Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6, 6090-6104
2024
Publisher: Learning Gate
DOI: 10.55214/25768484.v8i6.3328

Cybersecurity disclosure and audit fees: An empirical study of listed companies on the Indonesia stock exchange

Susanto[1*], Gatot Soepriyanto[2]
[1]Department of Accounting, School of Accounting - Master of Accounting, Bina Nusantara University, Jakarta 11480, Indonesia; susanto010@binus.ac.id (S.)
[2]Accounting Department, School of Accounting, Bina Nusantara University, Jakarta, Indonesia; gsoepriyanto@binus.edu (G.S.)

Abstract: Cyber attacks on companies cause substantial financial and non-financial losses for all countries, including Indonesia. This empirical study was conducted to identify how cybersecurity risk disclosure (CRD) affects audit fees. This initial study analyzes cybersecurity risk disclosure across all company sectors on the Indonesia Stock Exchange (IDX) list. The current research continues the study of Calderon & Gao (2021) by combining keywords with the research of Li et al. (2018), which were collected manually to extract cybersecurity risk disclosure. During 2019-2023, our sample consisted of 172 companies with 860 observations, and the data obtained is then analyzed using the Stata application. The results show that cybersecurity risk disclosure significantly affects audit fees. This statement indicates that the more words in the cybersecurity risk disclosure, the more the audit fees the company must pay the external auditor tend to increase. When auditors assess a high risk, they need more time to conduct a more in-depth examination so that audit costs increase.

Keywords: *Audit fees, Cybersecurity disclosures, Cybersecurity key words, Cybersecurity, Indonesia stock exchange.*

1. Introduction

Digital transformation is vital in facilitating economic growth towards sustainability in the digital era [1]. Its impact goes beyond just the technological aspect but also impacts business strategy and the overall economic paradigm [1]. This digital transformation not only reflects technological advances but also leads to significant changes in the way companies present and manage financial information. This digital change is evident from the rising investment of companies in software, which is a significant factor in digital transactions. Thus, companies are trying to meet market demand through accelerating digital transformation, which is linear with improving the financial performance of banking companies listed on the IDX [2]. The automated nature of digital technology allows for simplifying and accelerating various tasks that previously required human intervention, such as recording transactions, processing data, and preparing financial reports. However, implementing digital technology also brings significant challenges, primarily related to the security and privacy of company data [3].

Cybercrime cases in Indonesia have attacked various business sectors. Cybersecurity cases increased by 40% in 2019 and more than 77% in 2023. Indonesia is ranked 5th in Southeast Asia, and out of 176 countries, Indonesia is ranked 48th with a cybersecurity index of 64% [4]. Several cases of data breaches have occurred in several banks and companies. In October 2021, news emerged that Bank Jatim was suspected of experiencing a customer data leak. Based on the news, Bank Jatim's customer data was traded on a hacker forum for USD 250 thousand, equivalent to IDR 3.5 billion [5]. It was recorded that general banks in Indonesia experienced losses of IDR 246.5 billion, the possible loss of general banks was IDR 208.5 billion and recovery costs were IDR 302.5 billion [6]. On March 20, 2020, Tokopedia was successfully attacked by hackers, which caused data leaks on 15 million users, the database (which was hacked) including email, password hash, and name [7].

As cybersecurity risks change, it is essential for auditors to continually evaluate the potential for cybersecurity incidents to have a notable consequence in the financial statement disclosure. According

* Correspondence: susanto010@binus.ac.id

to the Center for Audit Quality [8], involvement of external auditors includes two critical contexts, namely, the audit of the company's financial position and the evaluation of internal control over financial reporting and disclosure. Securities and Exchange Commission (SEC) adopted regulations requiring public companies to make specified cybersecurity disclosures. These regulations are designed to produce consistent, comparable, and decision-making-friendly disclosures. The mandatory annual disclosures regarding the company's governance and risk management concerning cybersecurity risks, including the board's oversight of cybersecurity risks, are based on new disclosure items required in Form 10-K and Form 20-F.

High or low audit fees are determined through a negotiation process between stakeholders and the Public Accounting Firm that carries out the audit by considering various factors. The research results by Fisabilillah, Fahria, and Praptiningsih (2020) [9] and Vinidita and Ghozali (2021) [10] stated that there is no significant influence between audit risk and audit fees. Meanwhile, the research results by Mundiroh and Khikmah (2021) [11] stated that audit risk affects audit fees. Research conducted by Anggara, Suhendro, and Siddi (2021) [12] and Amelia et al. (2022) [13] stated that the complexity of a company can significantly affect audit fees. However, according to research conducted by Nisa and Triyanto (2022) [14], complexity does not affect the determination of audit fees. In addition, there is also disclosure of cybersecurity risks. Calderon and Gao (2020) [15] and Karyani et al. (2023) [16] found that overall disclosure of cybersecurity risks can affect audit fees.

CRD can significantly impact audit costs because higher risks can drive more processes of organizing audit design and testing to justify that the financial reporting on internal control is correct without arranging. Internal control systems that contain Arrangements are acts of errors or fraud that can result in higher and material misstatements. In addition, cybersecurity threats can have significant implications for the effectiveness of internal control in the future. Auditors need to design and perform various procedures to assess audit risk; they identify that cybersecurity-related risks significantly impact the company's financial statements [15].

The existence of cybersecurity issues that require auditors to conduct more comprehensive testing has an impact on increasing audit costs because there is an increase in inherent risk and control risk in the company, requiring auditors to reduce detection risk by conducting more detailed testing (Hogan & Wilkins, 2008) in (Calderon & Gao, 2020) [15]. The number of words clients use in CRD can affect audit costs [15]. Similar results in Karmelina (2021) [17] study stated that the increasing amount of content (number of words) in CRD can increase the determination of audit fees that need to be paid by the company.

This study is also similar to the study conducted by Karmelina (2021) [17]. Karmelina (2021) [17] revealed cybersecurity risks with keywords developed in the 2020 Héroux & Fortin study. This study combined keywords that refer to keywords in the disclosure of cybersecurity risks developed in the study of Gordon et al. (2010) [18] and those developed by Li et al. (2018) [19]. Karmelina (2021) [17] study has limitations because it does not use control variables. Other variables can influence audit costs; the research results will be more accurate if there are control variables. Another limitation is the focus of the object, which only covers banking companies listed on the IDX. However, the banking sector is not the only one that utilizes information technology in its operational activities.

In recent years, cyberattacks have been increasingly prevalent in Indonesia. Both individuals, private companies, and government institutions have become cybercrime targets. Nearly 6 million cyber threats were recorded during the first quarter of 2024 [21]. In this new era of cyber transparency, the SEC has released new regulations requiring company management to disclose how they manage cybersecurity risks and threats as part of their reporting responsibilities, which investors can use to make informed decisions [22]. The board and audit committees will turn to the internal audit function to gain an independent perspective on whether their company's cybersecurity risk mitigation strategies and programs are robust and aligned with their objectives and to ensure the organization is ready to comply with the new disclosure requirements [23]. One independent external audit assessment aspect is the company's internal controls. External auditors may face higher audit complexities with the new cybersecurity disclosure rules. Research conducted by [12] and [13] indicates that a company's complexity can significantly affect audit costs, while a study [14] suggests that complexity does not

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 6090-6104, 2024
DOI: 10.55214/25768484.v8i6.3328

influence the determination of audit fees. The contribution of this study is to provide empirical evidence on the impact of cybersecurity disclosures on audit costs in the annual reports of companies listed on the IDX. This study's findings can benefit both internal and external auditors and the management of companies listed on the IDX. This research opens a new avenue for investigating the relationship between cybersecurity disclosures and audit costs—an area not explored before in IDX-listed companies.

2. Literature Review

Previous studies have shown that cybersecurity disclosure and audit fees are related (Calderon & Gao, 2020 [15]; Smith et al., 2019 [20] ; Rosati et al., 2019 [24]). Information security has become critical in business operations (Gordon et al., 2010) [18]. Companies of all sizes face daily cybersecurity risks (Bendovschi, 2015) [25]. Currently, most companies view cybersecurity as critical, which can ultimately impact audit quality and the reliability and integrity of financial reporting (Calderon & Gao, 2020) [15]. Cybersecurity breaches can result in significant financial losses for companies (Gao et al., 2020) [26].

Cybersecurity disclosure can be through 10k content (Word Count), language readability, and litigation language [15]. Empirical findings show that a company's audit fees are influenced by the word count content, readability and litigation disclosed in the CRD (Calderon & Gao, 2020) [15]. Similar results in Karmelina's (2021) [17] study stated that more content (word count) in cybersecurity risk disclosure could increase the audit fees needed by banking companies listed on the IDX. Researchers also believe that the more disclosure, the greater the auditor's effort to assess the implications of audit risk. Therefore, researchers expect an effect of cybersecurity risk disclosure on audit fees. According to the previous discussion, the researcher's hypothesis is as follows:

Hypothesis 1: Cybersecurity risk disclosure affects audit fees.

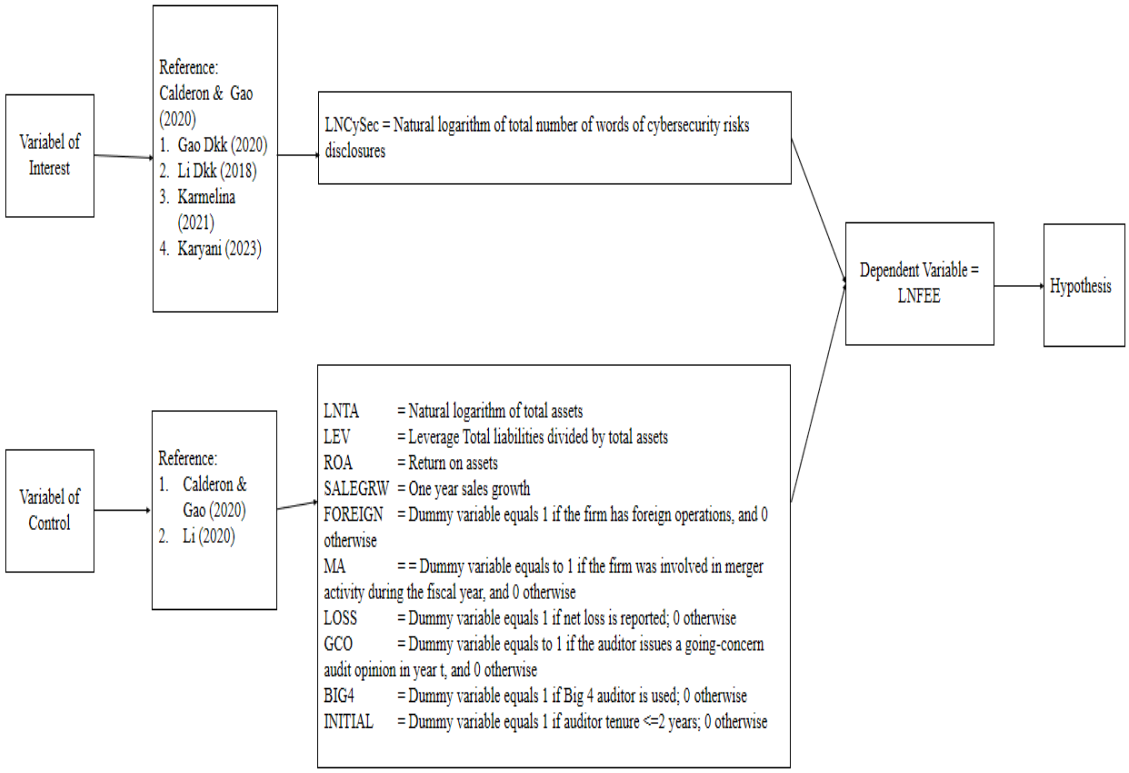

Figure 1.
Research model.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 6090-6104, 2024
DOI: 10.55214/25768484.v8i6.3328

3. Research Methodology

3.1. Sample Collection and Data Collection

The final sample consists of 860 observations from 172 companies listed on the IDX from 2019 to 2023. Data were collected from the English version of the annual report available on the official IDX website, and the company's official website. The sampling method in this study used purposive sampling technique.

3.2. Variables Description

Variabel independent. Cybersecurity disclosure is how companies inform stakeholders about cybersecurity policies, strategies, and risks. Cybersecurity risk disclosure can be collected from the company's annual report in the from of the total of words to measure the variable Gao, Calderon, & Tang (2020) [26]. This variable is measured from the natural logarithm (LNPumber of Words). This study focuses on CRD based on the keywords identified by Gordon et al. (2010) [18] and Li et al. (2018) [19]. Keywords Used in this Study are attached: 1. Keywords were collected using https://voyant-tools.org/ with electronic counts.

Variabel dependent. Audit fees are the service fees received by Public Accountants after carrying out audit services. The fees usually depend on, among other things, the risk, complexity, level of expertise, audit fee structure and the KAP carrying out the services.

Variabel Control. Furthermore, control variables are used based on previous research, including LNTA, LEV, ROA, and SALEGRW. Control variables can use dummy variables, including FOREIGN, MA, LOSS, GCO, BIG 4, and INITIAL.

Table 1.
Variables description.

Dependent variable:
LNFEE = The natural log of audit fees;
Independent variables:
LNCySec = The natural log of total word count of CRD
Independent control variables:
LNTA = The natural log of total assets
LEV = Ratio Leverage
ROA = Ratio Return on Assets
SALEGRW = 1 year sales growth
FOREIGN = A value of 1 is given if the company has operations abroad, a value of 0 is given if it does not.
MA = A value of 1 is given if the company carries out a business merger, a value of 0 is given if it does not.
LOSS = A value of 1 is given if the company's income statement reports a net loss, and 0 is given if it does not.
GCO = A value of 1 is given if the auditor provides a going-concern opinion on the report of year t; a value of 0 is given if not.
BIG 4 = A value of 1 is given if the auditor used is from the Big 4, a value of 0 is given if not.
INITIAL = A value of 1 is given if the auditor's tenure is less than or equal to 2 years; a value of 0 is given if not.

3.3. Analytical Methods

The data in this study were analyzed using the Stata application. This study uses a quantitative research method. Data analysis used panel data because the observations covered several companies (cross-section) and five years (time series). The regression model used is based on the hypothesis to be tested:

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 6090-6104, 2024
DOI: 10.55214/25768484.v8i6.3328

Model = $LNFee = \alpha + \alpha_1 LNCySec_{it} + \alpha_2 LNTA_{it} + \alpha_3 LEV_{it} + \alpha_4 ROA_{it} \alpha_5 SALEGRW_{it} + \alpha_6 FOREIGN_{it} + \alpha_7 MA_{it} + \alpha_8 LOSS_{it} + \alpha_9 GCO_{it} + \alpha_{10} BIG4 + \alpha_{11} INITIAL_{it} + \varepsilon_{it}$

4. Result and Discussion of Findings

4.1. Descriptive Statistics

This study focuses on companies listed on the IDX. The sample used was 172 companies based on the purposive sampling technique. From the available results, the total population was 926 companies, of which 610 did not disclose audit fees in the 2019-2023 annual report. Meanwhile, 140 companies did not disclose cybersecurity in the 2019-2023 annual report. Four companies had annual reports that could not detect cybersecurity disclosures, including GMTD, HDTX, PICO, and REAL, from the number of companies included in the criteria, namely 172 companies, multiplied by the research period, which lasted for five years.

Tables 2 and 3 show the outcome of descriptive statistics of the variables in this study. LNFEE is measured by the natural logarithm of the audit fees disclosed in the annual report. Based on the descriptive analysis of the LNFEE variable, the average value (mean) before using the natural logarithm was Rp3,145,868,341.-, while the average value (mean) after using the natural logarithm was 20.88107. This value can be interpreted that the average amount of audit fees incurred for audit services in the companies that are the samples of this study is Rp3,145,868,341,-, or 20.88107, and the standard deviation before using the natural logarithm was Rp9,057,763,583.- while the standard deviation value after using the natural logarithm was 1.218101. The comparison between the mean and standard deviation values is Rp3,145,868,341.- > Rp9,057,763,583.- or 20.88107 > 1.218101 where the mean has a higher value (>) than the standard deviation value, indicating that audit costs experience high distribution and fluctuation. Meanwhile, the Median before using the natural logarithm is Rp1,090,000,000.- while after using the natural logarithm, it is 20.8094. The minimum value for this variable before using the natural logarithm is Rp100,000,000.-, while the minimum value after using the natural logarithm is 18.42068. Moreover, the maximum value before using the natural logarithm is Rp120,000,000,000.-, while the maximum value after using the natural logarithm is 25.51076. For the LNCySec variable, the logarithm of the word count disclosure in the annual reports is used, in line with the research of Calderon and Gao (2020), who used the logarithm of the word count disclosure in the 10-k filings report.

Based on the results of identifying items using keywords collected using https://voyant-tools.org/ attached in Appendix 2, the keywords that often appear in the annual reports of this research sample are business continuity, which is 8405 words, information security as many as 2741 words, cyber security as many as 2107 words, disaster recovery as many as 1572 words, security management as many as 1110 words, cybersecurity as many as 1084 words, cyber risk as many as 422 words, system security as many as 281 words, phishing as many as 217 words, security monitoring as many as 208 words, network security as many as 199 words, cyber attack as many as 195 words, information technology security as many as 188 words, authentication as many as 181 words, malware as many as 175 words, confidential data as many as 173 words, hacker as many as 157 words, data confidentiality as many as 133, hacking as many as 125 words, confidentiality of data as many as 124 words, access control as many as 107 words, security incident as many as 101 words, cyber threat and encryption as many as 95 words, cyber incident as many as 93 words, ransomware as many as 87 words, social engineering as many as 73 words, intrusion as many as 58 words, unauthorized access as many as 32 words, cyber-based attack as many as 31 words, computer security as many as 27 words, denial of service as many as 26 words, security breach as many as 24 words, data theft as many as 20 words, data breach as many as 17 words, cyber fraud as many as 15 words, infosec as many as 14 words, cyber insurance as many as 9 words, espionage and computer virus as many as 5, security measure as many as 4 words, corruption of data as many as 2 words. At the same time, keywords such as computer attack, computer intrusion, computer system security, computer break-in, crimeware, computer breach, cyber-terrorist, cyber-threat, cyber-terrorist, cyber-security, cyber-risk, cyber-insurance, cyber-incident data corruption, information technology attack, keylogger, network break-in, cyber-attack, cyber-fraud, and security expenditure are 0 words. According on the outcome of the data displayed in Table 2 and Table 3, the LNCySec variable

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 6090-6104, 2024
DOI: 10.55214/25768484.v8i6.3328

obtained an average value (mean) before using the natural logarithm of 24.1127907, while after using the natural logarithm it was 2.55641. The standard deviation before using the natural logarithm was 32.35304484, while after using the natural logarithm it was 1.113222. At the same time, the median value before using the natural logarithm was 12.5, while after using the natural logarithm, it was 2.524928. The minimum value for this variable before using the natural logarithm is 2, while after using the natural logarithm, it is .6931472. Moreover, the maximum value before using the natural logarithm is 282; after using the natural logarithm, it is 5.641907.

Table 2.
Descriptive statistics.

Variable	Obs.	Mean	Std. dev.	Median	Min.	Max.
LNFEE	860	20.88107	1.218101	20.8094	18.42068	25.51076
LNCySec	860	2.55641	1.113222	2.524928	0.6931472	5.641907
LNTA	860	29.89419	1.891664	29.6805	24.15394	35.31545
LEV	860	0.5775537	0.3241551	0.5636302	0.0274889	2.471253
ROA	860	0.0234799	0.1114129	0.019017	-0.9488978	0.5993045
SALEGRW	860	0.1293344	0.5966194	0.049193	-0.9155377	6.189807
FOREIGN	860	0.1139535	0.3179397	0	0	1
MA	860	0.0104651	0.1018217	0	0	1
LOSS	860	0.1930233	0.3949008	0	0	1
GCO	860	0.1976744	0.3984769	0	0	1
BIG4	860	0.4837209	0.5000257	0	0	1
INITIAL	860	0.2232558	0.4166708	0	0	1

Description:
LNFee = Audit fee
LNCySec = The natural logarithm of the total number of words of cybersecurity risk disclosure
LNTA = The natural logarithm of total assets
LEV = Leverage
ROA = Return on assets
SALEGRW = One-year sales growth
FOREIGN = A value of 1 is given if the company has operations abroad, a value of 0 is given if it does not.
MA = A value of 1 is given if the company carries out a business merger, a value of 0 is given if it does not.
LOSS = A value of 1 is given if the company's income statement reports a net loss, and 0 is given if it does not.
GCO = A value of 1 is given if the auditor provides a going-concern opinion on the report of year t; a value of 0 is given if not.
BIG4 = A value of 1 is given if the auditor used is from the Big 4, a value of 0 is given if not.
INITIAL = A value of 1 is given if the auditor's tenure is less than or equal to 2 years; a value of 0 is given if not.

Table 3.
Descriptive statistics data before data transformation.

Variable	FEE (Rp)	CySec (Word)	TA (Rupiah)
Obs.	860	860	860
Mean	3,145.,868,341	24.1127907	65,299,432,864,903
Sd.	9,057,763,583	32.35304484	223,710,093,657,553
Median	1,090,000,000	12,5	7,763,818,606,419
Min.	100,000,000	2	30,897,597,001
Max.	120,000,000,000	282	2,174,219,449,000,000

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 6090-6104, 2024
DOI: 10.55214/25768484.v8i6.3328

4.2. Result

4.2.1. Test of Determination Coefficient

The determination test can be seen in Table 4, with an R-Square (R2) value of 0.1157. This value can be explained by the influence of the variables LNCySec, LNTA, LEV, ROA, SALEGRW, FOREIGN, MA, LOSS, GCO, BIG4 and INITIAL on audit fees (Audit Fee) in companies listed on the IDX is 0.1157 or 11.57%. Thus, it can be concluded that the ability of the cybersecurity risk disclosure variable (CySec) on audit fees (Audit Fee) with LNTA, LEV, ROA, SALEGRW, FOREIGN, MA, LOSS, GCO, BIG4 and INITIAL as control variables can explain the audit fee variable (Audit Fee) by 11.57% while other factors influence the rest.

Table 4.
Results of the R-square test.

Number of obs.	860
R-Squared (Within)	0.1157
R-Squared (Between)	0.6475
R-Squared (Overall)	0.6097

Table 5.
Results of partial regression test (t-test).

Variabel	**Regression model**				
	Fixed effect model				
	Predicted sign.	**Coefficients**	**Std. err.**	**t**	**Prob.**
Cons.		1.616.438	2.00181	8.07	0.000
LNCySec	+	0.1146513	0.0237267	4.83	0.000**
LNTA	+	0.1398401	0.066872	2.09	0.038*
LEV	-	-0.018137	0.1023315	-0.18	0.860
ROA	-	0.059107	0.128963	0.46	0.647
SALEGRW	-	0.018559	0.0221888	0.84	0.404
FOREIGN	+	0.252207	0.0403672	6.25	0.000**
MA	-	-0.0463513	0.0761599	-0.61	0.544
LOSS	-	-0.0221795	0.0457998	-0.48	0.629
GCO	-	-0.0323182	0.0545905	-0.59	0.555
BIG4	+	0.4878585	0.1207169	4.04	0.000**
INITIAL	-	-0.0165347	0.0330046	-0.50	0.617
Number of Obs.		860			
Adjusted R-squared (Within)		0.1157			
sig. F(10,171)		0.0000			

4.2.2. Partial Regression Test (t-Test)

Description:
*significance 5%
**significance 1%
LNFee = Audit fee
LNCySec = The natural logarithm of the total number of words of cybersecurity risk disclosure
LNTA = The natural logarithm of total assets
LEV = Ratio Leverage
ROA = Ratio Return-on-assets
SALEGRW = 1 year sales growth
FOREIGN = A value of 1 is given if the company has operations abroad, a value of 0 is given if it does not.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 6090-6104, 2024
DOI: 10.55214/25768484.v8i6.3328

MA = A value of 1 is given if the company carries out a business merger, a value of 0 is given if it does not.

LOSS = A value of 1 is given if the company's income statement reports a net loss, and 0 is given if it does not.

GCO = A value of 1 is given if the auditor provides a going-concern opinion on the report of year t; a value of 0 is given if not.

BIG4 = A value of 1 is given if the auditor used is from the Big 4, a value of 0 is given if not.

INITIAL = A value of 1 is given if the auditor's tenure is less than or equal to 2 years; a value of 0 is given if not.

This study hypothesises that cybersecurity risk disclosure has a significant positive effect on audit fees. The regression results for Table 5 consistently show the magnitude of the t-count value for the LNCySec variable, which is 4.83, which indicates a positive value. This shows that the t-count is greater (>) t-table (4.83 is more significant than (>) 1.96), so there is an influence between the LNCySec variable and LNFee. In addition, the probability level shows a value of 0.000, which is lower (<) than the significance level of 0.05 (0.000 is smaller (<) 0.05), which confirms that there is a significant influence. The results of this test indicate an influence of the cybersecurity risk disclosure variable on the audit fee variable in companies listed on the IDX in 2019-2023.

Meanwhile, the test results of the control variables show that LNTA has a t-value of 2.09 with a level of significance is 0.038. LEV shows a t-value of -0.18 with a level of significance is 0.860. ROA shows a t-value of 0.46 with a level of significance is 0.647. SALEGRW shows a t-value of 0.84 with a level of significance is 0.404. FOREIGN shows a t-value of 6.25 with level of significance is 0.000. MA shows a t-value of -0.61 with a significance level of 0.544. LOSS shows a t-value of -0.48 with a level of significance is 0.629. GCO shows a t-value of -0.59 with a level of significance is 0.555. BIG4 shows a t-value of 4.04 with a level of significance is 0.000. Moreover, the INITIAL control variable results show a t-count value of -0.50 with a level of significance is 0.617.

Based on the results of the ten control variables above, there are only three control variables, namely LNTA, FOREIGN and BIG4, which significantly affect audit fees. Where the results show a t-count value more significant than (>) ttable (1.96) and the probability value is lower (<) compared to the level of significance (0.05)

4.2.3. Partial Regression Test (Simultaneous F Test)

Based on table 5 containing the outcomes of the F-Square test, the probability value is 0.000 <0.05. This demonstrates a simultaneous or joint influence between the independent variables, namely LNCySec, LNTA, LEV, ROA, SALEGRW, FOREIGN, MA, LOSS, GCO, BIG4 and INITIAL on LNFEE. In this study, LNCySec, LNTA, LEV, ROA, SALEGRW, FOREIGN, MA, LOSS, GCO, BIG4 and INITIAL simultaneously influence the LNFEE variable.

5. Discussion

The regression model applied in this study is outlined below:

$$LNFee = 16.16438 + .1146513\ LNCySec_{it} + .1398401 LNTA_{it} + -.018137 LEV_{it} + .059107 ROA_{it} + .018559 SALEGRW_{it} + .252207 FOREIGN_{it} + -.0463513 MA_{it} + -.0221795 LOSS_{it} + -.0323182 GCO_{it} + .4878585 BIG4 + -.0165347 INITIAL_{it} + \varepsilon_{it}$$

The equation represents that the LNCySec variable, namely cybersecurity risk disclosure, significantly affects the LNFee variable, namely audit fees. Meanwhile, the control variables, namely LNTA, FOREIGN, and BIG4, significantly affect LNFEE. At the same time, the control variables, namely LEV, ROA, SALEGRW, MA, LOSS, GCO and INITIAL, do not significantly affect LNFEE.

The findings from the partial test indicate an influence on the variable number of words in CRD on audit costs. A smaller t-count value indicates this compared to the t-table value (4.83> 1.96) and a higher p-value for the variable test (0.0000 <0.05).

This study's findings reveal a positive correlation between CRD and audit fees. Thus study has proved that the proposed hypothesis can be accepted, that is to say that there is an influence between the variable number of CRD words on audit fees. Consistent with agency theory, the results show that the

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 6090-6104, 2024
DOI: 10.55214/25768484.v8i6.3328

extent of risk disclosure can affect the audit costs incurred because it can increase the scope of work the auditor must complete. The perceived level of risk associated with the company's operations can affect audit fees, with auditors tending to charge higher costs if the auditor can assess the risk of the company's cybersecurity disclosure.

The number of cybersecurity risk disclosure words in this study identifies items using keywords collected using https://voyant-tools.org/ with electronic counts on the annual report. The more words in a cybersecurity risk disclosure in a annual report, the more influence it has in increasing audit costs.

The study's outcomes align with research conducted by previous researchers. The outcomes of this research are no different from the research of Calderon and Gao (2020) [15], which states that the number of words in the CRD affects the amount of audit fees to be paid. Total disclosure, causes, and impacts of cyber risk are directly related to audit fees (Karyani et al., (2023) [16]. Furthermore, Karmelina (2021) [17] states that the greater the number in the CRD, the greater the determination of audit fees that need to be paid by the company.This is because auditors can use cybersecurity risk disclosure in the company's annual report as a source for assessing company risk. When auditors assess a high risk, they need more time to conduct a more in-depth examination so that audit costs increase.

Rosati, Gogolin, and Lynn (2019) [24] stated that the increase in audit service fees that occurs in the year of a cyber breach is temporary. Before the incident, auditors have anticipated cybersecurity risks in their audit risk assessment. The higher the cybersecurity risk, the higher the cost that the company must pay auditors. Li, No, and Boritz (2020) [27] also stated that companies facing cyber incidents in the current period experience a more significant increase in audit service fees.

This study's findings practically show that audit costs are significantly affected by these factors; this indicates that cybersecurity disclosure can affect audit costs because cybersecurity disclosure in the annual report is a source of information to assess the company's risk. Thus, the company's inherent risk and control risk can increase, requiring auditors to minimize detection risk through more detailed testing. When auditors assess high risk in auditing clients, auditors need to conduct complex examinations or situations requiring a high level of judgment, thus requiring more time and increasing audit costs.

The existence of cybersecurity issues that require auditors to conduct more comprehensive testing has an impact on increasing audit costs because there is an increase in inherent risk and control risk within the company, requiring auditors to reduce detection risk by conducting more detailed testing [15]. The number of words clients use in CRD can affect audit costs [15]. Similar results in Karmelina's (2021) [17] study stated that the increasing number of words in CRD can increase the determination of audit fees that need to be paid by the company.

6. Conclusion

This study investigates empirical evidence on the effect of CRD on audit fees. The findings indicate that CRD significantly affects audit fees. This statement disloses that the more words in the cybersecurity risk disclosure, the higher the audit fee the company must pay the external auditor. The control variables LNTA, FOREIGN and BIG4 affect audit fees. Meanwhile, the control variables LEV, ROA, SALEGRW, MA, LOSS, GCO, and INITIAL do not affect audit fees.

7. Limitation

This study has limited data on the inclusion of audit fees, which are still voluntary in the company's annual report, so not all companies include the amount of audit fees given to auditors. The company lists audit fees and other professional fees so that the data cannot be used as research data. Some annual reports cannot be found on the IDX site or the company's official website. There are several PDF files of company annual reports with low quality, so it is not possible to count the number of words in cybersecurity disclosure. This study only uses annual report data with an observation period of 2019 to 2023 (5 years). The results obtained may be different if a more extended period is used.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 6090-6104, 2024
DOI: 10.55214/25768484.v8i6.3328

References

[1] Togatorop, A., Darmawan, D., & Hidayati, R. (2024). 'Transformasi Digital Dalam Mencapai Keberlanjutan Di Bidang Ekonomi Dan Keuangan' in Manajemen Business Innovation Conference 2024: *Optimalisasi UMKM Melalui Transformasi Digital*, Pontianak, Indonesia.

[2] Lantip, S., & Daljono. (2023). 'Pengaruh Transformasi Digital Terhadap Kinerja', *Diponegoro Journal Of Accounting*, Vol 12, [online]. Available: http://ejournal-s1.undip.ac.id/index.php/accounting.

[3] Salsabila, D., & Rahman, A. (2023). 'Pengaruh Teknologi Digital Terhadap Bidang Akuntansi Pada Perusahaan Swasta' in Konferensi Nasional Ilmu Administrasi 7.0: *Memperkokoh Pembangunan Bangsa Melalui Penguatan Nilai Publik Yang Berdampak Dalam Manapaki Indonesia Berdaulat, Maju, dan Mandiri*. 7 September 2023. Bandung, Indonesia.

[4] Patria, W. (2024). *Ancaman Siber Meningkat, Wamenkominfo Tekankan Pelindungan Data Pribadi*. [online]. Available: Https://Www.Kominfo.Go.Id/Content/Detail/55668/Siaran-Pers-No-243hmkominfo032024-Tentang-Ancaman-Siber-Meningkat-Wamenkominfo-.

[5] Pratama, G. (2023). *Perbankan RI Sasaran Empuk Serangan Siber, Ini Faktanya*. [online]. Available: Https://Infobanknews.Com/Perbankan-Ri-Sasaran-Empuk-Serangan-Siber-Ini-Faktanya/.

[6] Bestari, N. (2021). *Serangan Siber Hacker Jahat Bikin Bank Tekor Rp 246,5 Miliar*. [online]. Available: Https://Www.Cnbcindonesia.Com/Tech/20211028133440-37-287239/Serangan-Siber-Hacker-Jahat-Bikin-Bank-Tekor-Rp-2465-Miliar.

[7] Iqbal, M. (2020). *Beredar Isu 15 Juta Akun Pengguna Tokopedia Bocor, Apa Benar?* [online]. Available: Https://Www.Cnbcindonesia.Com/Tech/20200502221818-37-155860/Beredar-Isu-15-Juta-Akun-Pengguna-Tokopedia-Bocor-Apa-Benar.

[8] The Center For Audit Quality. (2020). *The Role Of Auditors In Non-Gaap Financial Measures And Key Performance Indicators: Present And Future*. [online]. Available: https://www.thecaq.org/wp-content/uploads/2020/09/2020_09_caq-role-of-the-auditor-non-GAAP-and-KPIs.pdf.

[9] Fisabilillah, P., Fahria, R., & Praptiningsih. (2020). 'Pengaruh Ukuran Perusahaan, Risiko Perusahaan, Dan Profitabilitas Klien Terhadap Audit Fee', *Jurnal Ilmiah Akuntansi Kesatuan*, Vol. 8. [online]. Available: https://doi.org/10.37641/jiakes.v8i3.388.

[10] Vinidita, G., & Ghozali, I. (2021). 'Pengaruh Risiko Audit Terhadap Biaya Audit Eksternal Di Indonesia', Diponegoro Journal of Accounting, Vol. 10, No. 4, pp.1-15 [online]. Available: https://ejournal3.undip.ac.id/index.php/accounting/article/view/32978/26343.

[11] Mundiroh, & Khikmah, S. (2021). 'Analisis Faktor-Faktor Yang Mempengaruhi Fee Audit Eksternal', *Borobudur Accounting Review*, Vol. 1, No.1, pp. 46-56, DOI: 10.31603/bacr.4931.

[12] Anggara, D., Suhendro, & Siddi, P. (2021). 'Faktor-Faktor Yang Mempengaruhi Audit Fee Perusahaan Pertambangan Yang Terdaftar Di Bei Tahun 2014-2019', *Jurnal Ilmiah Akuntansi*, Vol. 18 [online]. Available: https://doi.org/10.46306/rev.v3i2.210.

[13] Amelia, R., Abbas, D., Hamdani, & Hakim, M. (2022). 'Pengaruh Kompleksitas Perusahaan, Jenis Industri, Profitabilitas Klien, Ukuran Perusahaan Dan Komite Audit Terhadap Fee Audit', *Jurnal Mahasiswa Manajemen dan Akuntansi*, Vol. 1[online]. Available: https://doi.org/10.30640/jumma45.v1i2.331.

[14] Nisa, T., & Triyanto, D. (2022). *Pengaruh Ukuran Perusahaan, Kompleksitas Perusahaan, Profitabilitas, Dan Komite Audit Terhadap Fee Audit (Studi Empiris Pada Perusahaan Indeks Lq45 Yang Listed Di Bursa Efek Indonesia Periode 2016-2020)*. Unpubliashed theses, Universitas Telkom, Bandung, Indonesia.

[15] Calderon, T., & Gao, L. (2020). 'Cybersecurity Risks Disclosure And Implied Audit Risks: Evidence From Audit Fees', *International Journal of Auditing*, Vol. 25. [online]. Available: https://onlinelibrary.wiley.com/doi/epdf/10.1111/ijau.12209

[16] Karyani, E., Noveria, A., Faturohman, T., & Rahadi, R. (2023). 'Disclosures Of Cyber Exposure And Audit Fees: Evidence From Asean-4 Banking', *Corporate Governance and Organizational Behavior Review*, Vol 7, p. 299–312. [online]. Available: https://doi.org/10.22495/cgobrv7i4sip8.

[17] Karmelina, Y. (2021). *Pengaruh Cybersecurity Disclosure Terhadap Audit Fee Dengan Kompetensi Auditor Internal Sebagai Variabel Moderasi*. Unpubliashed theses, Universitas Pendidikan Indonesia, Bandung, Indonesia.

[18] Gordon, L., Loeb, M., & Sohail, T. (2010). 'Market Value Of Voluntary Disclosures Concerning Information Security', *MIS Quarterly*, Vol. 34, p. 567-594 [online]. Available: DOI: 10.2307/25750692.

[19] Li, H., No, W., & Wang, T. (2018). 'Sec's Cybersecurity Disclosure Guidance And Disclosed Cybersecurity Risk Factors', *International Journal of Accounting Information Systems*, Vol. 30, pp.40-55, DOI: 10.1016/j.accinf.2018.06.003.

[20] Smith, T., Higgs, J., Pinsker, R., Dull, R., Boritz, J., & Wang, T. (2019). 'Do Auditors Price Breach Risk In Their Audit Fees?', *Journal of Information Systems Forthcoming*, [online]. Available: https://ssrn.com/abstract=3234312.

[21] CNN (2024). *Indonesia Digempur 6 Juta Ancaman Siber di Awal 2024, Cek Modusnya*. [online]. Available: https://www.cnnindonesia.com/teknologi/20240603103200-185-1105033/indonesia-digempur-6-juta-ancaman-siber-di-awal-2024-cek-modusnya.

[22] SEC. (2023). *SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companie*. [online]. Available: https://www.sec.gov/newsroom/press-releases/2023-139.
[23] PWC. (2024). *Cybersecurity disclosures and the role of internal audit*. [online]. Available: https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/sec-final-cybersecurity-disclosure-rules/cybersecurity-and-internal-audit.html.
[24] Rosati, P., Gogolin, F., & Lynn, T. (2019). 'Audit Firm Assessments Of Cyber-Security Risk: Evidence From Audit Fees And Sec Comment Letters', *The International Journal of Accounting*, Vol. 54, p. 1950013. [online]. Available: https://doi.org/10.1142/S1094406019500136.
[25] Bendovschi, A. (2015). 'Cyber-Attacks – Trends, Patterns And Security Countermeasures', *Procedia Economics and Finance*, Vol. 28. [online]. Available: https://doi.org/10.1016/S2212-5671(15)01077-1.
[26] Gao, L., Calderon, T., & Tang, F. (2020, 9). 'Public Companies' Cybersecurity Risk Disclosures', *International Journal of Accounting Information Systems*, Vol. 38, p. 100468. [online]. Available: https://doi.org/10.1016/j.accinf.2020.100468.
[27] Li, H., No, W. G., & Boritz, J. (2020). Are External Auditors Concerned About Cyber Incidents? Evidence From Audit Fees. *International Journal Of Accounting Information Systems*.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 6090-6104, 2024
DOI: 10.55214/25768484.v8i6.3328

Appendix 1.

	Keywords based on previous research	No	Keywords that will be used in this research
Li et al.	Encryption	1	Encryption
	Computer (Virus|Breach|Break-In|Attack|Security)	2	Computer virus
		3	Computer breach
		4	Computer break-in
		5	Computer attack
		6	Computer security
	Security (Breach|Incident)	7	Security breach
		8	Security incident
	(Information|Network|Computer) Security	9	Information security
		10	Network security
		10	*
	Intrusion	11	Intrusion
	Hacking|Hacker	12	Hacking
		13	Hacker
	Denial Of Service	14	Denial of service
	Cyber(-|)(Attack|Fraud|Threat|Risk|Terrorist|Incident|Security)	15	Cyber-attack
		16	Cyber-fraud
		17	Cyber-threat
		18	Cyber-risk
		19	Cyber-terrorist
		20	Cyber-incident
		21	Cyber-security
		22	Cyber attack
		23	Cyber fraud
		24	Cyber threat
		25	Cyber risk
		26	Cyber terrorist
		27	Cyber incident
		28	Cyber security
	Cyber-based attack	29	Cyber-based attack
	Cybersecurity	30	Cybersecurity
	Infosec	31	Infosec
	System security	32	System security
	Information Technology (Security|Attack)	33	Information technology security
		34	Information technology Attack
	Data theft	35	Data Theft
	Phishing	36	Phishing
	Malware	37	Malware
	Data confidentiality	38	Data confidentiality
	Confidentiality of data	39	Confidentiality of data
	Confidential data	40	Confidential data
	Unauthorized access	41	Unauthorized access
	Data corruption	42	Data corruption
	Corruption of data	43	Corruption of data
	Network break-in	44	Network break-in
	Espionage	45	Espionage
	Cyber(-|)Insurance	46	Cyber-insurance

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 6090-6104, 2024
DOI: 10.55214/25768484.v8i6.3328

		47	Cyber insurance
	Data breach	48	Data breach
	Crimeware	49	Crimeware
	Ransomware	50	Ransomware
	Keylogger	51	Keylogger
	Keystroke logging	52	Keystroke logging
	Social engineering	53	Social engineering
Gordon et al. (2010)	Security measure	54	Security measure
	Authentication	55	Authentication
	Encryption	55	*
	Computer virus	55	*
	Security breach	55	*
	Disaster recovery	56	Disaster recovery
	Information security	56	*
	Network security	56	*
	Computer security	56	*
	Access control	57	Access control
	Intrusion	57	*
	Business continuity	58	Business continuity
	Security management	59	Security management
	Hacker	59	*
	Security monitoring	60	Security monitoring
	Denial of service	60	*
	Cyber security	60	*
	Cyber attack	60	*
	Security incident	60	*
	Infosec	60	*
	Security expenditure	61	Security expenditure
	Computer system security	62	Computer system security
	Cyber security	62	*
	Computer breach	62	*
	Computer intrusion	63	Computer intrusion

Note: *Double.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 6090-6104, 2024
DOI: 10.55214/25768484.v8i6.3328

Appendix 2.

No	Keywords to be used in research	Number of words appearing in the annual report
1	Encryption	95
2	Computer virus	5
3	Computer breach	0
4	Computer break-in	0
5	Computer attack	0
6	Computer security	27
7	Security breach	24
8	Security incident	101
9	Information security	2741
10	Network security	199
11	Intrusion	58
12	Hacking	125
13	Hacker	157
14	Denial of service	26
15	Cyber-attack	0
16	Cyber-fraud	0
17	Cyber-threat	0
18	Cyber-risk	0
19	Cyber-terrorist	0
20	Cyber-incident	0
21	Cyber-security	0
22	Cyber attack	195
23	Cyber fraud	15
24	Cyber threat	95
25	Cyber risk	422
26	Cyber terrorist	0
27	Cyber incident	93
28	Cyber security	2107
29	Cyber-based attack	31
30	Cybersecurity	1084
31	Infosec	14
No	Keywords to be used in research	Number of words appearing in the annual report
32	System Security	281
33	Information technology security	188
34	Information technology attack	0
35	Data theft	20
36	Phishing	217
37	Malware	175
38	Data confidentiality	133
39	Confidentiality of data	124
40	Confidential data	173
41	Unauthorized access	32
42	Data corruption	0
43	Corruption of data	2
44	Network break-in	0
45	Espionage	5
46	Cyber-insurance	0
47	Cyber insurance	9

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 6090-6104, 2024
DOI: 10.55214/25768484.v8i6.3328

48	Data breach	17
49	Crimeware	0
50	Ransomware	87
51	Keylogger	0
52	Keystroke logging	0
53	Social engineering	73
54	Security measure	4
55	Authentication	181
56	Disaster recovery	1572
57	Access control	107
58	Business continuity	8405
59	Security management	1110
60	Security monitoring	208
61	Security expenditure	0
62	Computer system security	0
63	Computer intrusion	0

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 6090-6104, 2024
DOI: 10.55214/25768484.v8i6.3328