Akuntabilitas: Jurnal Ilmu Akuntansi
Volume 16 (2), 2023

P-ISSN: 1979-858X;
E-ISSN: 2461-1190
Page 125 - 138

Role of Board Composition on Voluntary Cybersecurity Disclosure: Evidence of Banking Companies in Southeast Asia

Naougy Hurun Ain[1], Kenny Fernando[2*], Budi Kurniawan[3], Elfina Astrella Sambuaga[4]
[1,2,3]Sampoerna University
[4]Universitas Pelita Harapan
E-mail: [1]naougy.ain@sampoernauniversity.ac.id; [2]kenny.fernando@sampoernauniversity.ac.id;
[3]budi.kurniawan@sampoernauniversity.ac.id; [4]elfina.sambuaga@uph.edu
[*)]Correspondence author

Abstract

This study aims to examine the correlation between board composition and cybersecurity disclosure (CSD) in Southeast Asia banking companies, while investigating the influence of financial characteristics such as profitability, leverage, and firm size on CSD practices. The quantitative analysis methodology is employed in this paper. The level of cybersecurity disclosure in annual reports is analyzed using content analysis with 54 keywords, analyzed through NVIVO 14 software. The correlation between variables is examined using STATA Software with panel data comprising 391 observations. The study focuses on 101 Southeast Asia banking companies from 2017 to 2021. The results indicate that only firm size, measured by the natural logarithm of total assets, has a positive and significant influence on CSD. This suggests that larger firms with higher total assets are more likely to voluntarily disclose cybersecurity information in their annual reports. No statistically significant correlation is found between board composition, other financial factors, and CSD during the study period. This paper acknowledges its limitations and proposes directions for future research. Firstly, the study is limited to listed commercial banks. Future research should include a larger sample encompassing non-financial industry firms. Secondly, the study employs automated content analysis, specifically counting keywords, to assess the quantity of CSD. Future research could conduct discourse analysis of CSD narratives to provide a more meaningful analysis. This approach would evaluate whether the language and tone of CSD convey substantial information to stakeholders or if it is merely a standardized practice. Additionally, future research should explore other variables impacting voluntary CSD and examine economic consequences, such as the effect on the cost of capital. The findings have implications for regulators, policymakers, and companies, enabling regulators to better understand the current level of CSD and determine the need for further guidance.

Keywords: Cyber-Security Disclosure, Board Composition, Banking Industry

Abstrak

Penelitian ini bertujuan untuk menguji hubungan antara komposisi dewan direksi dan pengungkapan keamanan siber (CSD) pada perusahaan perbankan di Asia Tenggara, serta menyelidiki pengaruh karakteristik keuangan seperti profitabilitas, leverage, dan ukuran perusahaan terhadap praktik CSD. Metodologi analisis kuantitatif digunakan dalam makalah ini. Tingkat pengungkapan keamanan siber dalam laporan tahunan dianalisis menggunakan analisis konten dengan 54 kata kunci, dianalisis melalui software NVIVO 14. Korelasi antar variabel diperiksa menggunakan Software STATA dengan data panel sebanyak 391 observasi. Penelitian tersebut berfokus pada 101 perusahaan perbankan Asia Tenggara pada tahun 2017 hingga 2021. Hasil penelitian menunjukkan bahwa hanya ukuran perusahaan yang diukur dengan logaritma natural total aset yang mempunyai pengaruh positif

dan signifikan terhadap CSD. Hal ini menunjukkan bahwa perusahaan besar dengan total aset lebih tinggi cenderung mengungkapkan informasi keamanan siber secara sukarela dalam laporan tahunan mereka. Tidak ditemukan korelasi signifikan secara statistik antara komposisi dewan direksi, faktor keuangan lainnya, dan CSD selama periode penelitian. Makalah ini mengakui keterbatasannya dan mengusulkan arah untuk penelitian masa depan. Pertama, penelitian ini terbatas pada bank-bank komersial yang terdaftar. Penelitian di masa depan harus mencakup sampel yang lebih besar yang mencakup perusahaan industri non-keuangan. Kedua, penelitian ini menggunakan analisis konten otomatis, khususnya menghitung kata kunci, untuk menilai kuantitas CSD. Penelitian di masa depan dapat melakukan analisis wacana narasi CSD untuk memberikan analisis yang lebih bermakna. Pendekatan ini akan mengevaluasi apakah bahasa dan nada CSD menyampaikan informasi penting kepada pemangku kepentingan atau hanya sekedar praktik standar. Selain itu, penelitian di masa depan harus mengeksplorasi variabel lain yang berdampak pada CSD sukarela dan mengkaji konsekuensi ekonomi, seperti dampaknya terhadap biaya modal. Temuan ini mempunyai implikasi bagi regulator, pembuat kebijakan, dan perusahaan, sehingga memungkinkan regulator untuk lebih memahami tingkat CSD saat ini dan menentukan perlunya panduan lebih lanjut.

Kata kunci: *Cyber-Security Disclosure, Board Composition, Banking Industry*

http://journal.uinjkt.ac.id/index.php/akuntabilitas
DOI: 10.15408/akt.v16i1.35014

INTRODUCTION

Nowadays, businesses, governments, as well individuals have placed an increasing emphasis on cybersecurity. According to the Pulse Survey of 2022 conducted by PwC, cyber is the top company threat, about 40% of those surveyed identifying greater frequency along with greater cyber-attacks as a major danger and 38% as a moderate risk. The escalating frequency of cyberattacks against enterprises reflects the increased cyber risk. According to a report by Coveware, the average ransom demand for a business in 2020 was $233,817, up from $84,116 in 2019. Furthermore, over $54 million was lost due to over 241,000 reported phishing attempts received by the Internet Crime Complaint Center of FBI (IC3) within 2020. These numbers illustrate the increasing hazard that cyberattacks pose to businesses. According to a report by Accenture, the average cost of cybercrime per company in 2020 will be $13 million. This represents a 27% increase since 2016. These statistics demonstrate the increasing cost of cybercrime, the rising average ransom demand for businesses, and the high number of phishing attempts, highlight the growing threat of cyberattacks to businesses of all sizes and industries. Companies, irrespective of their scale or sector, can fall victim to cyberattacks, leading to substantial financial setbacks, harm to their reputation, and potential legal obligations (Bourdon, 2017).

As cyber threats continue to evolve and become more sophisticated, it's critical for businesses of all sizes and industries to take proactive measures to protect themselves. According to (Krus, 2012), public enterprises should recognize the vitality of cybersecurity and disclose relevant data on this topic. Providing such information will enable corporations to publicly show their accountability and commitment on this issue, thereby enhancing stakeholder confidence (Matters, 2021). Investors may view strong cybersecurity practices as an indication of good governance and risk management, which can contribute to a company's overall financial health (PwC, 2021). Customers may also feel more confident in doing business with a company that takes cybersecurity seriously and protects their personal information.

Lately, there has been a noticeable surge in the inclusion of cybersecurity disclosures in the regular financial reports of companies. The objective behind these disclosures is to furnish stakeholders with valuable insights into the organization's approaches to handling cybersecurity risks, vulnerabilities, and incidents. By disclosing such information, companies can effectively demonstrate their commitment to cybersecurity and proactive approach to mitigating cyber risks (SecurityScorecard, 2021). In the accounting research community, the relationship between cybersecurity disclosure (CSD) and financial reporting has garnered considerable attention due to its impact on the veracity and dependability of financial information. The field's academics have demonstrated a growing interest in this topic. According to a study by (L. Gao et al., 2020; Li et al., 2018), cybersecurity disclosure is considered quasi- mandatory in both Canada and the United States, where a vast of extant research on CSD has been undertaken. Guidelines or regulations have been issued mandating the disclosure of information regarding a company's cybersecurity risks and incidents. In addition, research by (Radu & Smaili, 2022) concludes that board of directors are responsible for implementing adequate cybersecurity precautions within their organizations to combat cyber risk and warrant disclosures. Comparatively, developing

nations are more vulnerable to intrusions, primarily due to inadequate cybersecurity infrastructures and regulations (United Nations, 2011). In spite of this, there is a dearth of research on CSD practices in developing nations, where companies may not be required by law to disclose such information and may do so voluntarily. Hence, the endpoint of this research is to assess CSD actions within the framework of a developing economy, specifically a developing nation with a swiftly expanding economy, particularly Southeast Asian nations.

Despite the fact that all sectors are susceptible to cyberattacks, the banking industry has been singled out as the primary target of this research due to the increased danger it poses. According to Mirchandani (2018), the likelihood of a cyberattack occurring at a business in the banking and financial sector is three hundred times higher than it occurs in other sectors. This is mostly attributable to the widespread adoption of "financial technologies," which includes mobile and internet banking, digital currencies, blockchain, and artificial intelligence. These "financial technologies" are crucial for banks to utilize in order to provide adequate assistance for their customers. According to the findings of Creado & Ramteke (2020) research, however, these technologies are also very sensitive to malicious operations carried out by cybercriminals.

This study is carried out to investigate the Cybersecurity Disclosure (CSD)'s practices among companies operating within the Southeast Asian (SEA) nations. These countries have adopted a voluntary approach when it comes to disclosing such information. The study aims to assess the accuracy and relevance of the disclosed information, while also examining the key factors that influence businesses' decision-making processes regarding the disclosure of cybersecurity-related information. The outcomes of this research hold significant implications not only for decision-makers, regulators, and investors operating within emerging economies but also for businesses operating within these environments. The study's primary goal is to shed light on legislative and regulatory frameworks aimed at promoting transparency and accountability, with the ultimate aim of enhancing cybersecurity practices throughout the region. This will be achieved by examining the factors that impact organizations' choices in disclosing cybersecurity-related information. Furthermore, the study's result can offer valuable guidance to businesses operating in these burgeoning economies, enabling them to improve their cybersecurity protocols and effectively meet the expectations of their stakeholders.

METHOD

The sample used in this study comprises of 101 Southeast Asia banks listed on each country's Stock Exchange between 2017 and 2021. The selection of the sample is based on the accessibility of annual reports on the official website during the study period. The research employs a technique of purposive sampling to select banks that published annual reports during the study period. As it satisfies the minimum requirement of 50 observations for regression analysis, the sample size is deemed sufficient for the study.

This study investigates Southeast Asia stock exchange-listed banking companies from various countries. The purpose is to analyze a particular phenomenon or topic

http://journal.uinjkt.ac.id/index.php/akuntabilitas
DOI: 10.15408/akt.v16i1.35014

comprehensively by gathering factual data from historical and existing sources and expanding on established theories. The research employs quantitative methodology centered on numerical data analysis. Diverse data sources were utilized for this study, including manual data collection for independent variables and secondary data from S&P for control variables. The dependent variable, CSD, is evaluated utilizing the NVIVO software to run an automated content analysis with 54 CSD-related keywords. Board size (BSIZE), board independence (BIND), and board gender diversity (BGDIV) are the three independent variables utilized in this study to characterize board composition. In addition, the study includes control variables such as bank size, profitability, and leverage. The study employs regression analysis to assess the hypotheses, favoring fixed-effect (year) estimation over pooled OLS and random effect estimations based on the Breusch and Pagan Lagrangian multiplier (LM) test and Hausman test. Then, based on the outcome of the Hausman Test, the researcher decided to employ a random effect model. The result indicates that the probability is greater than chi2 of 0.1648, which is greater than 0.05. In addition, a correlation analysis is performed to investigate multicollinearity among the independent variables, which reveals no significant multicollinearity issue. To ensure the accuracy of CSD identification, 10% of the sample annual reports are selected at random and the content identified by keyword search as valid CSD is manually verified. The study uses board size, board independence, and board gender diversity as research variables to evaluate board composition, with board size measured by the total number of directors, board independence approximated by the proportion of independent directors, and gender diversity measured by the proportion of female directors.

Tabel 1. Research Samples

No.	Criteria	Number
1.	Number of countries	6
2.	Number of banking companies	101
3.	Companies with incomplete data	(20)
4.	**Total Sample (Number of Companies)**	**81**
5.	Observation Period (2017-2021)	5
6.	**Total Observations (year of companies)**	**391**

Sources: Data Proceed, 2022

In investigating the impact of board of directors on Voluntary Cybersecurity Disclosure in listed banking companies across ASEAN, this study considers Cybersecurity Disclosure (CSD) as the dependent variable. The independent variables are Board Size, Board Independence, and Board Gender Diversity. Additionally, the analysis incorporates control variables such as profitability, leverage, and firm size to account for their potential influence on the relationship.

Table 2. Operating Variables

Research Variable	Indicator of Measurement	Reference
Cyber- security Disclosure (CSD)	Sentence Level of 54 keywords using automated content analysis NVIVO 14	Mazumder & Hossain, 2021
Board Size (BSIZE)	Total Number of board of directors (BOD)	Mazumder & Hossain, 2021
Board Independence (BIND)	$\frac{\text{Total Independent Directors}}{\text{Total BOD}}$ x 100%	Mazumder & Hossain, 2021
Board Gender Diversity (BGDIV)	$\frac{\text{Total Women in BOD}}{\text{Total BOD}}$ x 100%	Mazumder & Hossain, 2021
Profitability (PROV)	$\frac{\text{Net Profit after Tax}}{\text{Total Asset}}$	Mazumder & Hossain, 2021
Leverage (LEV)	$\frac{\text{Total Debt}}{\text{Total Asset}}$	Mazumder & Hossain, 2021
Firm Size (SIZE)	*Log (Total Asset)*	Mazumder & Hossain, 2021

Sources: Data Proceed, 2022

RESULT AND DISCUSSION

The study uses a list of 54 keywords related to CSD developed based on prior voluntary cybersecurity disclosure research and annual reports review. The study counts related "keyword" as a unit of analysis over alternative "sentence- level analysis" as considering sentence as a unit of measurement may skip the possibility that differences in the use of grammar or sentence structure might lead to a different number of sentences irrespective of conveying the similar message by two different writers. The study considers counting sentences relatively more burdensome and subjective than relying on relevant keywords as risk information remains merged with the mass piece of other information provided through the annual report. Below is the list of keywords:

Table 3. List of keywords

"cyber" "cyber-risk" "cyber-threat" "cyber-attack" "cyber-security" "cyber- insurance" "online-security" "online-threat" "security-breach" "security-incident" "security-threat" "virus" "computer-virus" "system-security" "information- technology-security" "infosec" "technology-risk" "technology-threat" "information-technology-risk" "information-technology-threat" "malware" "ransomware" "crime-ware" "spyware" "key-logger" "keystroke-logging" "espionage" "data-breach" "data-security" "data-corruption" "corruption-of-data" "data-confidentiality" "confidentiality-of-data" "confidential-data" "hacking" "hacker" "data-theft" "computer-security" "network-security" "information- security" "intrusion" "phishing" "unauthorized-access" "social-engineering" "network-break-in" "ICT-risk" "ICT-security" "technology-risk" "technological- failure" "secured-way" "encryption" "decryption" "secure-network" "firewall".

The relationship between CSD and board composition is examined using a multiple linear regression model. Random-effect (year) regression model is utilized to test the hypotheses formulated in this study.

http://journal.uinjkt.ac.id/index.php/akuntabilitas
DOI: 10.15408/akt.v16i1.35014

$$CSD_{i,t} = a_0 + \beta_1 BSIZE_{i,t} + \beta_2 BIND_{i,t} + \beta_3 BGDIV_{i,t} + \gamma_1 PROFIT_{i,t} + \gamma_2 LEV_{i,t} + \gamma_3 SIZE_{i,t}$$

The subscript i denotes each bank, and subscript t denotes each year.

The data used in this study includes a list of 54 CSD keywords, Board Composition, Profitability, Leverage, and Firm Size. Table 4 shows the descriptive statistics of the independent variable control variables and dependent variables.

Table 4. Statistic Descriptive

Variable	Obs	Mean	Std. dev.	Min	Max
CSD	391	.0047505	.0021463	.0001	.0090462
BSIZE	391	7.877238	4.241464	1	21
BIND	391	.4831244	.2124088	0	1
BGDIV	391	.1816494	.1403553	0	.6666667
PROF	391	.0063439	.021001	-.1805767	.1080233
LEV	391	.8544761	.0991495	.1110664	.9682249
SIZE	391	38710.76	77459.42	45.89301	508888.3

Sources: Data Proceed, 2022

The output shows the summary statistics for the variables CSD, BSIZE, BIND, BGDIV, PROF, LEV, and SIZE. The "Obs" column shows the number of observations for each variable, which is 391 for all variables. According to the descriptive analysis of cyber-security disclosure (CSD), the mean value of CSD is 0.0047505, indicating that, on average, CSD values are close to 0.4%, which is relatively low because CSD values are less than 1. It indicates that, on average, each company's disclosure of cybersecurity in its annual report is considered to be low. This is due to the fact that the average percentage of keyword disclosure is still low, and not every company publishes its annual report on the official website, and some of those that perform sometimes provide it in an unreadable scanned pdf format. In addition, the "Std. dev." column displays the standard deviation of each variable, which is a measure of the values' dispersion around the mean. The CSD standard deviation is 0.0021463, or 0.2%, indicating that there is a small variance in the level of cyber-security disclosure among Southeast Asian banking institutions.

Board size (BSIZE) has a minimum value of 1 and maximum of 21. As for the mean, it resulted in 7.877238. From this descriptive statistic, it shows that each company each year has at least one director and has a maximum of 21 directors. In average, each company has a total board of director (BOD) of 8. The "Std. dev." column shows the standard deviation of each variable, which is a measure of how spread out the values are from the mean. The standard deviation of BSIZE is 4.241464, which means that the values of BSIZE are spread out over a range of approximately 4 units. The mean value of Board Independence (BIND) for each company each year is 0.4831243 independent directors. It indicates that, on average, 48% of board members have no conflicts of interest that could compromise their impartiality and objectivity when making decisions. These board members are regarded independent because they have no substantial financial or personal ties to the organization or its leadership. Board Gender Diversity (BGDIV) has a mean value of 0.1816494, indicating that, on average, 18% of board of directors' members are female.

The control variables, such as profitability (PROV), show a mean value of 0.0063439. The standard deviation value is 0.021001, which indicates that the variation in the profitability between companies is relatively low. Other control variables such as leverage (LEV) show a mean value of 0.8544761 and standard deviation of 0.0991495 which also indicates a relatively low variation of leverage between companies. The mean value of the firm size (SIZE) is 38710.76 and standard deviation of 77459.42.

Overall, the summary statistics provide a quick and easy way to get an overview of the distribution of the variables in the dataset.

Regression Results

According to Corlett & Aigner (1971), the selection of the most appropriate multiple linear regression model for panel data needs to be conducted. After doing several analysis using chow test and LM test, it was determined that the fixed effect model or the random effect model was the most appropriate regression model for this study. To validate this selection further, it is necessary to conduct the Hausman test. The Hausman test compares the fixed effect model and the random effect model to determine which model is most applicable for analysis.

The prob > chi2 = 0.1648 is more than 0.1 which indicates that H0 is accepted. The Hausman test suggests that the Random Effect Model is a better regression estimation approach for this research than the Fixed effect Model.

Table 5. Regression Results

CSD	Coefficient	Std. err.	z	P>|z|	[95% conf.	interval]
BSIZE	-.0000103	.0000409	-0.25	0.802	-.0000905	.00007
BIND	.0004781	.0007066	0.68	0.499	-.0009068	.0018629
BGDIV	.0006353	.0008804	0.72	0.471	-.0010902	.0023609
PROF	.0035292	.0046755	0.75	0.450	-.0056347	.012693
LEV	.0019333	.0013813	1.40	0.162	-.000774	.0046406
SIZE	4.91e-09	2.40e-09	2.05	0.040	2.16e-10	9.61e-09
cons	.0026179	.0012842	2.04	0.041	.0001009	.0051348
sigma_u	.00138161					
sigma_e	.00157892					
rho	.43364481	(fraction of variance due to u_i)				

Sources: Data Proceed, 2022

The Stata output presents the results of a random-effects GLS regression (xtreg) for the variables CSD, BSIZE, BIND, BGDIV, PROF, LEV, and SIZE. The coefficients for the random-effects model are presented with their standard errors, z-scores, p-values, and 95% confidence intervals. From the table, p-values show that all variables except SIZE have a significant level greater than 5% indicating that those variables have insignificant relationship to the disclosure of cyber-security while only SIZE that has a p-value of 0.040, indicating that it is statistically significant at the 5% level. The table also indicates that if all independent variables have a value of zero, the number of cyber-security disclosures will rise by up to 0.003 percent. BSIZE's coefficient is -0.00000103, which indicates that if BSIZE score increases by 1%, the number of CSD will decrease by 0.00001%, assuming

http://journal.uinjkt.ac.id/index.php/akuntabilitas
DOI: 10.15408/akt.v16i1.35014

all other factors remain constant. Positive coefficients for BIND and BGDIV are 0.0004781 and 0.0006353, respectively. Consequently, if all other parameters remain constant, the number of CSD will increase by 0.0005% and 0.0006% if the BIND and BGDIV scores rise by 1%. Other control variables, such as PROV and LEV, have positive coefficients of 0.0035292 and 0.0019333, respectively. Consequently, if the PROV and LEV scores increase by 1%, the number of CSD will increase by 0.003% and 0.002%, respectively, presuming that all other factors remain constant. Additionally, the SIZE coefficient is positive 4.91e-09. This implies that a 1% increase in SIZE scores will result in a 4.91e-09% increase in CSD, assuming all other factors remain constant.

From this regression result, it can be seen that all independent variables (BSIZE, BIND, BGDIV), which are believed to have an effect on the dependent variable, turned out do not have a significant effect on the cyber-security disclosure. Indeed, the control variable, firm size, as measured by the natural logarithm of total assets, has a positive influence on voluntary cybersecurity disclosures.

Based on the regression result, it was discovered that the level of cyber- security disclosure in Southeast Asia banking industries are still low. This is presumably due to cyber-security disclosure is voluntary and there are no regulations requiring companies to include cyber-security information in their annual reports. Consistent with the research findings of Barry et al. (2021), which found that the strong regulatory framework in China externalizes cybersecurity, reducing the need for individual companies to disclose their cybersecurity awareness, Chinese firms have lower levels of cybersecurity disclosure.

This result also indicates that Firm Size, measured by natural logarithm of total assets, is the only significant factor that has an influence on the voluntary cyber-security disclosure in Southeast Asia banking companies. The positive coefficient suggests that larger companies with higher total assets are associated with a higher level of cyber-security disclosure, as represented by sentence-level of the 54 keywords in the annual reports of the listed Southeast Asian banking companies. This is consistent with the findings of previous research by Gao et al. (2020), who found that the frequency of cybersecurity risk disclosures increased linearly during the study period. This increase is due to several factors, including company size. However, the outcome of this research is subject to several factors. One factor influencing this event can be observed through the lens of agency theory, which suggests that as a company's assets increase, the shareholders, who act as principals, will exert heavier pressure on the agents or decision makers within the company to provide timely and transparent information. The situation can be resolved effectively by voluntarily disclosing information regarding cybersecurity within the annual report. Cybersecurity is deemed crucial to disclose in the annual report of the banking industry, particularly a well- established bank with a large total asset. Larger banks are more susceptible to cyber-attacks due to their diverse consumer base and use of sophisticated technology, which leaves them widely exposed. According to X. Gao & Zhong (2015), the more attractive firm invests more in information security, suffers more frequent attacks, and enjoys a lower expected benefit, whereas the hacker obtains a greater expected benefit from targeted attacks than under mass attacks. Therefore, it is essential that they include cyber-security information in their annual reports. As a result of the study, it was discovered that the higher the firm size, the awareness to disclose cyber-security information in the annual report also increases.

The relationship between Board Size (SIZE) as measured by the total number of directors and CSD was insignificant. This study does not provide conclusive evidence of a consistent relationship between board size and CSD in the annual reports of listed banking companies. Previous research by Mazumder & Hossain (2022) highlights a consistent finding that they were unable to establish a connection between board size and cyber-security disclosure. However, this result contradicts the first hypothesis mentioned before. This may be driven by some factors. In certain Southeast Asian nations, there is an absence of awareness regarding the significance of preventing cyberattacks. This suggests that these countries may not entirely comprehend the hazards and adverse effects associated with cyber threats (Mizan & Ma, 2019). The consequences of this blindness are frightening. Without a thorough understanding of the urgency in securing cyberattacks, these nations may have underdeveloped cybersecurity awareness, which subsequently contributes to the low level of board of director concern about CSD. This situation not only jeopardizes their own interests, but also the security of the international community as a whole.

Moreover, examining the association of board independence, which measured by number of independent directors in the board, and CSD, results showed that there is also insignificant influence board independence and cybersecurity disclosure in Southeast Asia banking industries. This is supported by previous research conducted by Nahar et al. (2016); Saggar & Singh (2017) as they did not find any conclusive evidence about significant relationship between board independence and risk disclosure in Bangladeshi banks and Indian listed companies. There are several plausible explanations for the insignificance of board independence. This may be due to the limited competence of members with vested interests to identify cyber threats and formulate recommendations for cyberspace resilience and risk mitigation The regression result also shows a low percentage of board independence of the total board which could limit their ability to advocate for more comprehensive cybersecurity disclosure.

In addition, board gender diversity (BGDIV), which measured by the percentage of female in the board, may not have a direct influence on CSD because regression shows insignificant relationship. This is inversely correlated to hypothesis 3 and previous research's conclusion from Radu & Smaili (2022); Saggar & Singh (2017) concluded that board gender diversity has a substantial positive influence on voluntary cyber security disclosure. Low percentages of female director in the board as shown in the regression result could limit their effectiveness in influencing cyber-security disclosure.

Furthermore, a potential reason for the lack of a significant relationship between profitability and leverage to cybersecurity disclosure is that cybersecurity risks can result in substantial financial losses, damage to reputation, and legal liabilities regardless of a business' profitability and leverage level. Companies may therefore prioritize cybersecurity disclosure as an approach of preventing these risks and protecting their stakeholders, regardless of their company profitability and leverage. In addition, disclosure regarding cybersecurity is not solely motivated by financial considerations. It is also impacted by stakeholder expectations, the need for transparency and accountability, and the importance of company safety. Companies may disclose their cybersecurity practices to demonstrate their dedication to protecting sensitive data and preserving consumer confidence.

http://journal.uinjkt.ac.id/index.php/akuntabilitas
DOI: 10.15408/akt.v16i1.35014

CONCLUSION

The role of Board Composition to the disclosure of cyber-security in annual reports of Southeast Asia banks has no significant influence. This means that board size, board independence, as well board gender diversity is not considered as a driven factors influencing CSD. This study focuses on how specific board composition characteristics, such as board size, independence, and gender diversity, influence CSD in listed commercial banks across Southeast Asia. Building on agency theory and resource-based theory, the study suggests that larger firms are more likely to have a positive impact on CSD. However, this study does not provide conclusive evidence regarding the consistent association between board composition and CSD in the annual reports of listed banks. Limited existing research on cybersecurity disclosure (CSD) serves as the motivation for this current study. Notably, this research stands out by examining the extent and determinants of CSD in banking companies within a developing economy specifically in Southeast Asia, where CSD is voluntary.

The paper acknowledges its limitations and proposes several directions for future research. Firstly, the study focuses exclusively on listed commercial banks, and therefore, the results cannot be generalized to companies in other sectors. Future research should include a larger sample comprising non-financial industry firms. Secondly, the study relies on automated content analysis, specifically counting keywords to assess the quantity of CSD. Future research could expand to include a more meaningful analysis by conducting a discourse analysis of CSD narratives. This approach would enable researchers to evaluate whether the language and tone of CSD convey meaningful information to stakeholders or if it is merely a generic and standardized practice. Additionally, future research should explore other variables that may impact voluntary CSD and examine the economic consequences, such as the effect on the cost of capital and firm value.

Despite its limitations, the authors believe that this study contributes valuable preliminary evidence to the limited research on CSD within the context of an emerging economy. To the best of the authors' knowledge, this is the first study to explore the relationship between board composition and CSD in Southeast Asia banking companies. The study serves as a catalyst for further research in this intriguing area. Beyond research implications, this study also carries policy implications. The findings shed light on the current state of CSD in banks, urging banking regulators and stock market regulators to consider issuing guidance to streamline reporting practices in the interest of stakeholders, including depositors and borrowers, and to maintain public trust in the banking industry. Notably, Zaini et al. (2010) highlights that risk-related disclosure is among the least common categories of disclosure for companies in emerging countries. Lastly, the study emphasizes to banks and corporate governance policymakers the importance of increasing independence and diversity in board composition by raising the percentage of independent and female directors.

The findings of these studies have implications for regulators, policymakers, and companies. Regulators can use the findings to better understand the current level of CSD and determine whether further guidance is required.

REFERENCES

Abeysekera, I. (2010). The influence of board size on intellectual capital disclosure by Kenyan listed firms. *Journal of Intellectual Capital*, *11*(4), 504–518. https://doi.org/10.1108/14691931011085650

Accenture. (1970, July 2). Accenture and Ponemon Institute Report: Cyber crime drains $11.7 million per business annually, up 62 percent in five years.

Newsroom. https://newsroom.accenture.com/news/accenture-and-ponemon- institute-report-cyber-crime-drains-11-7-million-per-business-annually-up- 62-percent-in-five-years.htm

Abraham, S., & Cox, P. (2007). Analysing the determinants of narrative risk information in UK FTSE 100 annual reports. *British Accounting Review*, *39*(3), 227–248. https://doi.org/10.1016/j.bar.2007.06.002

Adams, R. B., & Ferreira, D. (2009). Women in the boardroom and their impact on governance and performance. *Journal of Financial Economics*, *94*(2), 291–309. https://doi.org/10.1016/j.jfineco.2008.10.007

Adams, R. B., Hermalin, B. E., & Weisbach, M. S. (2011). The Role of Boards of Directors in Corporate Governance: A Conceptual Framework & Survey.

SSRN Electronic Journal. https://doi.org/10.2139/ssrn.1299212 Barry, T., Jona, J., & Soderstrom, N.S. (2021). The Impact of Country

Institutional Factors on Firm Disclosure: Cybersecurity Disclosures in Chinese Cross-Listed Firms. *SSRN Electronic Journal*.

Beretta, S., & Bozzolan, S. (2004). A framework for the analysis of firm risk communication. *International Journal of Accounting*, *39*(3), 265–288. https://doi.org/10.1016/j.intacc.2004.06.006

Bourdon, B. (2020, November 3). The avoidable mistakes executives continue to make after a data breach. Harvard Business Review. https://hbr.org/2017/11/the-avoidable-mistakes-executives-continue-to- make-after-a-data-breach

Cabedo, J. D., & Tirado, J. M. (2004). The disclosure of risk in financial statements. *Accounting Forum*, *28*(2), 181–200. https://doi.org/10.1016/j.accfor.2003.10.002

Campbell, J. L., Chen, H., Dhaliwal, D. S., Lu, H., & Steele, L. B. (2012). The Information Content of Mandatory Risk Factor Disclosures in Corporate Filings. *SSRN Electronic Journal*, *October*. https://doi.org/10.2139/ssrn.1694279

Coffey, B. S., & Wang, J. (1998). Board diversity and managerial control as predictors of corporate social performance. *Journal of Business Ethics*, *17*(14), 1595–1603. https://doi.org/10.1023/A:1005748230228

Corlett & Aigner. (1971). *regression, even when it seems inappropriate, mainly in order that*. 770–772.

Creado, Y., & Ramteke, V. (2020). Active cyber defence strategies and techniques for banks and financial institutions. *Journal of Financial Crime*, *27*(3), 771–780. https://doi.org/10.1108/JFC-01-2020-0008

Daily, C. M., & Dalton, D. A. N. R. (2003). *Introduction To Special Topic Forum Corporate Governance : Decades of Dialogue and Data*. *28*(3), 371–382.

Donnelly, R., & Mulcahy, M. (2008). Board structure, ownership, and voluntary disclosure in Ireland. *Corporate Governance: An International Review*, *16*(5), 416–429. https://doi.org/10.1111/j.1467-8683.2008.00692.x

Elzahar, H., & Hussainey, K. (2012). Determinants of narrative risk disclosures in UK interim reports. *Journal of Risk Finance*, *13*(2), 133–147. https://doi.org/10.1108/15265941211203189

Fama, E. (2012). Agency problems and the theory of the firm. *The Economic Nature of the Firm: A Reader, Third Edition*, *88*(21), 270–282. https://doi.org/10.1017/CBO9780511817410.022

FBI. (2021, March 17). IC3 releases 2020 internet crime report. FBI. https://www.fbi.gov/news/press-releases/fbi-releases-the-internet-crime- complaint-center-2020-internet-crime-report-including-covid-19-scam- statistics

http://journal.uinjkt.ac.id/index.php/akuntabilitas
DOI: 10.15408/akt.v16i1.35014

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

Gao, X., & Zhong, W. (2015). Information security investment for competitive firms with hacker behavior and security requirements. *Annals of Operations Research*, *235*(1), 277–300. https://doi.org/10.1007/s10479-015-1925-2

Hillman, A. J., & Dalziel, T. (2003). Boards of directors and firm performance: Integrating agency and resource dependence perspectives. *Academy of Management Review*, *28*(3), 383–396. https://doi.org/10.5465/AMR.2003.10196729

Jensen, M. C. (2005). Modern Industrial Revolution, Exit, and the Failure of Internal Control Systems. *SSRN Electronic Journal*, *December 2000*. https://doi.org/10.2139/ssrn.93988

Jensen, M. C., & Meckling, W. H. (1976). Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure, 3 J. Fin. Econ. 305 (1976). *Economic Analysis of the Law, H. MECKLING Copyright © 2003 by Blackwell Publishing Ltd*, 162–176.

Kent Baker, H., Pandey, N., Kumar, S., & Haldar, A. (2020). A bibliometric analysis of board diversity: Current status, development, and future research directions. *Journal of Business Research*, *108*(August 2019), 232–246. https://doi.org/10.1016/j.jbusres.2019.11.025

Kolsi. (2017). Journal of Accounting in Emerging Economies Article information : The Determinants of Corporate Voluntary Disclosure Policy : Evidence from Abu Dhabi Securities Exchange (ADX). *Journal of Accounting in Emerging Economies*, *7*(2).

Krus, C. M. (2012). Who is listening? The SEC emphasizes importance of cybersecurity disclosure. *Journal of Investment Compliance*, *13*(1), 30–32. https://doi.org/10.1108/15285811211216673

Kshetri, N. (2008). Chinese technology enterprises in developing countries: sources of strategic fit and institutional legitimacy. *The Rapidly Transforming Chinese High-Technology Industry and Market*, 181–200. https://doi.org/10.1016/b978-1-84334-464-3.50012-x

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

Linsley, P. M., & Shrives, P. J. (2006). Risk reporting: A study of risk disclosures in the annual reports of UK companies. *British Accounting Review*, *38*(4), 387–404. https://doi.org/10.1016/j.bar.2006.05.002

Loasby, B. J. (1979). Review Authors: Brian J . Loasby Review by : Brian J . Loasby Published by : Wiley on behalf of the Royal Economic Society Stable URL : http://www.jstor.org/stable/2231527 Accessed : 27-06-2016 01 : 38 UTC. *The Economic Journal*, *89*(356), 969–970. http://www.jstor.org/stable/2231527

Lopes, P. T., & Rodrigues, L. L. (2007). Accounting for financial instruments: An analysis of the determinants of disclosure in the Portuguese stock exchange. *International Journal of Accounting*, *42*(1), 25–56. https://doi.org/10.1016/j.intacc.2006.12.002

Matters, B. (2021). *Ey-Cbm-Cybersecurity-Disclosures-2021*. *September*, 1–10.

Mazumder, M. M. M., & Hossain, D. M. (2022). Voluntary cybersecurity disclosure in the banking industry of Bangladesh: does board composition matter? *Journal of Accounting in Emerging Economies*. https://doi.org/10.1108/JAEE-07-2021-0237

Mirchandani, B. (2018, September 4). Laughing all the way to the bank: Cybercriminals targeting U.S. Financial Institutions. Forbes. https://www.forbes.com/sites/bhaktimirchandani/2018/08/28/laughing-all- the-way-to-the-bank-cybercriminals-targeting-us-financial-institutions/

Mizan, N. S. M., & Ma, M. Y. (2019). *CNDS-Cybersecurity : Issues and Challenges in ASEAN Countries International Journal of Advanced Trends in Computer Science and Engineering Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse1781.42019.pdf CNDS- Cybersecurity : Issues a*. *October*.

Nahar, S., Azim, M., & Jubb, C. A. (2016). Risk disclosure, cost of capital and bank performance. *International Journal of Accounting and Information Management*, *24*(4), 476–494. https://doi.org/10.1108/IJAIM-02-2016-0016

Neri, L., Elshandidy, T., & Guo, Y. (2018). Determinants and impacts of risk disclosure quality: evidence from China. *Journal of Applied Accounting Research*, *19*(4), 518–536. https://doi.org/10.1108/JAAR-07-2016-0066

Oliveira, J., Rodrigas, L. L., & Craig, R. (2011). Risk-related disclosures by non-finance companies Portuguese practices and disclosure. *Managerial Auditing Journal*, *26*(9), 817–839. https://doi.org/10.1108/02686901111171466

PricewaterhouseCoopers. (n.d.-a). A C-suite united for a cyber-ready future. PwC. https://www.pwc.com/us/en/services/consulting/cybersecurity-risk- regulatory/library/global-digital-trust-insights.html

PricewaterhouseCoopers. (n.d.-b). PWC Pulse Survey: Managing Business Risks. PwC. https://www.pwc.com/us/en/library/pulse-survey/managing-business- risks.html

Prince, J. Ben, & Dwivedi, N. (2013). A third dimension to understanding voluntary disclosures. *Journal of Business Strategy*, *34*(4), 48–54. https://doi.org/10.1108/JBS-11-2012-0063

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

Saggar, R., & Singh, B. (2017). Corporate governance and risk reporting: Indian evidence. *Managerial Auditing Journal*, *32*(4–5), 378–405. https://doi.org/10.1108/MAJ-03-2016-1341

Siegel, B. (2022, January 24). Ransomware payments up 33% in Q1 2020. Coveware. https://www.coveware.com/blog/q1-2020-ransomware- marketplace-report

Srinidhi, B., Gul, F. A., & Tsui, J. (2011). Female directors and earnings quality. *Contemporary Accounting Research*, *28*(5), 1610–1644. https://doi.org/10.1111/j.1911-3846.2011.01071.x

Syeliya Md Zaini, Grant Samkin, Umesh Sharma, H. D. (2010). Journal of Accounting in Emerging Economies. *Journal of Applied Accounting Research*, *11*(1). https://doi.org/10.1108/jaar.2010.37511aaa.003

Tejedo-Romero, F., Rodrigues, L. L., & Craig, R. (2017). Women directors and disclosure of intellectual capital information. *European Research on Management and Business Economics*, *23*(3), 123–131. https://doi.org/10.1016/j.iedeen.2017.06.003

Terjesen, S., Couto, E. B., & Francisco, P. M. (2016). Does the presence of independent and female directors impact firm performance? A multi-country study of board diversity. *Journal of Management and Governance*, *20*(3), 447–483. https://doi.org/10.1007/s10997-014-9307-8

Terjesen, S., Sealy, R., & Singh, V. (2009). Women directors on corporate boards: A review and research agenda. *Corporate Governance: An International Review*, *17*(3), 320–337. https://doi.org/10.1111/j.1467-8683.2009.00742.x

United Nations. (n.d.). Developing countries most vulnerable to cyberattacks – un UN news. United Nations. https://news.un.org/en/story/2011/12/397922 Veltrop, D. B., Molleman, E., Hooghiemstra, R., & van Ees, H. (2018). The

Relationship Between Tenure and Outside Director Task Involvement: A Social Identity Perspective. *Journal of Management*, *44*(2), 445–469. https://doi.org/10.1177/0149206315579510

Virtanen, A. (2012). Women on the boards of listed companies: Evidence from Finland. *Journal of Management and Governance*, *16*(4), 571–593. https://doi.org/10.1007/s10997-010-9164-z 155. https://doi.org/10.30630/jam.v15i2.114

http://journal.uinjkt.ac.id/index.php/akuntabilitas
DOI: 10.15408/akt.v16i1.35014