01-2023-0010

Kurniasih, T., & Sari, M. M. R. (2013). Pengaruh Return on Assets, Leverage, Corporate Governance, Ukuran Perusahaan, dan Kompensasi Rugi Fiskal pada Tax Avoidance. *Buletin Studi Ekonomi*, *18*(1), 58–66.

Marsinah, M. (2021). Pengaruh Struktur Kepemilikan Saham, Struktur Modal dan Profitabilitas terhadap Nilai Perusahaan pada Perusahaan Manufaktur Sub Sektor Properti dan Real Estate yang Terdaftar di Bursa Efek Indonesia. *Ekonomica Sharia: Jurnal Pemikiran dan Pengembangan Ekonomi Syariah*, *7*(1), 47–66. https://doi.org/10.36908/esha.v7i1.313

Masoud, N., & Al-Utaibi, G. (2022). *The determinants of cybersecurity risk disclosure in firms' financial reporting: Empirical evidence.* Research in Economics

Mazumder, M. M. M., & Hossain, D. M. (2023). Voluntary Cybersecurity Disclosure in the Banking Industry of Bangladesh: Does Board Composition Matter? *Journal of Accounting in Emerging Economies*, *13*(2), 217–239. https://doi.org/10.1108/JAEE-07-2021-0237

Mazumder, M. M. M., & Sobhan, A. (2021). The Spillover Effect of the Bangladesh Bank Cyber Heist on Banks' Cyber Risk Disclosures in Bangladesh. *Journal of Operational Risk*, *15*(4), 53–76. https://doi.org/10.21314/JOP.2020.249

Vol. 9, No.12; 2025

ISSN: 2456-7760

Moloi, T. (2016). Governance of risks in South Africa's public higher education institutions (HEIs). *Investment Management and Financial Innovations*, *13*(2-1), 226-234. https://doi.org/10.21511/imfi.13(2-1).2016.09

Morgan, S. (2020, November 13). *Cybercrime to cost the world $10.5 trillion annually by 2025*. Cybercrime Magazine. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Nilayanti, M., & Suaryana, I. G. N. A. (2019). Pengaruh Kepemilikan Manajerial dan Kepemilikan Institusional Terhadap Kinerja Keuangan Perusahaan Dengan Kebijakan Deviden Sebagai Pemoderasi. *E-Jurnal Akuntansi Universitas Udayana*, *26*(2), 906–936. https://doi.org/10.24843/EJA.2019.v26.i02.p03

Nugroho, R. S. (2023, Maret 15). *Daftar Emiten Bank di Bursa Efek Indonesia 2023*. IDXChannel. https://www.idxchannel.com/market-news/daftar-emiten-bank-di-bursa-efek-indonesia-2023

Otoritas Jasa Keuangan. (2022). *Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum*.

Pasaribu, M. R., & Ningtias, S. R. A. (2025). Perlindungan Nasabah dalam Penggunaan Layanan Mobile Banking di Bank Syariah Kota Medan. *Rewang Rencang: Jurnal Hukum Lex Generalis*, *6*(2), 1–22.

Pitafi, Z. R., & Awan, T. M. (2024). Perspective Chapter: Cybersecurity and Risk Management—New Frontiers in Corporate Governance. In *Corporate Governance - Evolving Practices and Emerging Challenges*. IntechOpen. https://doi.org/10.5772/intechopen.1005153

Prasetyo, M. S. (2023). Pengaruh Kepemilikan Institusional, Kepemilikan Asing terhadap Pengungkapan Corporate Social Responsibility. *Jurnal Ekonomi Dan Bisnis*, *15*(2), 61–69. https://doi.org/10.55049/jeb.v15i2.224

Prayoga, E. B. (2013). Pengaruh Struktur Kepemilikan Dan Ukuran Perusahaan Terhadap Pengungkapan Manajemen Risiko. *Jurnal Akuntansi & Keuangan*, *4*(1), 1–19. http://doi.org/10.36448/jak.v4i1.237

Radu, C., & Smaili, N. (2022). Board Gender Diversity and Corporate Response to Cyber Risk: Evidence from Cybersecurity Related Disclosure. *Journal of Business Ethics*, *177*(2), 351–374. https://doi.org/10.1007/s10551-020-04717-9

Rahmadani, S. (2023). *Pengaruh Keberagaman Gender Dewan Direksi terhadap Agresivitas Pajak dengan Kinerja Keberlanjutan sebagai Variabel Mediasi* (Skripsi). Universitas Islam Negeri Raden Mas Said Surakarta.

Ristiyana, R. (2017). Pengaruh Mekanisme Good Corporate Governance terhadap Luas Pengungkapan Corporate Social Responsibility. *Jurnal Ekonomi dan Bisnis*, *26*(1).

Sari, L., Adam, M., Fuadah, L. L., & Yusnaini, Y. (2024). Determinant Factors of Cyber Security Disclosure: A Systematic Literature Review. *8th Sriwijaya Economics, Accounting, and Business Conference*, 387–398. https://doi.org/10.18502/kss.v9i14.16113

Sari, R. P. (2024, Desember 23). *Siapkah perusahaan Indonesia hadapi ancaman siber 2025?* CSIRT Indonesia. https://csirt.or.id/berita/siapkah-indonesia-hadapi-siber-2025

Shleifer, A., & Vishny, R.W. (1997). A Survey of Corporate Governance. *Journal of Finance*, *52*(2), 737–783. https://doi.org/10.1111/j.1540-6261.1997.tb04820.x

Shleifer, A., & Vishny, R. W. (1986). Large Shareholders and Corporate Control. *Journal of Political Economy*, *94*(3), 461–488. https://doi.org/10.1086/261385

Shukla, P., & Pandey, A. (2023). *Cybersecurity oversight and board diversity: The disclosure paradigm*. In R. Prasad (Ed.), *Cyberfeminism and gender violence in social media* (pp. 129–148). IGI Global. https://doi.org/10.4018/978-1-6684-5214-1.ch006

Singh, H. (2025). Voluntary Cybersecurity Risk Disclosures and Firms' Characteristics: The Moderating Role of the Knowledge-Intensive Industry. *Asian Journal of Accounting Research*, *10*(2), 168–185. https://doi.org/10.1108/AJAR-12-2023-0413

Smaili, N., Radu, C., & Khalili, A. (2023). Board Effectiveness and Cybersecurity Disclosure. *Journal of Management and Governance*, *27*(4), 1049–1071. https://doi.org/10.1007/s10997-022-09637-6

Sofiani, M., Ramadhanty, D. P., & Jubaedah, S. (2024). Cyber Risk Management Disclosure: The Impact of Firm Size, Profitability, and Intangible Asset. *International Journal of Entrepreneurship and Business Development*, *07*(05), 929–937. https://doi.org/10.29138/ijebd.v7i5.2844

Sujoko, S., & Soebiantoro, U. (2007). Pengaruh Struktur Kepemilikan Saham, Leverage, Faktor Intern, dan Faktor Ekstern terhadap Nilai Perusahaan. *Jurnal Manajemen Dan Kewirausahaan*, *9*(1), 41–48. https://doi.org/10.9744/jmk.9.1.pp. 41-48

Sulimany, H. G., Ramakrishnan, S., Chaudhry, A., & Bazhair, A. H. (2021). Impact of Corporate Governance and Financial Sustainability on Shareholder Value. *Studies of Applied Economics*, *39*(4), 1–17. https://doi.org/10.25115/eea.v39i4.4318

Susanto, E., & Indrabudiman, A. (2023). Pengaruh Good Corporate Governance dan Corporate Social Responsibility terhadap Nilai Perusahaan dengan Kinerja Keuangan sebagai Variabel Intervening. *Jurnal Keuangan Dan Perbankan*, *19*(2), 69–80. https://doi.org/10.35384/jkp.v19i2.386

Trikarinaputri, E. (2025, Februari 22). *BCA Catat 4 Miliar Serangan Siber ke Sistem Perbankan pada 2024*. Tempo. https://www.tempo.co/ekonomi/bca-catat-4-miliar-serangan-siber-ke-sistem-perbankan-pada-2024-1210740

Yamada, R. (2024). Impact of Cybersecurity Regulations on Corporate Compliance Practices in Japan. *International Journal of Law and Policy*, *9*(2), 28–38. https://doi.org/10.47604/ijlp.2705

Yani, N. P. T., & Suputra, I. D. G. D. (2020). Pengaruh Kepemilikan Asing, Kepemilikan Institusional dan Leverage terhadap Pengungkapan Corporate Social Responsibility. *E-Jurnal Akuntansi*, *30*(5), https://doi.org/1196–1207. 10.24843/EJA.2020.v30.i05.p10

Yanti, N. L. E. K., Endiana, I. D. M., & Pramesti, I. G. A. A. (2021). Pengaruh Ukuran Perusahaan, Ukuran Dewan Komisaris, Kepemilikan Institusional, Leverage, dan Profitabilitas terhadap Pengungkapan Corporate Social Responsibility. *Jurnal KHARISMA*, *3*(1), 42–51.

Zhang, X., Taylor, D., Qu, W., & Wise, V. (2013). Institutional Ownership, Audit Committee and Risk Disclosure – Evidence from Australian Stock Market. *Corporate Board: Role, Duties and Composition, 9(3),* 66–81. https://doi.org/10.22495/cbv9i3art6