CIREBON INTERNATIONAL CONFERENCE ON EDUCATION AND ECONOMICS (CICEE)

CYBER RISK MANAGEMENT DISCLOSURE

Agung Musta'in[1], Mira Sofiani[2], Diani Putri Ramadhanty[3], Siti Jubaedah[4]
[1,2,3,4] Universitas Swadaya Gunung Jati, Cirebon, Indonesia

*Corresponding author: agungmustain17@gmail.com

Abstract
Cyberattacks have become a significant threat to critical infrastructure and digital businesses. This research examines the importance of disclosing cyber risk management information in supporting investor confidence and corporate reputation management amid the growing threat. The study uses statistical data to highlight the prevalence of cyberattacks in ASEAN countries, with Indonesia leading in the number of cases. The voluntary disclosure of cyber risk management in corporate financial reports is studied in the context of factors such as company size, profitability and leverage. The results show that companies with larger size tend to make more extensive disclosures, while high profitability and low leverage also contribute to greater voluntary disclosure practices. The implications of this study highlight the need for the adoption of better disclosure practices as a strategy to manage information risk and build trust in today's digitalized global marketplace.
Keywords: Cyber Risk Management Disclosures, Size, Profitability, Leverage.

INTRODUCTION

Cyberattacks can compromise power grids, telecommunications networks, modern transportation infrastructure networks, and digital financial flows Greenberg, (2019). Financial businesses that have evolved towards digital, will continue to be faced with various cyber threats such as ransomware attacks, business email compromise (BEC), distributed denial-of-service attacks, data breaches, and the spread of remote access malware exploiting international transfer systems, and suspicious theft (Dupont et al., 2023).

According to Kaspersky's statistics also released by Interpol on the ASEAN cyberattack threats in 2021, Indonesia ranks first with 1.3 million most frequent cyberattack cases; Vietnam ranks second with 886,874 cases; Thailand ranks third with 192,652 cases; the Philippines ranks fourth with 137,366 cases; and Malaysia, Indonesia's closest neighbor, ranks fifth with 136,636 cases BSSN, (2022). According to A. T. Kearney, a global consulting firm, ASEAN countries are expected to experience losses of 10 quadrillion due to the many cyber-attack cases Natalia & Aprilia, (2023), Priatna Sari et al., (2023).

Due to the high rate of data breaches, according to Anderson et al., (2019), stakeholders and shareholders must be protected, with voluntary information disclosure programs, such as cyber risk management disclosures. Therefore, risk disclosure is very important in a business context, especially in the stock market. According to Ibrahim et al., (2019), more transparent reporting will increase shareholder investor confidence.

According to Alsheikh & Alsheikh, (2020) and Al-Dubai & Abdelhalim, (2021), state that shareholders and regulators demand companies to disclose reliable information and risk information as investment decision-makers. According to Md Zaini et al., (2018) and Tsang et al., (2019) voluntary disclosure in developing countries, including Indonesia, is still low. Scholarly publications defining cyber risk management disclosures are still low and hard to find (Strupczewski, 2021). Therefore, this research is very important as it relates to voluntary disclosure of cyber risk management information.

LITERATURE REVIEW

Size of Cyber Risk Management Disclosure

Voluntary disclosures including cyber risk management disclosures in corporate financial statements have become an important and popular research topic in the accounting literature. A number of studies show that firm size, as measured by total assets as well as by market capitalization, has a significant influence on the level of voluntary disclosure. Ali, Chen and Radhakrishnan, (2007) found that companies with larger size tend to make more extensive voluntary disclosures, which may be related to their efforts to manage reputation and improve access to capital. Similar results were also found by Haniffa and Cooke, 2002), which showed that large companies tend to make more disclosures in an effort to meet public and investor expectations. However, there are also studies that indicate that the relationship between firm size and voluntary disclosure may vary depending on the institutional context. As research conducted by Abdullah and Ismail, (2016) suggest that in countries with diverse ownership structures, the effect of firm size on voluntary disclosures including cyber risk management disclosures may be influenced by complex institutional factors. Furthermore, (Hossain & Reaz, 2007) found that in the context of emerging capital markets, firm size is not always the main predictor of the level of voluntary disclosure, as factors such as stricter supervision from regulators can also influence the disclosure practices of cyber risk management information.

Profitability of Cyber Risk Management Disclosure

Corporate profitability is often considered as a factor influencing the level of voluntary disclosure including cyber risk management disclosure in accounting literature. Voluntary disclosure is a strategy used by companies to increase transparency and build trust with stakeholders. According to a study conducted by(Dhaliwal et al., 2011), companies with higher levels of profitability tend to make more extensive voluntary disclosures including cyber risk management information. They noted that companies with good financial performance may feel more confident to disclose additional information as a way to demonstrate their performance and financial health to investors and the public. Similar findings were also presented by Soliman and Ben-Amar, (2022), who found that more profitable firms have a tendency to be more transparent in disclosing information about their managerial practices. However, research by Hossain and Reaz, (2007)suggests that the relationship between profitability and voluntary disclosure can be complex depending on the industry context and firm characteristics. They suggest that in certain sectors, firms may be more inclined to withhold strategic information despite having high profitability, perhaps to maintain a competitive advantage.

Leverage of Cyber Risk Management Disclosure

advantage Leverage, or the level of corporate debt, is an important factor in the accounting literature related to voluntary disclosure practices including information on cyber risk

management. Voluntary disclosure is often considered a corporate strategy to manage market perceptions and reduce information asymmetry between management and investors. The study by Chen et al, (2014) found that companies with high levels of leverage tend to make more extensive voluntary disclosures including cyber risk management disclosures. They indicated that companies may be more inclined to disclose additional information to increase transparency and gain trust from stakeholders, particularly in an effort to reduce the risk of negative perceptions associated with high debt levels. However, research by Barton and Simko, (2002) suggests that the relationship between leverage and voluntary disclosure can be complex and dependent on financial conditions and industry. They found that firms may reduce their voluntary disclosures when their leverage increases, to avoid disclosing information that could potentially affect the cost of capital or the firm's credit standing. Similar findings were also presented by Conyon and Sadler, (2010), who found that firms with higher leverage tend to make more limited voluntary disclosures, possibly for competitive security reasons.

CONCLUSION

The research highlights the complexity of the challenges faced by enterprises in managing their sensitive information. The study illustrates the importance of transparency in the face of the growing threat of cyberattacks. The statistics presented show significant attack rates in ASEAN countries, with Indonesia taking the top spot. With the emergence of threats such as ransomware and the spread of malware, the need for cyber risk disclosure is becoming increasingly urgent for companies, particularly in supporting investor confidence and reputation management. In addition, factors such as firm size, profitability and leverage have been shown to influence the level of voluntary disclosure, reflecting firms' efforts to manage market perceptions and mitigate the information risks faced. Therefore, this study highlights the importance of adopting better disclosure practices in the context of cyber risk management, not only as a regulatory necessity, but also as an integral strategy to build corporate trust and resilience in today's digital era.

REFERENCES

Abdullah, S. N., & Ismail, K. N. I. K. (2016). Women directors, family ownership and earnings management in Malaysia. Asian Review of Accounting, 24(4), 525–550. https://doi.org/10.1108/ARA-07-2015-0067

Al-Dubai, S. A. A., & Abdelhalim, A. M. M. (2021). The relationship between risk disclosure and firm performance: empirical evidence from Saudi Arabia. J. Asian Finance Econ. Bus, 8, 255–266. https://doi.org/https://doi.org/10.13106/jafeb.2021.vol8.no6.0255

Ali, A., Chen, T.-Y., & Radhakrishnan, S. (2007). Corporate disclosures by family firms. Journal of Accounting and Economics, 44(1–2), 238–286. https://doi.org/10.1016/j.jacceco.2007.01.006

Alsheikh, A., & Alsheikh, W. (2020). Board quality and risk disclosure: evidence from Saudi arabian publicly listed companies. Int. J. Supply Chain Manag, 9, 2051–3771. Google Scholar

Anderson, R., Barton, C., Boehme, R., Clayton, R., & Ganan, C. (2019). Measuring the Changing Cost of Cybercrime. The 18th Annual Workshop on the Economics of Information Security. https://doi.org/doi.org/10.17863/CAM.41598

Barton, J., & Simko, P. J. (2002). The Balance Sheet as an Earnings Management Constraint. The Accounting Review, 77(s-1), 1–27. https://doi.org/10.2308/accr.2002.77.s-1.1

BSSN. (2022). RI hit by 700 million cyber attacks in 2022, extortion mode dominant. CNN Indonesia. https://www.cnnindonesia.com/teknologi/20220701164212-192-816150/ri-dihantam-700-juta-serangan-siber-di-2022-modus-pemerasan-dominan

Chen, C. J. P., Ding, Y., & Xu, B. (2014). Convergence of accounting standards and foreign direct investment. The International Journal of Accounting, 49(1), 53–86. https://doi.org/10.1016/j.intacc.2014.01.007

Conyon, M., & Sadler, G. (2010). Shareholder Voting and Directors' Remuneration Report Legislation: Say on Pay in the UK. Corporate Governance: An International Review, 18(4), 296–312. https://doi.org/10.1111/j.1467-8683.2010.00802.x

Dhaliwal, D. S., Li, O. Z., Tsang, A., & Yang, Y. G. (2011). Voluntary Nonfinancial Disclosure and the Cost of Equity Capital: The Initiation of Corporate Social Responsibility Reporting. The Accounting Review, 86(1), 59–100. https://doi.org/10.2308/accr.00000005

Dupont, B., Shearing, C., Bernier, M., & Leukfeldt, R. (2023). The tensions of cyber-resilience: From sensemaking to practice. Computers & Security, 132, 103372. https://doi.org/10.1016/j.cose.2023.103372

Greenberg, A. (2019). Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most. Anchor Books.

Haniffa, R. M., & Cooke, T. E. (2002). Culture, Corporate Governance and Disclosure in Malaysian Corporations. Abacus, 38(3), 317–349. https://doi.org/10.1111/1467-6281.00112

Hossain, M., & Reaz, M. (2007). The determinants and characteristics of voluntary disclosure by Indian banking companies. Corporate Social Responsibility and Environmental Management, 14(5), 274–288. https://doi.org/10.1002/csr.154

Ibrahim, A., Habbash, M., & Hussainey, K. (2019). Corporate governance and risk disclosure: evidence from Saudi Arabia. International Journal of Accounting, Auditing and Performance Evaluation, 15(1), 89. https://doi.org/10.1504/IJAAPE.2019.096748

Md Zaini, S., Samkin, G., Sharma, U., & Davey, H. (2018). Voluntary disclosure in emerging countries: a literature review. Journal of Accounting in Emerging Economies, 8(1), 29–65. https://doi.org/10.1108/JAEE-08-2016-0069

Natalia, T., & Aprilia, Z. (2023). Cyberattacks in the Financial Sector, not just BCA & BPD Bali. CNBC Indonesia. https://www.cnbcindonesia.com/market/20231117134511-17-489875/serangan-siber-di-sektor-keuangan-bukan-cuma-bca-bpd-bali

Priatna Sari, Y., Suhardjanto, D., Probohudono, A. N., & Honggowati, S. (2023). The Stakeholders Influence On Risk Disclosure Of State-Owned Enterprises. Media Riset

Akuntansi, Auditing & Informasi, 23(1), 131–150. https://doi.org/10.25105/mraai.v23i1.16473

Soliman, M., & Ben-Amar, W. (2022). Corporate social responsibility orientation and textual features of financial disclosures. International Review of Financial Analysis, 84, 102400. https://doi.org/10.1016/j.irfa.2022.102400

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

Tsang, A., Xie, F., & Xin, X. (2019). Foreign Institutional Investors and Corporate Voluntary Disclosure Around the World. The Accounting Review, 94(5), 319–348. https://doi.org/10.2308/accr-52353