AKURASI Jurnal Studi Akuntansi dan Keuangan
p-ISSN : 2720-9067
e-ISSN : 2685-1059
Program Studi Magister Akuntansi
Fakultas Ekonomi dan Bisnis
Universitas Mataram

CYBER SECURITY DISCLOSURE: THE ROLE OF STAKEHOLDER PRESSURE AND GOVERNANCE QUALITY

Muhammad Fadhly Rizky Octavio[1*], Noorfaiz Athallah Koeswandana[2]
Accounting Department, Universitas Islam Indonesia, Yogyakarta [12]
Corresponding author: fadhlyvio@uii.ac.id

ARTICLE INFORMATION

Article history:
Received: 23/02/2026
First Revision:5/03/2026
Accepted: 16/04/2026
Available online:30/06/2026

ABSTRAK

Penelitian ini mengkaji pengaruh Customer Pressure (CP), Public Digital Pressure (PDP), dan Corporate Governance Quality (CGS) terhadap Cyber Security Disclosure (CSD) pada sektor perbankan Indonesia. Menggunakan pendekatan kuantitatif data panel, penelitian ini menganalisis 115 observasi dari bank yang terdaftar di Bursa Efek Indonesia periode 2020–2024. CSD diukur melalui analisis frekuensi kata menggunakan Voyant Tools, CP dengan total simpanan nasabah, PDP dengan skor Google Trends, dan CGS dengan Management Score dari LSEG. Regresi data panel dengan uji robustness melalui regresi variabel lag dan Propensity Score Matching digunakan sebagai metode analisis. Hasil penelitian menunjukkan bahwa CP, PDP, dan CGS berpengaruh positif dan signifikan terhadap CSD. Perbedaan pola pengungkapan antara bank milik negara dan non-milik negara turut teridentifikasi. Temuan ini memperluas teori legitimasi pada konteks keamanan siber di perbankan negara berkembang sekaligus memvalidasi Google Trends sebagai proksi tekanan digital publik.

Kata Kunci: Pengungkapan Keamanan Siber, Tekanan Nasabah, Tekanan Digital Publik, Kualitas Tata Kelola Perusahaan, Perbankan

ABSTRACT

This study explores how customer pressure, public digital pressure, and the quality of corporate governance influence cybersecurity disclosure in Indonesia's banking sector. Using a quantitative panel data design, this study analyzed 115 observations by banks listed on the Indonesia Stock Exchange over 2020–2024. Cybersecurity disclosure was measured using word frequency analysis by Voyant Tools, while customer pressure was proxied by total customer deposits, public digital pressure by Google Trends scores, and corporate governance quality by the LSEG Management Score. Panel data regression by robustness checks through lagged regression and Propensity Score Matching were employed. Outcomes confirm that CP, PDP, and CGS each positively and significantly influence CSD. Differences in disclosure among state-owned and non-state-owned banks were also identified. Overall, the outcomes extend legitimacy theory to cybersecurity disclosure in emerging-market banking and support the use of Google Trends as a practical proxy for public digital pressure.

Keywords: Cyber Security Disclosure, Customer Pressure, Public Digital Pressure, Corporate Governance Quality, Banking

 DOI: https://doi.org/10.29303/akurasi.v9i1.902

1. Introduction

The implementation of technology in financial services during the digital transformation revolution necessitates that Indonesian banks revise their business strategies. In 2024, 649 thousand cyber-attacks aimed at the Indonesian banking sector were detected: Kaspersky ReportKaspersky Report (infobanknews, 2025). Such a staggering number is proportionate to the massive increase in electronic money transfer transactions, which increased from IDR 22.4 trillion in 2019 to IDR 303 trillion for the first half of 2024 (Binar Academy, 2025). The rapid growth of electronic transactions has exposed banking companies to an average of 1,162 cyberattacks per week (Nurrizky & Nugroho, 2025). The high frequency of these attacks demonstrates that digitalisation carries significant security risks (Koeswandana & Yulfiatmi, 2025). Such threats forces banking companies to have cyber security policies and disclose them as a transparency towards stakeholders.

In the past few years, cyber attacks on Indonesian banks to have produce clear and real effects. Bank Syariah Indonesia to have get hit by LockBit ransomware in May 2023. This attack to have cause a data leak of 1.5 terabytes. The data to have come from about 15 million customers and 24,437 employees (Tempo, 2024). A similar attack to have impact Bank Rakyat Indonesia. The bank to have be the target of Bashe ransomware in December 2024 (Kompas, 2024). Earlier, Bank Indonesia was attacked by the ransomware Conti in late 2021 (Tempo, 2024). These recurring events indicate that no banking institution is completely safe from cyber threats. The repercussions include financial losses, erosion of public trust as well as extended reputational risk.

Over time, OJK and Bank Indonesia have stepped in to implement more stringent regulations aimed at requiring the banks involved to have strong and dependable cybersecurity systems due to the increasing cyber threats. OJK issued Regulation No. 11/POJK.03/2022 on Information Technology Management and Circular Letter No. 29/SEOJK.03/2022 on Cyber Resilience and Security (KPMG, 2023). Concurrently, Bank Indonesia released Regulation No. 2/2024 about Information System Security and Cyber Resilience, that became effective as of April 2024 (Bank Indonesia, 2024). Both regulations require banks to adopt anticipatory, adaptive and proactive cyber security systems. These regulatory frameworks create compliance pressures which make it increasingly prudent for banks to enhance transparency in their cybersecurity disclosures to stakeholders.

Indonesia recorded 221.56 million internet users in 2024, by an internet penetration rate of 79.5% (Intimedia, 2025), and 96% of digital payment users adopted e-wallets as their primary payment method (Statista, 2025). With customers becoming increasingly digitally literate, they are now well-informed of cybersecurity risks and expect better visibility from banks. Highly publicized cybersecurity incidents have raised even greater concern for the security of their personal data. Social media platforms have become prominent channels through that the public monitors and scrutinises the cyber security practices of banks. Customer pressure and the growing influence of public sentiment on digital platforms pose a direct threat to banks' legitimacy. Consequently, banks are compelled to disclose their data protection strategies and practices as a means of maintaining public trust.

2720-9067 (ISSN), **2685-1059** (E-ISSN)
open access at: https://akurasi.unram.ac.id

This phenomenon can be understood through the lens of legitimacy theory, that suggests that banks voluntarily disclose cybersecurity practices in response to external pressures. Suchman (1995) defines legitimacy as the general perception that the actions of an entity are appropriate inside of a socially constructed system of norms and values. In the In the context of cybersecurity, Mansour et al. (2025) argue that credible transparency can reduce information asymmetry, strengthen legitimacy, and at the same time signal operational resilience to both investors and regulators. When a cyber security incident occurs, it creates a legitimacy gap that threatens stakeholder confidence (Cram & D'Arcy, 2023). Therefore, customer pressure and public digital pressure, channelled through digital platforms, represent clear and tangible manifestations of threats to legitimacy (Bajwa et al., 2023), to that banks must respond through Cyber Security Disclosure. In this process, Corporate Governance Quality serves as a key determinant of a bank's effectiveness in addressing external pressures and implementing legitimacy strategies (Radu & Smaili, 2022). Conversely, failing to respond to the demands of customers and the public may lead to customer attrition and a decline in organizational performance.

Although legitimacy theory has long offered a strong foundation for explaining corporate disclosure behavior, research on Cyber Security Disclosure (CSD) in the banking sector is still fragmented and lacks theoretical consistency. Existing studies tend to rely on internal firm-level factors and employ divergent theoretical lenses, ranging by upper echelons and signaling theory to legitimacy theory, leaving the understanding of how external pressures translate into disclosure behaviour still limited. At the empirical level, outcomes have also been mixed. Héroux and Fortin (2024) found that board characteristics are key drivers of CSD in Canada, while Kiesow Cortez and Dekker (2022) showed that changes in disclosure behavior in the Benelux financial sector did not follow a linear path, despite increasing governance pressures. Firoozi and Mohsni (2023) further revealed that CSD levels among major North American banks vary considerably even under relatively similar regulatory frameworks, while López et al. (2025) confirmed that CSD determinants are highly contextual and their outcomes remain largely confined to developed market settings. This inconsistency implies a context-dependent relationship among legitimacy pressures and CSD. The literature is limited with few studies investigating Customer Pressure and Public Digital Pressure as drivers of CSD, especially in emerging markets such as Indonesia where increased digital banking adoption and repeated cyber incidents in a short period of time generate strong stakeholder expectations that until now have not received enough attention.

Drawing upon this gap, this study analyses the factors influencing Cyber Security Disclosure amongst banks listed on the Indonesia Stock Exchange over the period 2020 to 2024, by a primary focus on Customer Pressure, Public Digital Pressure, and Corporate Governance Quality. This study makes three main contributions. Theoretically, it extends legitimacy theory to the context of cybersecurity disclosure in emerging-market banking. While legitimacy theory classically posits that firms respond to social pressures to align their behaviour by societal expectations (Suchman, 1995; Dowling and Pfeffer, 1975), this framework was developed under conditions where information flows were constrained and sources of social pressure were relatively identifiable. In the digital age, these conditions

have shifted, as customers and the public can now access and share information instantly across digital platforms, creating legitimacy threats that stem not only by regulators but also by digitalised customer pressure and public opinion. This study therefore proposes that Customer Pressure and Public Digital Pressure constitute legitimacy-seeking channels that warrant integration into the cyber security disclosure framework. Empirically, it provides evidence on how external stakeholder pressures shape cybersecurity transparency in Indonesia. Practically, it offers guidance for regulators in formulating disclosure policies and assists bank management in designing communication strategies to build stakeholder trust in an increasingly digital environment.

2. Theoretical Framework dan Hypothesis Development

A growing body of research highlights several factors that motivate companies to engage in cybersecurity disclosure. Leverett (2024) and Jameel et al. (2025) demonstrate that regulatory pressures and stakeholder demands create an environment that encourages companies to enhance cyber security transparency as a form of compliance and social legitimation. In addition to external drivers, internal governance factors are equally important. Héroux & Fortin (2024) find that a cybersecurity committee, board-level IT expertise, board independence and gender diversity each play a significant role in the quality of firms' cybersecurity disclosure. These findings are supported further by Kiesow Cortez and Dekker (2022), who highlight the role of a corporate governance lens to influence disclosure practices. Meanwhile, Varghese et al. (2025) and Cheong et al. (2021) show that companies by a history of cybersecurity incidents tend to provide more detailed disclosures to help mitigate the negative consequences of those events.

Regarding the benefits of disclosure, Al Amosh and Khatib (2025) find that cyber security transparency enhances stakeholder trust and reduces information asymmetry, that in turn exerts a positive effect on financial performance and market value. Frank et al. (2023) these outcomes are complemented by evidence that voluntary disclosure can enhance investment attractiveness and create a competitive advantage. Despite this body of evidence, the majority of prior studies continue to focus on internal firm-level factors, particularly governance characteristics, inside of developed market contexts. The role of external pressures by customers and the public, particularly through digital platforms, in the banking sector of emerging markets such as Indonesia remains largely unexplored. Given that Indonesia exhibits a distinctive digitalisation dynamic and unique social pressures, it represents a highly relevant and important context for further investigation.

2.1. Legitimacy Theory

Legitimacy theory provides a theoretical foundation for understanding why companies engage in voluntary cyber security disclosure. Suchman (1995) defines legitimacy as the general perception that the actions of an entity are congruent by the prevailing system of social norms and values. Companies use disclosure as a strategic tool to maintain legitimacy in the eyes of their stakeholders. A substantial body of empirical research has identified the factors that influence disclosure inside of the legitimacy framework. Michelon (2011) finds that companies by strong financial performance and high media exposure are more inclined to engage in sustainability disclosure as a means of communicating their legitimacy. Khan et al. (2013) studies demonstrate that strong

2720-9067 (ISSN), 2685-1059 (E-ISSN)
open access at: https://akurasi.unram.ac.id

governance mechanisms, such as public ownership, board independence, and audit committees, have a positive influence on corporate social responsibility (CSR) disclosure. Gezgin et al. (2024) further show that Corporate Governance Quality mediates the relationship among financial performance and voluntary disclosure.

More recently, legitimacy theory has been employed in cybersecurity disclosure research because a cyber incident can give rise to a legitimacy gap that jeopardizes stakeholders' trust and confidence. López et al. (2025) focus on Cyber Security Disclosure in the financial sector to study how cyber incidents, governance structures, and regulatory frameworks influence disclosure patterns. Firoozi and Mohsni (2023) apply legitimacy theory inside of the banking industry and find that banks employ disclosure as a tool to preserve social legitimacy. Mansour et al, (2025) reinforce these outcomes by demonstrating that cybersecurity transparency reduces information asymmetry and strengthens organizational legitimacy. Legitimacy theory is particularly pertinent to the Indonesian banking context, given that banks manage public funds and personal data, both of that require a high degree of public trust. Customer pressure and public digital pressure conveyed through digital platforms can thus be seen as tangible threats to legitimacy, prompting banks to engage in cybersecurity disclosure.

2.2. Hypothesis Development

Customer Pressure and Cyber Security Disclosure

Customer pressure encourages banks to improve their cybersecurity disclosures through the lens of legitimacy theory. This theory suggests that companies disclose information to maintain the perception that their actions align by prevailing social norms and values (Patten, 1991; Suchman, 1995). Digital banking customers possess significant economic power, given the ease of switching banks and their direct exposure to cyber security risks (Huang & Kung, 2010). Besides, the legitimacy gap leads to trust deficiency that dilutes business continuity whenever there is a cyber disruption. Banking customers in Indonesia are unique, they are digitally savvy, very much aware of cybersecurity threat and active on social media. They are capable of rapidly amplifying security issues through digital platforms. Banks respond to this pressure by enhancing Cyber Security Disclosure as a legitimacy restoration strategy. Transparency in cybersecurity information signals a bank’s commitment to protecting customers and reflects the strength of its risk management practices.

Empirical studies demonstrate that stakeholder pressure exerts a positive influence on voluntary disclosure. Shen et al. (2020) establish this relationship in the context of carbon information disclosure in China. Sulemana et al. (2025) report similar outcomes in the context of sustainability disclosure in emerging markets. Sutantoputra (2022) confirms that customer demands influence environmental disclosure practices in Australia. The cybersecurity context differs by CSR, as customers have a direct economic interest in, and are directly exposed to cybersecurity risks (D’Arcy & Basoglu, 2022). Inside of the Indonesian banking industry, characterised by high digitalisation and a digitally native customer base, Customer Pressure for cyber security transparency is expected to be particularly strong. Economic consequences, such as customer attrition, reputational damage, and erosion of trust compel banks to enhance cybersecurity disclosure in order to

maintain legitimacy. On the basis of this theoretical foundation and the supporting empirical evidence, this study proposes the following hypothesis:

H_1: Customer Pressure has a positive influence on Cyber Security Disclosure in the Indonesian banking sector.

Public Digital Pressure and Cyber Security Disclosure

Public digital pressure, spread through online platforms, has a strong influence on how banks disclose cybersecurity information, largely explained by legitimacy theory. According to legitimacy theory, firms to have use disclosure. They to have want to keep a good image and impression. Their operations to have be within acceptable norms and social values in society (Dowling & Pfeffer, 1975; Suchman, 1995). The internet acts as an enzyme that speeds up how fast corporate performance is scrutinized (Octavio & Setiawan, 2024). Once a cybersecurity incident happens to have, information can travel to have very fast through social media and other digital platforms, and it can create to have strong public pressure. The Internet can allow to have people to debate and to counter-debate to have all the time and in real time, but traditional media can not do to have this. (Dong, 2024; Octavio & Setiawan, 2025b). Public digital attention tends to go viral, significantly amplifying the negative reputational impact of an incident on a bank. When banks face high levels of this digital pressure, they can experience a legitimacy gap, that pushes them to improve their cybersecurity disclosures as a way to restore trust.

Empirical studies indicate that public digital attention drives improvements in corporate disclosure. Octavio & Setiawan (2025a) find that public oversight through the internet has a positive influence on climate change disclosure. Cui et al. (2023) demonstrate that negative media attention enhances the quality of ESG disclosure. In the cybersecurity context, public digital pressure has unique characteristics. Cyber incidents directly affect the banking industry, that is responsible for managing the public's financial data. As a outcome, public attention to cybersecurity issues in banks tends to be more intense, creating stronger pressure for transparency. On the basis of this theoretical foundation and the supporting empirical evidence, this study proposes the following hypothesis:

H_2: Public Digital Pressure has a positive influence on Cyber Security Disclosure in the Indonesian banking sector.

Corporate Governance Quality and Cyber Security Disclosure

Corporate governance quality influences cybersecurity disclosure through the lens of legitimacy theory, as well as through more effective risk oversight mechanisms. Legitimacy theory posits that companies engage in disclosure to sustain the perception that their actions conform to the prevailing norms and social values inside of society (Aerts & Cormier, 2009; Gehman et al., 2017). High-quality corporate governance establishes a more rigorous system for risk management oversight (Octavio et al., 2025a), including cybersecurity risks. Good governance also enhances transparency and accountability in reporting risks to stakeholders. Banks with high Corporate Governance Quality have better internal control systems, which help them in identification, measurement and communication of cyber security risk in a holistic manner (Mazumder & Hossain, 2023).

2720-9067 (ISSN), **2685-1059** (E-ISSN)
open access at: https://akurasi.unram.ac.id

This also helps reduce information asymmetry among management and stakeholders regarding the company's cybersecurity risk exposure.

Empirical evidence consistently shows that stronger corporate governance is associated by better disclosure practices. Xu & Rhee (2018) find that governance quality significantly enhances the quality of information disclosure amongst companies listed in China. Ahsan et al. (2024) establish that high-quality governance substantially improves risk-related disclosure amongst companies in the United States. Sun et al. (2025) confirm that effective corporate governance practices significantly improve the quality of information disclosure, especially when it comes to risk-related information. In the cyber security context, Corporate Governance Quality holds particular relevance, as cyber security risks have a direct bearing on firm value and customer trust. Banks by strong corporate governance tend to be more transparent about their cybersecurity practices. By sharing this information proactively, they signal effective risk management and help build trust by stakeholders. Based on this theoretical perspective and supporting empirical evidence, this study proposes the following hypothesis.

H_3: Corporate Governance Quality has a positive influence on Cyber Security Disclosure in the Indonesian banking sector.

The conceptual framework of this study, that outlines the hypothesized relationships among the variables, is illustrated in Figure 1.

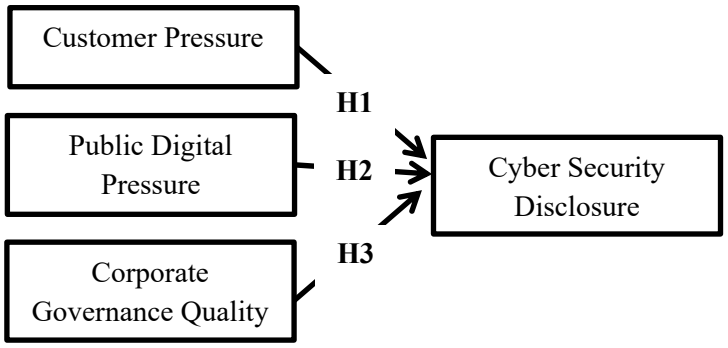

Figure 1. Research Framework

3. Research Method

3.1. Research Design and Data

This study adopts a quantitative approach using a panel data design to examine how Customer Pressure (CP), Public Digital Pressure (PDP), and Corporate Governance Quality (CGS) influence Cyber Security Disclosure (CSD) in the Indonesian banking sector. However, this panel data has attracted attention due to its ability to analyse cross-sectional and time-series variations simultaneously which allows for more precise estimates thus minimizing bias from unobserved heterogeneity (Baltagi, 2021). the study period is 2020 to 2024. This period of time was selected because it reflects the rapid acceleration in the digital transformation of Indonesian banking, motivated by the COVID-19 pandemic and heightened awareness of cybersecurity threats. The study utilises

secondary data obtained by the annual reports of banking companies, the LSEG (London Stock Exchange Group) database, and Google Trends.

3.2. Population and Sample

The study population includes all banking companies listed on the Indonesia Stock Exchange (IDX) by 2020 to 2024. The sample was selected using purposive sampling based on the following criteria:

1) banking companies listed on the IDX and actively operating throughout the study period;
2) companies that consistently published accessible annual reports each year;
3) companies by complete data for all research variables in the LSEG database; and
4) companies that used the Indonesian rupiah as their reporting currency.

These criteria were applied to ensure a consistent sample and sufficient data for panel analysis. The sample selection process, along by the number of excluded observations, is presented in Table 1. Based on these criteria, a sample of 23 banks was obtained, yielding a total of 115 observations over the five-year study period.

Table 1. Sample Selection Procedure

No.	Sample Selection Criteria	Number
	Total banking companies listed on the Indonesia Stock Exchange (IDX) during the study period 2020–2024	49
1	Less: Banking companies not listed and not actively operating throughout the entire study period 2020–2024	0
2	Less: Companies that did not consistently publish accessible annual reports throughout the study period	0
3	Less: Companies by incomplete data for all research variables in the LSEG database	-26
4	Less: Companies that did not use the Indonesian rupiah as their reporting currency	0
	Final number of sample companies	23
	Study period (years)	5
	Total observations (23 companies × 5 years)	115

3.3. Operational Definitions and Variable Measurement

Table 2 outlines how all variables in this study are defined and measured, including the dependent, independent, and control variables, along by their respective data sources. A more detailed explanation of each variable is presented in Table 1

Cyber Security Disclosure is measured by counting how often the word “cyber” appears in each bank’s annual report, using Voyant Tools. The measurement procedure involves four steps: (1) downloading the annual report in PDF format; (2) uploading the file to Voyant Tools (voyant-tools.org); (3) using the “Terms” feature to count how often the word “cyber” appears; and (4) recording that total as the Cyber Security Disclosure score. The measurement formula is as follows: CSD = Total frequency of the word "cyber" in the annual report. Voyant Tools was selected because it is a reliable, web-based text analysis tool that is widely used in content analysis research.

2720-9067 (ISSN), 2685-1059 (E-ISSN)
open access at: https://akurasi.unram.ac.id

Table 2. Operationalisation of Research Variables

Variable	Symbol	Measurement	Data Source
I. Dependent Variable			
Cyber Security Disclosure	CSD	The total frequency of the word 'cyber' in the annual report was analyzed using Voyant Tools (voyant-tools.org).	Annual report; Voyant Tools
II. Independent Variables			
Customer Pressure	CP	Natural logarithm of total customer deposits obtained by the LSEG database	LSEG database
Public Digital Pressure	PDP	Average monthly Google Trends score for each bank's official name (category: "Company"; scope: Worldwide): PDP = Total annual score / 12	Google Trends
Corporate Governance Quality	CGS	The LSEG Management Score is a composite index that covers management structure, governance policies, risk management, transparency, and oversight effectiveness.	LSEG database
III. Control Variables			
Return on Assets	ROA	Net income after tax divided by total assets	LSEG database
Firm Size	FS	Natural logarithm of total assets	LSEG database
Firm Age	FAGE	Number of years since the bank was established up to the observation year	LSEG database
Business Ethics Policy	BETP	Dummy variable: 1 if the company has a formally documented business ethics policy, 0 otherwise	LSEG database
Cyber Security Policy	CSP	Dummy variable: 1 if the company has a formally documented cyber security policy disclosed in its annual report, 0 otherwise	Annual report

Customer Pressure (CP) is measured using the total customer deposits obtained by the LSEG database. This variable reflects the degree of a bank's reliance on customer funding and the potential pressure by its customer base (Babajide et al., 2020). The measurement formula is as follows: CP equals total customer deposits. Higher values indicate a larger customer base and greater potential for customer pressure.

Public Digital Pressure (PDP) is measured using Google Trends data by entering the specific name of each bank and selecting the "Company" category to ensure that the search outcomes pertain exclusively to the respective institution (Octavio et al., 2025b). Google Trends data were collected for each bank using its official name, such as 'Bank Mandiri,' 'Bank BRI,' and 'Bank BCA', by the geographical scope set to 'Worldwide' and the category set to 'Company.' Monthly search scores over the course of a year were summed and divided by 12 to obtain the monthly average. The measurement formula is as follows:

PDP is calculated by dividing the total annual Google Trends score for the company name by 12. This measurement reflects the level of global public attention and scrutiny directed at each individual bank.

Corporate Governance Quality (CGS) is measured using the Management Score by the LSEG database, that covers five dimensions: (1) management structure and composition; and (2) corporate governance policies and practices; (3) risk management systems; (4) management transparency and accountability; and (5) the effectiveness of oversight and internal controls (Kaur & Vij, 2018). The LSEG Management Score is a validated composite index that has been widely used in corporate governance research. It ranges by 0 to 100, by higher values indicating better governance quality.

This study includes five control variables commonly used in disclosure research to ensure the robustness of the analytical outcomes. Return on Assets (ROA), calculated as net income divided by total assets, is used to control for firm profitability. Firm Size (FS) is measured using the natural logarithm of total assets to control for the company size effect. Firm Age (FAGE), calculated as the number of years since the bank was established, is included to control for organisational maturity. Business Ethics Policy (BETP) is measured as a dummy variable to account for the effect of corporate culture. Cyber Security Policy (CSP) is measured as a dummy variable, taking a value of 1 if the company has a formally documented cyber security policy disclosed in its annual report, and 0 otherwise. This variable is included to control for the effect of having a formal cybersecurity policy on the level of cybersecurity disclosure. These control variables were selected because prior research indicates that profitability, firm size, firm age, ethical culture, and the existence of a formal cyber security policy significantly influence disclosure practices. Controlling for these variables helps isolate the pure effect of the independent variables on cybersecurity disclosure.

3.4.Data Collection Technique

Cybersecurity disclosure data were collected through content analysis, using Voyant Tools to examine the annual reports of each bank in the sample. Google Trends data were collected manually by entering the name of each bank as a search term, by the category set to "Company" and the geographical scope set to "Worldwide", covering the period 2020–2024. Financial and governance data were sourced by the LSEG database, including details on customer deposits, total assets, net income, firm age, and Management Score. All data were compiled in a panel data format by a bank-year observation structure to facilitate panel data regression analysis

3.5.Regression Model Analysis

This study uses panel data regression by a fixed effects model to test the research hypotheses. The regression model is defined as follows:

$$CSD(it) = \beta 0 + \beta 1CP(it) + \beta 2PDP(it) + \beta 3CGS(it) + \beta 4ROA(it) + \beta 5FS(it) + \beta 6FAGE(it) + \beta 7BETP(it) + \beta 8CSP(it) + \alpha(i) + \lambda(t) + \varepsilon(it)$$

Where i denotes the bank; t denotes the year; α(i) represents individual fixed effects; λ(t) represents time fixed effects; and ε(it) is the error term. The model was chosen to have control for differences at the bank level that we cannot see, and to have control for shocks that affect all banks in the same time. A Hausman test will be done to have confirmation

2720-9067 (ISSN), 2685-1059 (E-ISSN)
open access at: https://akurasi.unram.ac.id

that the model is appropriate. Robustness checks will be performed using a random effects model and pooled OLS to validate the main outcomes.

3.6.Robustnest Check and Additional Analysis

To make sure to have reliable outcomes, this study includes to have several checks and to have additional tests. The checks are done to have two ways: to have lagged independent variables to reduce reverse causality, and to have Propensity Score Matching (PSM) to fix selection bias. To address potential endogeneity, this study uses the System GMM estimator. The validity of the instruments is confirmed using the Sargan test, while the Arellano-Bond AR(2) test verifies the absence of second-order autocorrelation. Additionally, a subsample analysis is conducted by partitioning the sample into state-owned banks and non-state-owned banks to examine whether ownership type influences the relationship among the independent variables and cybersecurity disclosure.

4. Results and Discussion

4.1. Descriptive Statistics

Table 2. Descriptive Statistics

Panel A: Continuous Variables					
Variable	**Obs**	**Mean**	**Std. Dev.**	**Min**	**Max**
CSD	115	41.957	58.095	0	544
CP	115	2.95×10^{14}	4.21×10^{14}	4.02×10^{10}	1.70×10^{15}
PDP	115	57.146	22.582	1.167	95.833
CGS	115	57.254	36.164	0	99.545
FS	115	3.94×10^{14}	5.81×10^{14}	7.21×10^{11}	2.43×10^{15}
ROA	115	0.009	0.03	−0.181	0.084
FAGE	115	39.739	20.216	1	83
Panel B: Dummy Variables					
Variable	**Category**		**Freq.**		**Percent**
BETP	0		36		31.30%
	1		79		68.70%
Total			**115**		**100%**
CSP	0		31		26.96%
	1		84		73.04%
Total			**115**		**100%**

Notes: CSD = Cyber Security Disclosure; CP = Customer Pressure; PDP= Public Digital Pressure; CGS = Corporate Governance Score; FS = Firm Size; ROA = Return on Assets; FAGE = Firm Age; BETP = Business Ethics Policy ; CSP = Cyber Security Policy

Table 2 reports the descriptive statistics for all variables used in this study. The dependent variable, Cyber Security Disclosure (CSD), has an average value of 41.957, by a standard deviation of 58.095 and a range by 0 to 544. This suggests considerable variation in cybersecurity disclosure practices among the sample companies. Turning to the independent variables, Customer Pressure (CP) is proxied by total customer deposits measured in thousands of Indonesian rupiah, by a mean value of 2.95×10^{14} and a standard deviation of 4.21×10^{14}, reflecting the considerable variation in Customer Pressure faced by each banking company in the sample. Public Digital Pressure (PDP) is measured using

Google Trends scores, by an average value of 57.146 and a standard deviation of 22.582. These scores capture the level of online public attention directed at each bank, that varies across companies and over time. Meanwhile, Corporate Governance Quality (CGS) has a mean value of 57.254 by a standard deviation of 36.164 and a range of 0 to 99.545, indicating considerable differences in governance quality amongst the sample companies. By regard to the control variables, Firm Size (FS) has a mean value of 3.94×10^{14} and a standard deviation of 5.81×10^{14}, indicating that the companies in the sample are generally large in scale. Return on Assets (ROA) has a relatively low mean value of 0.009 by values ranging by -0.181 to 0.084, indicating a wide variation in profitability across the sample. Firm Age (FAGE) averages 39.739 years, ranging by 1 to 83 years, reflecting the diversity in organisational maturity across the sample. Finally, approximately 68.70% of the sample companies have adopted a Business Ethics Policy (BETP) and 73.04% have implemented a Cyber Security Policy (CSP), indicating that the majority of sample companies have formally committed to both business ethics governance and cyber security management.

4.2.Multicolinierity Test

Table 3. Correlation Matrix

Variable	1	2	3	4	5	6	7	8	9
(1) CSD	1.000								
(2) CP	0.423***	1.000							
(3) PDP	0.251***	0.286***	1.000						
(4) CGS	0.476***	0.418***	0.189**	1.000					
(5) FS	0.264***	0.702***	0.024	0.430***	1.000				
(6) ROA	0.050	0.328***	0.155	0.250***	0.262***	1.000			
(7) FAGE	0.215**	0.265***	0.018	0.144	0.011	0.000	1.000		
(8) BETP	0.292***	0.349***	0.279***	0.647***	0.327***	0.254***	0.115	1.000	
(9) CSP	0.394***	0.343***	0.178*	0.505***	0.301***	0.121	0.128	0.615***	1.000

Notes: *** p < 0.01, ** p < 0.05, * p < 0.10.
CSD = Cyber Security Disclosure; CP = Customer Pressure; PDP= Public Digital Pressure; CGS = Corporate Governance Score; FS = Firm Size; ROA = Return on Assets; FAGE = Firm Age; BETP = Business Ethics Policy ; CSP = Cyber Security Policy

Before conducting the regression analysis, this study first assessed the potential for multicollinearity among the variables using two approaches: a correlation matrix (shown in Table 3) and the Variance Inflation Factor (VIF) along by tolerance values (reported in Table 4). The outcomes of the correlation matrix indicate that the highest correlation amongst the independent variables occurs among CP and FS at 0.702, whilst correlations amongst the remaining variables remain at relatively moderate levels. By reference to Hair et al. (2010), a correlation exceeding 0.90 amongst independent variables indicates a serious multicollinearity problem. Accordingly, the correlation values in this study fall inside of acceptable limits. Turning to the VIF outcomes presented in Table 3, all values are below 10, by the highest VIF of 3.85 observed for the CSP variable and an average VIF of 2.34. All tolerance values also exceed 0.10, by the lowest value of 0.260 recorded for the CSP variable. Based on the established criteria (Gujarati, 2004; O'Brien, 2007), VIF values below 10 and tolerance values above 0.10 indicate that no serious multicollinearity

2720-9067 (ISSN), **2685-1059** (E-ISSN)
open access at: https://akurasi.unram.ac.id

issues are present in the research model, suggesting that the regression coefficient estimates are reliable.

Table 4. Variance Inflation Factor (VIF)

Variable	VIF	Tolerance
CP	2.85	0.351
PDP	1.30	0.771
CGS	2.34	0.428
FS	2.52	0.398
ROA	1.23	0.815
FAGE	1.20	0.831
BETP	3.47	0.288
CSP	3.85	0.260
Mean VIF	2.34	

Notes: All VIF values < 10 and Tolerance (1/VIF) values > 0.10, indicating no serious multicollinearity concern.
CSD = Cyber Security Disclosure; CP = Customer Pressure; PDP= Public Digital Pressure; CGS = Corporate Governance Score; FS = Firm Size; ROA = Return on Assets; FAGE = Firm Age; BETP = Business Ethics Policy ; CSP = Cyber Security Policy

4.3. Regression Analysis Result

Table 5 shows the results of the overall regression model outcomes. For the most part, there is sufficient statistical fit of all three models with F-statistics which are significant at the 1% level (F = 7.020, 6.270 and 6.810 respectively), indicating that all independent variables jointly exert a significant influence on Cyber Security Disclosure (CSD). Adjusted R^2 between Full Model is 0.2971, which indicates that the Complete Model explains approx 29.71% var in Cyber Security Disclosure By comparison, the Stakeholder Pressure model and the Corporate Governance model explain only 24.45% and 23.43% of the variance, respectively.

Table 5. Regression Estimation Outcomes

Variable	Full Model		Stakeholder Pressure		Corporate Governance	
	Coef.	t	Coef.	t	Coef.	t
CP	0.181**	2.250	0.176**	2.120		
PDP	0.001*	1.753	0.001*	1.680		
CGS	0.012***	3.000			0.012***	3.000
FS	−1.36e−16	−0.55	2.41e−17	0.100	2.07e−16	1.120
ROA	−4.296	−1.28	−2.890	−0.84	−2.082	−0.61
FAGE	0.005	0.930	0.006	1.170	0.009*	1.820
BETP	−0.536	−1.47	−0.451	−1.20	−0.431	−1.17
CSP	0.554	1.380	1.058***	2.800	0.588	1.430
Obs	115		115		115	
R^2	0.3464		0.2909		0.2746	
Adj. R^2	0.2971		0.2445		0.2343	
F-stat	7.020***		6.270***		6.810***	

Notes: *** p < 0.01, ** p < 0.05, * p < 0.10.
CSD = Cyber Security Disclosure; CP = Customer Pressure; PDP= Public Digital Pressure; CGS = Corporate Governance Score; FS = Firm Size; ROA = Return on Assets; FAGE = Firm Age; BETP = Business Ethics Policy ; CSP = Cyber Security Policy

As for the first hypothesis, regression results show that Customer Pressure (CP) has a positive and significant impact on CSD in both the Full Model (β = 0.181; t = 2.250; p < 0.05) and Stakeholder Pressure model (β = 0.176; t = 2.120; p < 0.05). These outcomes suggest that banks by larger customer deposit bases tend to disclose more information about their cyber security practices. This outcome is consistent by the argument that customers by larger deposit values have a greater interest in the security of their data and assets, thereby compelling management to enhance transparency regarding cyber security practices. Accordingly, H1 is supported.

Regarding the second hypothesis, Public Digital Pressure (PDP) shows a positive and significant effect on CSD in both the Full Model (β = 0.001; t = 1.753; p < 0.10) and the Stakeholder Pressure model (β = 0.001; t = 1.680; p < 0.10). Whilst significant at the 10% level, the positive direction of the coefficient confirms that increasing online public attention towards cyber security issues, as proxied by Google Trends scores, encourages banking companies to enhance their Cyber Security Disclosure. This outcome is consistent by legitimacy pressure by the public, that encourages companies to be more responsive in communicating their cybersecurity protection efforts to stakeholders. Accordingly, H2 is supported.

By regard to the third hypothesis, Corporate Governance Quality (CGS) exerts a positive and significant influence on CSD in both the Full Model (β = 0.012; t = 3.000; p < 0.01) and the Corporate Governance model (β = 0.012; t = 3.000; p < 0.01). The finding indicates that firms with stronger corporate governance provide more informativeness of cybersecurity disclosure. This marks the commitment of both the board of directors and management to cybersecurity risk management as a governance priority. Accordingly, H3 is supported.

Regarding the control variables, Firm Size (FS), Return on Assets (ROA), Business Ethics Policy (BETP), and Cyber Security Policy (CSP) do not show a significant effect in the full model. However, CSP is an exception, as it is significant in the stakeholder pressure model (β = 1.058; t = 2.800; p < 0.01). Meanwhile, Firm Age (FAGE) demonstrates a positive and significant influence in the Corporate Governance model (β = 0.009; t = 1.820; p < 0.10), indicating that more established companies tend to exhibit higher levels of Cyber Security Disclosure.

4.4.Robustness Tests

To ensure the reliability of the study's main outcomes, two robustness checks were conducted: lagged variable regression (as shown in Table 6) and Propensity Score Matching (PSM) (as shown in Table 7). The first approach employs one-period lagged values (L1) for all primary independent variables to address the potential problem of reverse causality among the independent variables and CSD. The outcomes in Table 5 show that L1.CP remains positively and significantly associated by CSD in both the Full Model and the Stakeholder Pressure model. Similarly, L1.PDP is also significant in the Full Model, by its level of significance increasing further in the Stakeholder Pressure model. Meanwhile, L1.CGS also consistently exerts a positive and significant influence on CSD in both the Full Model and the Corporate Governance model. All three models in the lagged variable test remain jointly significant based on their F-statistics, confirming that the main regression outcomes are not spurious.

2720-9067 (ISSN), **2685-1059** (E-ISSN)
open access at: https://akurasi.unram.ac.id

Table 6. Robustness Test: Lagged Regression Outcomes

Variable	Full Model		Stakeholder Pressure		Corporate Governance	
	Coef.	t	Coef.	t	Coef.	t
L1.CP	0.163**	2.270	0.161**	2.170		
L1.PDP	0.001*	1.860	0.001**	2.110		
L1.CGS	0.007**	2.480			0.008***	2.630
FS	−1.21e−16	−0.55	3.70e−17	0.170	1.79e−16	1.040
ROA	−3.548	−1.09	−2.202	−0.67	0.362	0.110
FAGE	0.001	0.150	0.002	0.450	0.005	1.100
BETP	−0.472	−1.56	−0.484	−1.55	−0.498	−1.56
CSP	0.319	0.950	0.505	1.500	0.417	1.180
Obs		92		92		92
R^2		0.294		0.241		0.187
Adj. R^2		0.226		0.178		0.130
F-stat		4.310***		3.820***		3.270***

Notes: *** $p < 0.01$, ** $p < 0.05$, * $p < 0.10$.*

CSD = Cyber Security Disclosure; CP = Customer Pressure; PDP= Public Digital Pressure; CGS = Corporate Governance Score; FS = Firm Size; ROA = Return on Assets; FAGE = Firm Age; BETP = Business Ethics Policy ; CSP = Cyber Security Policy

Table 7. Robustness Test: Propensity Score Matching

Variable	Coef.	t
CP	0.146**	2.480
PDP	0.004**	1.960
CGS	0.015***	4.300
FS_Ln	0.051	0.550
ROA	14.105***	3.280
FAGE	0.008***	2.630
BETP	−0.636***	−3.80
CSP	2.282***	4.540
R^2		0.427
Adj. R^2		0.396
F-stat		13.890
Untreated		36
Treated		79
Total Obs		115

Notes: *** p < 0.01, ** p < 0.05, * p < 0.10.

CSD = Cyber Security Disclosure; CP = Customer Pressure; PDP= Public Digital Pressure; CGS = Corporate Governance Score; FS = Firm Size; ROA = Return on Assets; FAGE = Firm Age; BETP = Business Ethics Policy ; CSP = Cyber Security Policy

The second approach, shown in Table 6, uses Propensity Score Matching (PSM) to classify companies based on whether they have a Business Ethics Policy (BETP). Firms by a BETP are treated as the "treated" group, while those devoid of one are considered the "untreated" group. The outcomes presented in Table 6 indicate that CP, PDP, and CGS continue to exert a positive and significant influence on CSD, consistent by the outcomes

of the main regression. The increase in adjusted R^2 compared to the initial Full Model suggests that controlling for sample selection bias through PSM enhances the model's explanatory power. Taken together, the outcomes of both robustness tests provide strong confirmation that the main outcomes of this study are robust to both potential reverse causality bias and sample selection bias.

To address potential endogeneity concerns, this study employs the System GMM estimator, by the outcomes presented in Table 8. The diagnostic tests confirm that the instruments are valid and the model is free by second-order serial correlation, indicating that the estimation is reliable. All three independent variables have positive and significant effects on cybersecurity disclosure. Customer Pressure suggests that banks by a larger customer base tend to disclose more cybersecurity-related information, Public Digital Pressure suggests that greater public attention through digital channels encourages banks to increase disclosure, and Corporate Governance Quality reflects the role of sound governance mechanisms in promoting transparency.

Table 8. Endogeneity Test: GMM

Variable	Coefficient	z-statistic
CSD (L1)	0.374	2.460
CP	0.458	2.200
PAI	0.000	2.500
CGS	0.006	2.360
FS	1.83e−16	0.220
ROA	−2.7788	−0.82
FAGE	0.004	0.110
BETP	−0.2570	−0.63
CSP	0.533	1.650
Diagnostic Tests		
Obs		92
Wald chi2(8)	156.320	0.000
Sargan test chi2(8)	11.507	0.175
AR(1)	−2.416	0.016
AR(2)	−1.574	0.104

4.5. Discussion

The outcomes of this study enhance our understanding of the factors that drive cybersecurity disclosure in the Indonesian banking sector, viewed through the lens of legitimacy theory. All three hypotheses proposed in this study are empirically supported. Overall, these outcomes indicate that Cyber Security Disclosure is not merely a response to regulatory obligations, but rather a strategy through that banks maintain trust and legitimacy in the eyes of their stakeholders.

Customer pressure is found to encourage banks to enhance their cybersecurity disclosure. This outcome can be understood by considering the unique position of customers inside of the banking context. Unlike investors or the general public, customers entrust their financial data and assets directly to the bank. When a cyber incident occurs, customers become the most directly harmed party. This condition makes legitimacy threats originating by customers considerably stronger than social pressures related to issues such

2720-9067 (ISSN), 2685-1059 (E-ISSN)
open access at: https://akurasi.unram.ac.id

as environmental protection or CSR, whose impacts tend to be more diffuse and are not experienced directly by any single group. Suchman (1995) and Dowling and Pfeffer (1975) explain that companies will strive to maintain their legitimacy when it is threatened, including through voluntary disclosure. In banking, customer pressure often comes by real, tangible losses that people experience firsthand, something that naturally pushes banks to respond by being more transparent and improving their disclosures. The data breach incident at an Indonesian bank affecting millions of customers provides concrete evidence of how Customer Pressure compels banks to improve transparency (Tempo, 2023). This outcome extends the evidence of Shen et al. (2020) and Sulemana et al. (2025) on stakeholder-driven disclosure to the domain of cyber security disclosure in emerging market banking, that remains underexplored.

Public digital pressure captured through Google Trends data has been shown to have a statistically significant impact on how organizations disclose their cybersecurity practices. Nevertheless, its relatively small effect size indicates that this variable likely functions as an awareness trigger for bank management rather than as a direct driver of substantive disclosure action. In theory, digital platforms speed up the spread of information about cybersecurity incidents in real time, while also intensifying the reputational pressure that banks face. However, whether this increased public attention is subsequently translated into meaningful disclosure depends on two factors, namely the maturity of the bank's internal governance systems and how seriously management assesses the reputational risks involved. Accordingly, public attention in the digital space tends to alert management to existing legitimacy gaps, but a concrete disclosure response usually only emerges when the bank has sufficient internal capacity to act on it. This outcome enriches the arguments of Octavio and Setiawan (2025a) and Cui et al. (2023) by demonstrating that the pathway by digital pressure to improved disclosure quality is not direct, but rather mediated by the internal capacity of the organisation.

Corporate Governance Quality is found to have a positive influence on Cyber Security Disclosure, consistent by Ahsan et al. (2024) and Sun et al. (2025), who demonstrate that better governance quality drives more transparent and comprehensive disclosure practices. Beyond simply producing better disclosure as an output, governance quality appears to function as an internal capacity that determines how effectively a company responds to pressure by customers and the digital public through substantive disclosure (Smaili et al., 2023). Banks by higher governance scores possess more mature internal control systems and more structured procedures for identifying and communicating cyber security risks to stakeholders. By this capacity, banks are able to respond to customer pressure and public digital pressure in a more organized and credible manner. This outcome is consistent by Radu and Smaili (2022), who emphasise the role of governance as a key determinant of the effectiveness of legitimacy strategies, and extends that argument by positioning governance as an adaptive resource that enables banks to respond to stakeholder pressures that are increasingly amplified by digital platforms.

Taken together, this study extends the application of legitimacy theory to cybersecurity disclosure in the digital era, building on the work of Firoozi and Mohsni (2023) and Mansour et al. (2025). It demonstrates that in the digital age, legitimacy threats

no longer originate solely by formal regulatory pressures, but also increasingly by the direct pressure of harmed customers and rapidly evolving public attention in digital spaces. Proactive cybersecurity disclosure should be treated as a strategic means to engender trust with customers and the public by bank management, not simply a compliance obligation. For regulators like OJK and Bank Indonesia, these results indicate that regulations like OJK Regulation No. 11/POJK. 03/2022 and Bank Indonesia Regulation No. 2/2024 have implications beyond compliance, specifically that of corporate social accountability, re spawning a culture of transparency which is responsive to stakeholder pressure in an age of digitization.

4.6. Additional Analysis

To better understand how Cyber Security Disclosure patterns differ based on bank ownership, this study includes an additional analysis by dividing the sample into two groups: state-owned banks (shown in Table 9) and non-state-owned banks (shown in Table 8). The outcomes for the state-owned bank subsample indicate that Customer Pressure (CP) and Public Digital Pressure (PDP) continue to exert a positive and significant influence on Cyber Security Disclosure, whilst Corporate Governance Quality (CGS) does not demonstrate a significant influence inside of this group. This is likely due to the high level of public exposure and intense societal scrutiny faced by government-owned banks, where external pressures become the main driver of Cyber Security Disclosure for this group.

Table 9. Additional Analysis: state-owned banks Subsample

Variable	Full Model		Stakeholder Pressure		Corporate Governance	
	Coef.	t	Coef.	t	Coef.	t
CP	0.584*	1.870	0.418*	1.963		
PDP	0.003**	2.110	0.031*	1.900		
CGS	0.015	0.960			0.005	0.380
FS	1.43e-15**	2.220	1.33e-15**	2.090	0.000	0.840
ROA	5.320	0.800	3.149	0.500	-0.002	0.000
FAGE	0.025	0.490	-0.013	-0.400	-0.071**	-2.650
BETP	-0.685	-0.590	0.311	0.600	0.888	0.940
Obs		40		40		40
R^2		0.396		0.379		0.306
Adj. R^2		0.264		0.266		0.204
F-stat		3.000***		3.350***		3.000***

Notes: *** p < 0.01, ** p < 0.05, * p < 0.10.
CSD = Cyber Security Disclosure; CP = Customer Pressure; PDP= Public Digital Pressure; CGS = Corporate Governance Score; FS = Firm Size; ROA = Return on Assets; FAGE = Firm Age; BETP = Business Ethics Policy ; CSP = Cyber Security Policy

A different pattern emerges in the non-state-owned bank subsample, where Customer Pressure (CP) and Corporate Governance Quality (CGS) have a stronger and more significant influence, while Public Digital Pressure (PDP) does not show a significant effect. Inside of this group, internal governance quality plays a more dominant role in driving cyber security transparency than external pressure by the digital public. The

2720-9067 (ISSN), 2685-1059 (E-ISSN)
open access at: https://akurasi.unram.ac.id

contrasting patterns among the two groups indicate that the determinants of Cyber Security Disclosure are not uniform across the sample. Rather, these differences are shaped by banks' ownership structures, that create distinct legitimacy pressures for government-owned and privately owned banks.

Table 9. Additional Analysis: privately-owned banks Subsample

Variable	Full Model		Stakeholder Pressure		Corporate Governance	
	Coef.	t	Coef.	t	Coef.	t
CP	0.247***	3.240	0.264***	3.320		
PDP	0.001	0.300	0.002	0.380		
CGS	0.011***	2.750			0.012***	2.900
FS	-9.56e-16***	-2.670	-9.61e-16**	-2.560	0.000	-1.200
ROA	-3.485	-0.960	-1.724	-0.460	-0.254	-0.070
FAGE	0.013**	2.570	0.015***	2.670	0.021***	4.090
BETP	-0.449	-1.410	-0.332	-1.010	-0.528	-1.630
CSP	0.614*	1.740	1.064***	3.240	0.741*	1.980
Obs		75		75		75
R^2		0.551		0.499		0.464
Adj. R^2		0.496		0.447		0.417
F-stat		10.100***		9.530***		9.830***

Notes: *** p < 0.01, ** p < 0.05, * p < 0.10.

CSD = Cyber Security Disclosure; CP = Customer Pressure; PDP= Public Digital Pressure; CGS = Corporate Governance Score; FS = Firm Size; ROA = Return on Assets; FAGE = Firm Age; BETP = Business Ethics Policy ; CSP = Cyber Security Policy

5. Conclusion, Implications, and Limitations

This study aims to examine the influence of Customer Pressure (CP), Public Digital Pressure (PDP), and Corporate Governance Quality (CGS) on Cyber Security Disclosure (CSD) in the Indonesian banking sector by 2020 to 2024. All three primary independent variables are found to exert a positive and significant influence, such that all hypotheses are empirically supported. Customer pressure drives banks to enhance cybersecurity transparency, as customers have a direct economic interest in the security of their data and assets. Public Digital Pressure demonstrates that heightened online public attention compels management to respond through enhanced disclosure as a means of maintaining public trust. High-quality corporate governance enhances banks' ability to identify and communicate cybersecurity risks to stakeholders. Further analysis shows that, in state-owned banks, external pressures are the main drivers of cybersecurity disclosure, whereas in non-state-owned banks, internal governance quality plays a more prominent role. All outcomes are validated through robustness tests using lagged variable regression and Propensity Score Matching.

This study makes several important contributions. By a theoretical perspective, it extends the application of legitimacy theory to cybersecurity disclosure in emerging market banking, particularly by reconceptualizing how legitimacy functions in the digital age. Although legitimation theory in the literature mainly stresses regulatory and institutional pressures as main disclosure drivers, this research argues that the advent of

digital platfoms has extended the range of legitimacy threats to encompass Customer Pressure and Public Digital Pressure, both situation reflecting an increased capability for external actors to track and assess corporate behaviour in real time. This re-conceptualization helps towards a more nuanced understanding of legitimacy seeking behavior, especially in situations where digital adoption is moving quickly. Methodologically, it validates Google Trends scores as a relevant and innovative proxy for Public Digital Pressure in disclosure research which is replicable (and reusable) measurement that can be adopted by future studies in emerging markets. Empirically, the outcomes show that the determinants of Cyber Security Disclosure are not consistent across institutions. This is evident by the differing outcomes among state-owned and non-state-owned bank subsamples, suggesting that ownership structure creates meaningful institutional differences that one-size-fits-all frameworks may fail to capture.

This study is subject to several limitations that warrant consideration. Cyber Security Disclosure is measured based on the frequency of the word “cyber” in annual reports, following established content analysis methods widely used in prior disclosure research. While this approach ensures objectivity and replicability, future research may extend this by incorporating semantic and qualitative dimensions through artificial intelligence-based text analysis to further enrich the measurement of disclosure depth. Additionally, future research is encouraged to develop a more comprehensive cyber security disclosure index and to extend the analysis to industry sectors beyond banking.

Acknowledgements
The authors declare that no funding was received for this research

Conflict of Interest Statement
The authors declare that there is no conflict of interest regarding the publication of this article.

Data Availability Statement
The data supporting the outcomes of this study are available by the corresponding author upon reasonable request.

Author Contributions

Muhammad Fadhly Rizky Octavio: Conceptualization, Methodology, Software, Validation, Formal analysis, Investigation, Resources, Data curation, Writing – original draft, Writing – review & editing, Visualization, Supervision, Project administration.

Noorfaiz Athallah Koeswandana: Conceptualization, Methodology, Formal analysis, Writing – original draft, Writing – review & editing, Visualization, Data curation.

ORCID iDs
First Author: https://orcid.org/0000-0001-8781-5111
Second Author: https://orcid.org/0009-0004-6528-1058

2720-9067 (ISSN), **2685-1059** (E-ISSN)
open access at: https://akurasi.unram.ac.id

References

Aerts, W., & Cormier, D. (2009). Media legitimacy and corporate environmental communication. *Accounting, Organizations and Society*, *34*(1), 1–27. https://doi.org/10.1016/j.aos.2008.02.005

Ahsan, T., Albitar, K., Gull, A. A., & Hussainey, K. (2024). Does climate governance affect waste disclosure? Evidence by the U.S. *Applied Economics*, *56*(43), 5146–5162. https://doi.org/10.1080/00036846.2023.2244242

Al Amosh, H., & Khatib, S. F. A. (2025). COVID-19 pandemic, ESG performance, and sustainability disclosure in the European healthcare sector: Do GRI guidelines matter? *Business Strategy & Development*, *8*(2). https://doi.org/10.1002/bsd2.70128

Babajide, A., Abiodun Okaertunlola, F., Adedoyin, L., Okafor, T., & Isibor, A. (2020). Analysis of banks profitability: Domestic and foreign comparison. *WSEAS Transactions on Business and Economics*, *17*, 947–955. https://doi.org/10.37394/23207.2020.17.93

Bajwa, I. A., Ahmad, S., Mahmud, M., & Bajwa, F. A. (2023). The impact of cyberattacks awareness on customers' trust and commitment: an empirical evidence by the Pakistani banking sector. Information & Computer Security, 31(5), 635–654. https://doi.org/10.1108/ICS-11-2022-0179

Baltagi, B. H. (2021). *Econometric analysis of panel data*. Springer International Publishing. https://doi.org/10.1007/978-3-030-53953-5

Bank Indonesia. (2024, April 18). *Peraturan Bank Indonesia Nomor 2 Tahun 2024 tentang keamanan sistem informasi dan ketahanan siber bagi penyelenggara sistem pembayaran, pelaku pasar uang dan pasar valuta asing, serta pihak lain yang diatur dan diawasi Bank Indonesia*. Bank Indonesia. https://www.bi.go.id/id/publikasi/peraturan/Pages/PBI_022024.aspx

Binar Academy. (2025, March 27). *Strategi cybersecurity yang sukses untuk banking industry di Indonesia*. Binar Academy. https://www.binar.co.id/blog/strategi-cybersecurity-yang-sukses-untuk-banking-industry-di-indonesia

Cheong, A., Yoon, K., Cho, S., & No, W. G. (2021). Classifying the contents of cybersecurity risk disclosure through textual analysis and factor analysis. *Journal of Information Systems*, *35*(2), 179–194. https://doi.org/10.2308/ISYS-2020-031

Cram, W. A., & D'Arcy, J. (2023). 'What a waste of time': An examination of cybersecurity legitimacy. *Information Systems Journal, 33*(6), 1396–1422. https://doi.org/10.1111/isj.12460

Cui, W., Chen, X., Xia, W., & Hu, Y. (2023). Influence of media attention on the quality of environmental, social, and governance information disclosure in enterprises: An adjustment effect based on the shareholder relationship network. *Sustainability*, *15*(18), 13919. https://doi.org/10.3390/su151813919

D'Arcy, J., & Basoglu, A. (2022). The influences of public and institutional pressure on firms' cybersecurity disclosures. *Journal of the Association for Information Systems, 23*(3), 779–805. https://doi.org/10.17705/1jais.00740

Dong, X. (2024). Research on the impact of media attention on corporate ESG performance-based on the mediating effect of green innovation. *Academic Journal of Management and Social Sciences*, *6*(1), 1–6. https://doi.org/10.54097/xne4op89

Dowling, J., & Pfeffer, J. (1975). Organizational legitimacy: Social values and organizational behavior. *The Pacific Sociological Review*, *18*(1), 122–136. https://doi.org/10.2307/1388226

Firoozi, M., & Mohsni, S. (2023). Cybersecurity disclosure in the banking industry: A comparative study. *International Journal of Disclosure and Governance*, *20*(4), 451–477. https://doi.org/10.1057/s41310-023-00190-8

Frank, M. L., Grenier, J. H., Pyzoha, J. S., & Zielinski, N. B. (2023). Implications of enhanced cybersecurity risk management reporting and independent assurance. *Current Issues in Auditing*, *17*(1), P11–P18. https://doi.org/10.2308/CIIA-2022-018

Gehman, J., Lefsrud, L. M., & Fast, S. (2017). Social license to operate: Legitimacy by another name? *Canadian Public Administration*, *60*(2), 293–317. https://doi.org/10.1111/capa.12218

Gezgin, T., Özer, G., Merter, A. K., & Balcıoğlu, Y. S. (2024). The mediating role of corporate governance in the relationship among net profit and equity and voluntary disclosure in the context of legitimacy theory. *Sustainability*, *16*(10), 4097. https://doi.org/10.3390/su16104097

Gujarati, D. N. (2004). *Basic econometrics* (4th ed.). McGraw-Hill.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate data analysis* (7th ed.). Pearson.

Héroux, S., & Fortin, A. (2024). 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

Huang, C.-L., & Kung, F.-H. (2010). Drivers of environmental disclosure and stakeholder expectation: Evidence by Taiwan. *Journal of Business Ethics*, *96*(3), 435–451. https://doi.org/10.1007/s10551-010-0476-3

Infobanknews. (2025, August 19). *Tahun 2024, Kaspersky deteksi 649 ribu serangan siber ke perbankan Indonesia*. Infobanknews. https://infobanknews.com/tahun-2024-kaspersky-deteksi-649-ribu-serangan-siber-ke-perbankan-indonesia/

Intimedia. (2025, January). *Internet penetration rate in Indonesia over the past five years: Developments and challenges*. Intimedia. https://intimedia.id/read/internet-penetration-rate-in-indonesia-over-the-past-five-years-developments-and-challenges

Jameel, A. H., Khalaf, A. J., Saleh, A. F., Sadaa, A. M., Hindi, W. K., Abdulateef, D. A., & Mahdi, A. S. (2025). Corporate value at risk: Why we should care about climate (IFRS S2) and cybersecurity risks? *International Journal of Sustainable Development and Planning*, *20*(7). https://doi.org/10.18280/ijsdp.200732

Kaur, M., & Vij, M. (2018). Corporate governance index and firm performance: Empirical evidence by Indian banking. *Afro-Asian Journal of Finance and Accounting*, *8*(2), 190. https://doi.org/10.1504/AAJFA.2018.091065

Khan, A., Muttakin, M. B., & Siddiqui, J. (2013). Corporate governance and corporate social responsibility disclosures: Evidence by an emerging economy. *Journal of Business Ethics*, *114*(2), 207–223. https://doi.org/10.1007/s10551-012-1336-0

Kiesow Cortez, E., & Dekker, M. (2022). A corporate governance approach to cybersecurity risk disclosure. *European Journal of Risk Regulation*, *13*(3), 443–463. https://doi.org/10.1017/err.2022.10

Koeswandana, N. A., & Yulfiatmi , M. Y. . (2025). Do cyberattacks and religiosity impact customers' loyalty? Study on Bank Syariah Indonesia. *Jurnal Ekonomi & Keuangan Islam*, *11*(2), 179–195. https://doi.org/10.20885/JEKI.vol11.iss2.art2

Kompas. (2024, December 19). *Tak pernah transparan, serangan siber ke sektor perbankan terus berulang*. Kompas. https://www.kompas.id/artikel/lagi-dugaan-serangan-siber-terhadap-sektor-perbankan

KPMG. (2023). *Ketahanan dan keamanan siber bagi sektor perbankan Indonesia*. KPMG. https://assets.kpmg.com/content/dam/kpmg/id/pdf/2023/01/id-seojk-cyber-newsflash-jan23.pdf

2720-9067 (ISSN), **2685-1059** (E-ISSN)
open access at: https://akurasi.unram.ac.id

Leverett, R. (2024). Is sunlight the best disinfectant? The role of regulation in addressing cybersecurity concerns. *Vanderbilt Law Review*, *77*(6), 1935–1981.

López, F. A., Jara-Sarrúa, L., Morales-Parada, F., & Palos-Sánchez, P. R. (2025). Cybersecurity disclosure in the financial sector: An examination of the influence of incident exposure, governance practices, and regulatory context. *Electronic Commerce Research*. https://doi.org/10.1007/s10660-025-10081-5

Mansour, M., Zureigat, B. N., Alkhlifhalsaeed, A., & Alkhatib, A. (2025). Cybersecurity disclosure, board oversight, and financial performance: Evidence by European banking. *Corporate Board: Role, Duties and Composition*, *22*(1), Article 1. https://doi.org/10.22495/cbv22i1art1

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

Michelon, G. (2011). Sustainability disclosure and reputation: A comparative study. *Corporate Reputation Review*, *14*(2), 79–96. https://doi.org/10.1057/crr.2011.10

Nurrizky, A., & Nugroho, W. (2025). Analisis kebijakan Otoritas Jasa Keuangan dalam upaya menanggulangi cyber crime di sektor perbankan. *Recht Studiosum Law Review*, *4*(1), 84–94. https://doi.org/10.32734/rslr.v4i1.18452

O'Brien, R. M. (2007). A caution regarding rules of thumb for variance inflation factors. *Quality & Quantity*, *41*(5), 673–690. https://doi.org/10.1007/s11135-006-9018-6

Octavio, M. F. R., & Setiawan, D. (2024). The influence of board characteristics, ownership structure and public attention on climate change disclosure in banking sector companies. *Business Strategy and Development*, *7*(2). https://doi.org/10.1002/bsd2.394

Octavio, M. F. R., & Setiawan, D. (2025a). Climate change mitigation information disclosure: The impact of external attention on the internet. *Global Knowledge, Memory and Communication*. https://doi.org/10.1108/GKMC-06-2024-0364

Octavio, M. F. R., & Setiawan, D. (2025b). Does stakeholder and media attention influence climate change disclosure? Evidence by mining industry. *Journal of Applied Accounting Research*. https://doi.org/10.1108/JAAR-06-2023-0164

Octavio, M. F. R., Setiawan, D., Aryani, Y. A., & Arifin, T. (2025a). Corporate governance as a driver: Enhancing ESG performance in ASEAN companies. *Business Strategy and Development*, *8*(2). https://doi.org/10.1002/bsd2.70104

Octavio, M. F. R., Setiawan, D., Aryani, Y. A., & Arifin, T. (2025b). The relationship among corporate governance and sustainability performance: The moderating role of public attention. *Asian Review of Accounting*. https://doi.org/10.1108/ARA-01-2025-0009

Patten, D. M. (1991). Exposure, legitimacy, and social disclosure. *Journal of Accounting and Public Policy*, *10*(4), 297–308. https://doi.org/10.1016/0278-4254(91)90003-3

Radu, C., & Smaili, N. (2022). Board gender diversity and corporate response to cyber risk: Evidence by cybersecurity related disclosure. *Journal of Business Ethics*, *177*(2), 351–374. https://doi.org/10.1007/s10551-020-04717-9

Shen, H., Zheng, S., Adams, J., & Jaggi, B. (2020). The effect stakeholders have on voluntary carbon disclosure inside of Chinese business organizations. *Carbon Management*, *11*(5), 455–472. https://doi.org/10.1080/17583004.2020.1805555

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

Statista. (2025, November 27). *Leading digital payment methods usage Indonesia as of May 2025*. Statista. https://www.statista.com/statistics/1464890/indonesia-leading-digital-payment-methods-usage/

Suchman, M. C. (1995). Managing legitimacy: Strategic and institutional approaches. *Academy of Management Review*, *20*(3), 571–610. https://doi.org/10.2307/258788

Sulemana, I., Cheng, L., Agyemang, A. O., Osei, A., & Nagriwum, T. M. (2025). Stakeholders and sustainability disclosure: Evidence by an emerging market. *Sustainable Futures*, *9*, Article 100445. https://doi.org/10.1016/j.sftr.2025.100445

Sun, J., Zheng, L., & Zhan, M. (2025). New path to green transformation: Exploring the impact of corporate governance on environmental information disclosure quality of new energy companies. *Journal of Environmental Management*, *373*, Article 123789. https://doi.org/10.1016/j.jenvman.2024.123789

Sutantoputra, A. (2022). Do stakeholders' demands matter in environmental disclosure practices? Evidence by Australia. *Journal of Management and Governance*, *26*(2), 449–478. https://doi.org/10.1007/s10997-020-09560-8

Tempo. (2023, May 16). *15 juta data nasabah BSI diduga bocor, pakar siber: Hati-hati serangan phising ke pemilik rekening*. Tempo. https://www.tempo.co/ekonomi/15-juta-data-nasabah-bsi-diduga-bocor-pakar-siber-hati-hati-serangan-phising-ke-pemilik-rekening-187193

Tempo. (2024, December 19). *Daftar serangan ransomware ke lembaga keuangan Indonesia: BI, BSI dan terbaru BRI*. Tempo. https://www.tempo.co/sains/daftar-serangan-ransomware-ke-lembaga-keuangan-indonesia-bi-bsi-dan-terbaru-bri-1183490

Varghese, B. B., Tosyali, A. S., & Hansen, S. W. (2025). Cybersecurity show-and-tell: An analysis of firm disclosure behavior and the relevance of prior data breaches. *AMCIS 2025 Proceedings*.

Xu, H., & Rhee, C. S. (2018). Corporate governance structure and accounting information disclosure quality: Evidence by Shenzhen Stock Exchange in China. *Asian International Studies Review*, *19*(1), 99–116. https://doi.org/10.16934/isr.19.1.201806.99

2720-9067 (ISSN), **2685-1059** (E-ISSN)
open access at: https://akurasi.unram.ac.id