JDA | Jurnal Dinamika Akuntansi
Vol. 15, No. 2, 2023, pp. 180-190

p-ISSN 2085-4277 | e-ISSN 2502-6224
http://journal.unnes.ac.id/nju/index.php/jda

# Cyber Risk Management Disclosure of State-Owned Enterprises

**Yeni Priatna Sari**[1] ✉ **, Djoko Suhardjanto**[2]**,**
**Agung Nur Probohudono**[3]**, and Setianingtyas Honggowati**[4]

[1]Department of Accounting, Politeknik Harapan Bersama, Tegal
[2,3,4]Doctoral Program in Economics, Universitas Sebelas Maret, Surakarta

**DOI**: http://dx.doi.org/10.15294/jda.v15i2.44817

**Submitted: June 6th, 2023 Revised: August 1st, 2023 Accepted: October 16th, 2023 Published: October 17th, 2023**

**Abstract**

**Purposes:** The purpose of this research is to compile a cyber risk management disclosure index of State-Owned Enterprises (SOEs). This index is used to provide an overview of the disclosures that are expected by the stakeholders which are disclosed in the annual report of SOEs. Disclosure of cyber risk management is important for a business entity to show that the entity has readiness in facing digital technology which is one of the keys to the company's success.

**Methods:** The research method used is mixed method. The type of data is primary data sourced from Forum Group Discussion (FGD) inviting SOE Directors, audit committees, investors, risk management practitioners, and academics on how important the cyber risk management disclosure items formulated earlier are. Thirty corporate and SOE practitioners have been interviewed and internal auditor practitioners in SOEs have been sources of validity. The steps in compiling the index are first collecting cyber risk management disclosure items from the previous research and looking at ISO 31000 provisions regarding risk management.

**Findings:** The result of this study is the composition of the cyber risk management disclosure index as many as 18 (eighteen) items with weighting on each disclosure item.

**Novelty:** The novelty of this study is the formulation of a cyber risk management measurement index which is very important in relation to risk management in a company. This research is important to be carried out as a formulation of indicators for cyber risk management management carried out by the company. Researchers anticipate that this cyber risk management disclosure index will help the government create disclosure items for cyber risk management and serve as a norm for disclosing SOE cyber risk management in its annual report.

**Keywords***: Disclosure, Cyber Risk Management, SOEs, Financial Statements, Voluntary Disclosure.*

**How to cite (APA 7th Style)**

*Sari, Y. P., Suhardjanto, D., Probohudono, A. N., & Honggowati, S. (2023). Cyber Risk Management Disclosure of State-Owned Enterprises. Jurnal Dinamika Akuntansi, 15(2), 180-190.*

## INTRODUCTION

The industrial revolution can be said as a big change and fundamental to the pattern of human behavior in managing resources and producing goods that have an impact on the social, economic and cultural order of society. Currently, the industrial revolution 4.0 has brought many rapid changes to various fields of human life. Various countries have been competing to win the competition in the digital business world. Dalam penelitian nya Kunjana said in his writing that various cities in all countries in the world have been touched by digital technology in almost all economic sectors (Kunjana, 2017).

author (✉)
E-mail: yeni.priatna@gmail.com

Companies in the world invest most of their funds to make digital transformation. The Covid-19 pandemic has triggered the use of technology in various fields of life (McKinsey&Company, 2020). The lifestyle that has been used to be done offline, must change to use online because of the pandemic. It has an impact in all fields of life including economic and business life. The pandemic that occurred in ASEAN countries was very felt and triggered the acceleration of disruption in the economic sector throughout the region as a result of the decline in the tourism industry, disruption in air transportation, weakening purchasing power due to lockdowns, communal quarantine, and travel restrictions (ASEAN, 2020). The disruption that occurred due to the pandemic caused the development of the use of digital financial applications and the increasing use of other digital media as recommended by Deloitte (Deloitte, 2020). Besides Deloitte, research conducted by Nagel (Nagel, 2020) also recommends for companies that one of the solutions in overcoming the current pandemic is to implement digital work tools.

Technological changes that force companies to change work patterns or work tools make companies have to further improve their information technology governance. The ease that is given in providing information opens the door for hackers to enter the realm of the company. In 2015 cyber crime became the second cause of economic fraud that occurred in the business world in Canada (CyberRisk, 2016). Research conducted by Kearney, a global consulting firm, countries in ASEAN are expected to face losses due to cybercrime of 10 quadrillion, as a consequence of not allocating substantial funds for cybersecurity (Natalia, 2018). CNNIndonesia.com said that Indonesia is currently the second country that is expected to be most frequently cyberattacked during the covid-19 pandemic (CNN, 2020). A survey conducted by Kaspersky in 2019 published on the CNN Indonesia page, revealed that cybercrime mostly happened to companies in Southeast Asia, especially in the first quarter of 2020. The number of crimes recorded in Indonesia was 192,591 cases, in Vietnam it was 244 thousand attacks, and Thailand was in third place with 144 thousand attacks, an increase from the data in the previous period and Malaysia experienced 132 thousand attacks (CNN, 2020).

Research on risk management disclosure has also been conducted by Amran (Amran et al., 2009) Hashim and Koon (Hashim & Koon, 2016), Jia (Jia et al., 2019), Lajili et al (Zeghal, 2005) and Bello et al (Bello et al., 2019). The research conducted by Amran was conducted on non-financial companies, while other companies are public companies. The research conducted by Jia et al., 2019 is a content analysis research conducted on 100 public companies in Australia examining the influence of the risk management committee, the independence of the risk management committee and the number of risk management committee meetings. The research conducted by (Zeghal, 2005) is a research related to risk management disclosure using stakeholder theory with the characteristics of directors, risk management committees and ownership structures as explanatory variables. While the research conducted by Bello et al (Bello et al., 2019) was conducted on 9 (nine) insurance companies in Nigeria within 5 (five) years which explained the size of the risk management committee and its effect on risk management disclosure. All of the above studies are research related to risk management disclosures and no one has revealed cyber risk management disclosures that are more specific to companies.

This research will develop cyber risk management disclosure items that have never existed in previous research. Therefore research on cyber risk management disclosure practices carried out by State Owned Enterprises using the disclosure scoring method to this time has never been done. Data sourced from the Organization for Economic Co-operation and Development (OECD) in 2017 stated that SOEs in some Asian countries have a lower level of risk disclosure than companies listed on exchanges (OECD, 2017). This makes this research important because SOE has an important role in the country's economy but does not disclose commensurate risks.

This research is important to do because technological disruption is so fast and makes companies have to adapt, as well as the ASEAN vision in 2040 and the AEC 2025 blueprint which makes ASEAN countries have to improve governance related to cyber risk management in companies in general and SOEs in particular. Moreover, there is a need for a comparative study of the disclosure of cyber risk management in SOES in ASEAN countries. The term SOE is used in Indonesia to refer to State-Owned Companies, while in Malaysia it is better known as GLC (Government Link Corporation), SOC (State Owned Corporation) in Vietnam and SOE (State Owned Enterprises) in Singapore and Thailand.

## METHODS

This research is a mixed methode study that will formulate a cyber risk management index from state-owned companies that have gone public. There are 2 (two) ways to create disclosure items for cyber risk management. Utilizing content analysis is the first strategy. A technique used in content analysis is counting the number of disclosure items (Drisko & Maschi, 2016). The researcher chose not to utilize this method since it was deemed inadequate because it merely measured the number of disclosure items. The disclosure scoring technique was employed in this investigation. Disclosure scoring is a method of quantifying the disclosure window made by a firm in an annual report is disclosure scoring or disclosure index (Martin et al., 2018).

This research try to create the item of disclosure to measure cyber risk management disclosure. Disclosure scoring is the creation of disclosure items that will be used based on previous research that has been done. Researchers will conduct mapping, and then look for the level of urgency of each disclosure item based on discussions unearthed from practitioners and verified by an expert in the field of risk management. The following are the steps in preparing cyber risk management disclosures:

The first step is for researchers to identify and map previous research related to cyber risk management disclosures that have been developed in research conducted by Joshie and Haes (Joshi et al., 2018). After identifying several previous studies and identifying cyber risk management disclosure items from several previous studies, researchers then formulated cyber risk management disclosure items.

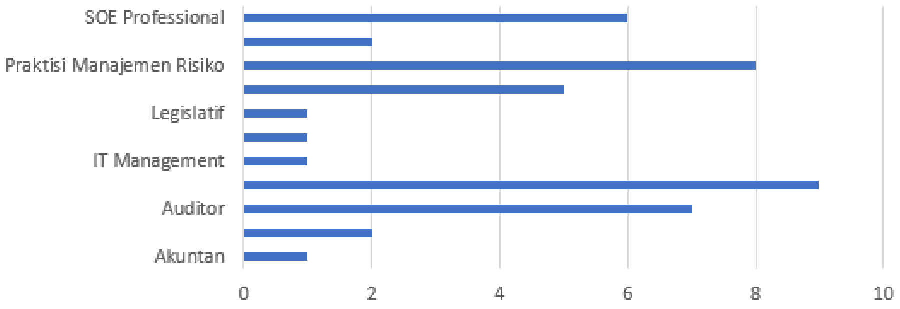
To formulate cyber risk management disclosure items, researchers conducted Focus Group Discussions (FGDs) with a total of 43 (forty-three) participants FGDs related to cyber risk management to analyze cyber risk management disclosures using the index/score method of each disclosure item. Furthermore, the items that get the highest weight reflect the issue of disclosure items that are most often informed and most needed by stakeholders (Suhardjanto & Miranti, 2010).

The activity of formulating the disclosure index is FGD conducted by inviting stakeholders and parties involved in making decisions on cyber risk management disclosure in SOEs or researchers who can be consulted. In this research, the FGD participants are practitioners who are familiar with risk management governance using ISO 31000. So that even though all are Indonesian citizens, it does not reduce the essence of the participants' understanding of the level of importance of cyber risk management.

In the disclosure scoring activity, researchers will take cyber risk management disclosure items that have been revealed in each previous research. Each participant is asked the level of importance and priority of cyber risk management disclosure items using a 7-scale Likert scale option. Participants of the discussion on the formulation of items on cyber risk management disclosure were academics in the field of risk management, corporate practitioners in SOE, risk management practitioners, and internal audit practitioners in SOEs. Participants in the discussion gave advice to researchers on the extent of disclosures made, as well as the priority of cyber risk management disclosures supplied by the company. Practitioners also offer guidance on the innovative disclosures that take place in the corporate environment.

The following is a description of the various professions of the Focus Group Discussion (FGD) participants that have been carried out as shown in table 1. After conducting focus group discussions with risk management practitioners, researchers looked at each company's annual report for the existence of each disclosure item and then multiplied it by the weight of each disclosure item that had been formulated.

**Table 1.** Profession of FGD Participants



Source: Processed Secondary Data (2022)

Furthermore, researchers also conducted validity and reliability tests with an intercoder index by practitioners in the field of risk management. The result of the validity and reliability test is the existence of valid and reliable Cyber Risk Management Disclosure items.

## RESULTS AND DISCUSSION

Information disclosure within the company consists of mandatory and voluntary disclosures. Voluntary disclosure refers to strategy risk, operational risk, empowerment risk, information process, technology risk as well as integrity risk (Kamaruzaman et al., 2019). More and more stakeholders need this voluntary risk disclosure. The underlying reason is that with this voluntary disclosure , stakeholders can better understand the company's strategy and performance (Chau & Gray, 2010).

Cyber risk is one of the technological risks faced by companies. Cyber risk is usually aimed at financial losses, changes or reputations of organizations due to information technology system errors. Cyber risks can impact several things such as: a) accidental access or unauthorized access to information systems; b) accidents over access to information system security; c) operational risks of information technology due to lack of system integrity (CyberRisk, 2016). The rise of various types of cybercrime is influenced by managerial restrictions on cyber risk. Cybercrime will always be a concern for businesses of all sizes. According to certain data, small-scale businesses are more frequently the targets of cybercrime. Without understanding cyberrisk and cybercrime, a business is unlikely to be able to solve the issue.

The following is a table of the results of the preparation of cyber risk management disclosure items that researchers obtained from several previous studies. Each item of disclosure is mapped according to a risk management plan that includes risk identification, risk assessment, risk response, risk control, and risk culture/governance. The organization should complete a number of disclosure items at each level of the risk management plan. This research uses the risk management process framework used by (Kosub, 2015b), while the disclosure items used are from research (Okul et al., 2019), (Haes & Grembergen, 2017), (Joshi et al., 2013).

These disclosure items are obtained using ISO 31000:2018 which is used as a risk management standard used by companies at the international level. The three elements of risk management, which consist of principles, frameworks and processes, this study will use disclosures related to the risk management process. The risk management process is a sequential and interrelated risk management activity.

The following is an explanation of the cyber risk management disclosure items that researchers use. The first disclosure item is risk identification. Risk identification means the company's activities to define and understand the company's business model, business goals, and assets, and understand the importance of IT to the company's business.

a. Cyber risk identification (Kosub, 2015a)

There are disclosures related to cyber risks faced, the company's annual report discloses

**Table 2.** Cyber Risk Management Disclosure Items

| Disclosure Items | (Kosub, 2015b) | (Okul et al., 2019) | (Haes & Grembergen, 2017) | (Joshi et al., 2013) | This Research, 2023 |
|---|---|---|---|---|---|
| **RISK IDENTIFICATION** | | | | | |
| 1. Cyber risk identifiction | ✓ | | | | ✓ |
| 2. IT-related business models | ✓ | | | | ✓ |
| 3. IT as a strategic issue | | | | ✓ | ✓ |
| 4. IT strengths as opportunities | | | | ✓ | ✓ |
| **RISK ASSESMENT & VALUATION** | | | | | |
| 5. Cyber assets are valuable assets | | ✓ | | | ✓ |
| 6. Cyber assets as a intangible asset | | | | ✓ | ✓ |
| **RISK RESPONSE** | | | | | |
| 7. Information and cyber security policy | | | | | ✓ |
| 8. Risk communication with stakeholders | | | | ✓ | |
| 9. Insurance / cyber security insurance | | | | | ✓ |
| 10. Company spending related to IT | | | | ✓ | ✓ |
| **RISK CONTROL** | | | | | |
| 11. Risk management IT committee capacity | | | ✓ | | ✓ |
| 12. IT Steering committee | | | ✓ | ✓ | ✓ |
| **RISK CULTURE & RISK GOVERNANCE** | | | | | |
| 13. IT governance | | | ✓ | | ✓ |
| 14. Information system planning | | | ✓ | | ✓ |
| 15. Management knowledge related to IT | | | ✓ | | ✓ |
| 16. Information and technology risk management governance | | | | | ✓ |

Source: Processed Secondary Data (2022)

about the challenges of the digital world, cyber risks and data breaches. Organizations may establish and maintain effective incident response and recovery plans by understanding potential cyber hazards. Knowing what types of incidents may occur allows businesses to better plan for them. Identifying cyber risks is the first thing that companies should do. This identification activity can be carried out by discussing with company leaders or with IT experts both within the company and outside the company.

b. IT-related business model (Kosub, 2015b)

Explains the business model that makes the company have to adapt to technology. Disclosure can be in the form of digital business, supply chain, big data, cloud databases or business models related to information and technology in helping company operations. The extent to which the company's use in technology has a major influence on the cyber risk management carried out by the company. In addition, the linkage of company technology will also increase the cyber risk that will be experienced by a company.

c. IT as a strategic issue (Joshi et al., 2013)

Policies related to IT become a strategic issue displayed by the company. IT-related matters are important in the company. Disclosures about platforms, digital, disruption, blockchain, innovation illustrate disclosures about this. Issues related to technology that occur in the company can also be an indicator of the level of company attention to cyber risk management carried out by the company. How much the company pays attention to handling cyber breach events is an indicator that must be considered.

d. IT power as an opportunity (Joshi et al., 2013)

The disclosure in question is that the power of IT in the company is disclosed as an opportunity for the company, providing broad benefits for the sustainability of the company. Disclosure in the form of technological advantages owned by the company is highlighted in the company's annual report. Businesses that triumph in technological competitions must think that their superior technology management skills will be a competitive advantage in and of itself.

The next stage is risk assessment and valuation.  Risk assessment is to quantify the risk and determine the likelihood of cyber risk events that will occur in the company (Kosub, 2015a).

a. Cyber assets as valuable assets (Okul et al., 2019)

The definition of cyber assets according to IT Law Wiki is electronic devices and programmable communication networks including hardware, software, and data (Wiki, 2012). This disclosure shows that the company's cyber assets in the form of information, data, hardware, software, documents, personal resources and company conditions are valuable assets for the company.Cyber assets are valuable assets for organizations in today's digital age due to their critical role in business operations, data management, and overall competitiveness. Here's an explanation of why cyber assets are considered valuable cyber assets used for data storage and management. Cyber assets include digital databases, servers, and storage systems that hold an organization's data. Data is often considered one of a business's most valuable assets. It includes customer information, financial records, intellectual property and operational data, all of which are important for decision making and maintaining business operations. Cyber asset such as software systems and automation tools, contribute to improved operational efficiency. They streamline processes, reduce manual work and improve resource allocation, ultimately leading to cost savings and improved profits.

b. Cyber assets as intangible assets (Joshi et al., 2013)

Disclosures about the company's cyber assets are disclosed as intangible assets. Disclosures such as digital assets, software as intangible assets illustrate this disclosure. The corporation acknowledges the value of these assets by disclosing them as intangible assets, demonstrating their importance to the organization. This is significant because it can demonstrate how much attention businesses give to their cyber assets.

The stage of risk management activities after risk assessment is to respond/treat the risk. Response to risk can be done in several ways including avoiding risk, mitigating risk, transferring risk and accepting the risk itself. The disclosure items used in this study are the expression of information security policies displayed by the company and the explicit expression of IT-related expenditures made by the company (Joshi et al., 2013). In addition, researchers also compiled disclosure sub-items related to cyber security insurance and effective communication with stakeholders (Joshi et al., 2013).

a. Information policy and information security

Disclosures made regarding company policies related to corporate information and information security. Data security policies are another sign of effective cyber risk management on the part of the business. All employees should be aware of the company's security policies, since this will help ensure that all employees' protection efforts are successful.

b. Cyber communication with stakeholders (Joshi et al., 2013)

Cyber communication carried out by the company in an effort to communicate cyber risks to stakeholders. Disclosures about social media and disclosures through other media illustrate this item. The company's attempts to mitigate cyber risk also heavily rely on communication with stakeholders. Here, cyber communication is being used to spread information about the company's efforts to stop data breaches and to interact effectively with all stakeholders. Stakeholders will have a favourable perception as a result of good communication. While ineffective communication will give customers a bad view of the business and convey the idea that the business does not take cyber hazards seriously.

c. Insurance/cyber security insurance

Disclosure about insurance especially related to cyber security insurance illustrates this disclosure. An important aspect of controlling cyber risk in businesses is the significance of cyber risk insurance. In the event of a data breach, both the company's assets and reputation may be lost. Consequently, the business needs insurance to cover cyber threats.

d. IT-related corporate expenditures (Joshi et al., 2013)

Company disclosures related to company expenditures that have been made in an effort to make IT breakthroughs and development. Disclosures such as software licenses, IT staff, networks, servers, enterprise software, data center systems, software development, communication services, investment hardware illustrate this disclosure.

Risk control disclosures are also used by researchers to show the existence of risk management in the company. Risk control is a company activity to monitor and proactively supervise the risks that may occur in the company(Kosub, 2015a). Researchers see that risk control has been carried out in the company if at least the company discloses the existence of a risk committee, and the existence of an IT committee in the company (Joshi et al., 2013).

a. IT competence Risk management committee (Haes & Grembergen, 2017)

Disclosure of competencies related to information and technology risk management committee in the company. The Risk Management Committee should be mandatory in the company. Similarly, competencies related to digitalization and information technology. Because capabilities in the field of information and technology have an important role in managing cyber risks in the company. Minimum insight related to digitalization and information technology.

b. IT steering committee (Haes & Grembergen, 2017)

The IT steering committee, often simply called the "steering board," is the key governance body within an organization responsible for making strategic decisions related to IT initiatives and resources. . This committee plays a key role in aligning IT with the organization's business goals and objectives. Disclosure of the existence of a special committee related to IT in the company. Information about IT committees that deal with cyber hazards is crucial. because the risk management committee in the organization will oversee the risk control operations carried out by this committee.

The last item in the cyber risk management disclosure is the disclosure of risk culture and risk governance. Risk culture and risk governance are company activities to take various actions that can be taken to prevent unwanted cyber attacks from happening to the company (Haes & Grembergen, 2017). When a company discloses its compliance with IT governance, the existence of information system planning, the existence of adequate management knowledge in terms of IT, and the existence of a cyber risk governance program implemented by the company, researchers will examine disclosures related to risk management culture and governance in the company.

a. IT governance (Haes & Grembergen, 2017).

Information and technology governance (IT governance) is a framework and set of processes that organizations put in place to ensure that their information and technology assets are managed, used and protected. effectively, in accordance with the strategic goals of the organization. IT governance encompasses a range of activities, policies, and structures designed to guide decision making, risk management, and resource allocation in IT. Disclosures related to IT governance in the company. Can be disclosed in the form of IT governance, IT compliance and ICT governance. Disclosures related to IT governance can be made with disclosures related to the company's compliance with applicable rules related to the management of information technology and the internet.

b. Information system planning (Haes & Grembergen, 2017)

Information systems planning is the process of designing, developing, and strategically implementing information systems to support the business objectives and operational needs of an organization. This includes assessing current technology infrastructure, determining future IT needs, setting priorities, and creating a roadmap for technology investments and systems implementation. Information systems planning ensures that technology is aligned with the organization's goals and helps optimize the organization's operations and decision-making. Disclosures related to information system planning such as IT implementation, digital base, digital information system can describe this disclosure. Good planning is the final consequence of risk management. Planning for the installation of IT, information systems, and company data security is a sign of how well the business is managing its exposure to cyber risk.

c. IT-related management knowledge (Haes & Grembergen, 2017)

Information technology management knowledge refers to the understanding and expertise required to effectively manage IT resources and activities within an organization. It covers a variety of aspects including strategic planning, resource allocation, risk management, project management and leadership, all tailored to the specific needs of the sector. IT. This knowledge is essential for aligning IT with business goals, optimizing IT operations, and ensuring the safe and effective use of technology to support organizational goals. IT becomes strategic and illustrates management knowledge related to IT. Disclosures such as IT strategic, technological innovation, ICT strategic illustrate this disclosure. It's necessary to reveal management-related IT expertise in addition to IT planning and information systems. The disclosure of the management's and directors' information technology proficiency serves as evidence of this disclosure.

d. IT-related risk management

Information technology management knowledge refers to the understanding and expertise required to effectively manage IT resources and activities within an organization. It covers a variety of aspects including strategic planning, resource allocation, risk management, project management and leadership, all tailored to the specific needs of the sector. IT. This knowledge is essential for aligning IT with business goals, optimizing IT operations, and ensuring the safe and effective use of technology to support organizational goals. Disclosures related to risk management in terms of IT and cyber such as disclosures of IT risk, ICT risk, digital implementation, digital innovation, digital transformation. In reality, the disclosure of IT-related risk management and the disclosure of cyber risk identification are very similar. The distinction in this disclosure is also related to potential dangers associated with technology and cyberspace that may arise in businesses that have used technology.

## CONCLUSIONS

The preparation of the cyber risk management index aims to provide early warning to the company on how the company conducts governance related to cyber risk in the company. The disclosure items that have been developed are a mapping of various prior studies to industry practitioners, researchers, and risk management practitioners that have undergone validity and reliability assessments.

Cyber risk management disclosure is importance in today's digital landscape due to several significant reasons: a) Company need for transparency and accountability: Disclosing cyber risk management practices and incidents promotes transparency and accountability within an organization. It shows that the organization is willing to share information about its cybersecurity efforts, which can enhance trust among stakeholders; b) Increasing investor confidence: Investors, both institutional and individual, consider cybersecurity practices and risks when making investment decisions. Comprehensive disclosure can boost investor confidence by demonstrating that the organization takes cyber threats seriously and has effective risk mitigation strategies in place; c) Regulatory Compliance: Many jurisdictions have put in place policies and laws requiring firms to disclose cybersecurity-related information. Failure to comply with these requirements may result in legal and financial consequences. Compliance with these rules is ensured by proper disclosure; d) Consumer Trust: Customers and clients are becoming increasingly concerned about the protection of their personal and financial data. Consumers can be reassured that their data is being handled appropriately and that the organization is committed to protecting their interests if cyber risk management methods are made public, e) The Third-Party Relationships: Before entering into partnerships or collaborations, business partners, suppliers, and vendors frequently assess their counterparts' cybersecurity posture. Comprehensive transparency can help these assessments and keep business partnerships healthy; f) Risk Assessment and Management: A detailed awareness of the hazards that a company faces is required for effective risk management. Organizations are encouraged to do thorough risk assessments and establish robust risk management policies as a result of public disclosure, ultimately improving cybersecurity resilience; g)Insurance and Risk Transfer: When a firm seek cybersecurity insurance, insurers frequently evaluate their risk management strategies. Full disclosure of these practices may result in better insurance terms and premiums; h) Incident Response and Recovery: In the event of a cybersecurity problem, swiftly and publicly disclosing the situation can help limit reputational harm and legal ramifications. Clear communication methods should be included in effective incident response and recovery strategies; i) Benchmarking and Improvement: Organizations can compare their cybersecurity measures to industry standards and peer groups by making their practices public. This technique can help to identify areas for improvement as well as guide strategic decisions; j) Reputation Management: A cyber incident can severely harm an organization's reputation. Timely and truthful disclosure can reflect the organization's commitment to resolving the issue and assist limit reputational harm; k) Legal Considerations: Failure to disclose cyber threats and occurrences might result in legal liability in some situations. Being forthright about cybersecurity issues can shield a company from potential litigation and regulatory measures; and shows long-term sustainability: Disclosure of risk management measures gives a signal that the firm is devoted to its long-term survival and performance in an increasingly digital world. In summary, cyber risk management disclosure is essential for promoting transparency, accountability, and trust. It helps organizations meet regulatory requirements, maintain good relationships with stakeholders, and demonstrate their commitment to safeguarding sensitive data and assets in an age of evolving cyber threats.

Items related to cyber risk management disclosure are crucial to disclose because they serve a number of important purposes, including informing stakeholders about the company's strategic condition, giving employees assurance that the company's cyber culture can keep them comfortable at work and prevent data breaches, demonstrating the effectiveness of top management or directors who have performed their duties, and providing references for investors. Companies with a low level of risk management disclosure may manage cyber risk management well, but if cyber risk management is not properly disclosed to stakeholders, it will reduce the potential for positive information provided. Impacts that can reduce the potential for positive information include reduced stakeholder trust, stock prices and employee confidence. Despite the fact that the business depends on the confidence and support of its stakeholders to operate.

Future research can also make disclosures about the quality of cyber risk management disclosures in companies. The quality of each cyber risk management item disclosed by the company will be measured in various ways. Development can be carried out in measuring each item such as the quality of the cyber risk management process carried out by the company, the effectiveness of communication carried out by the company to stakeholders and so on.

## REFERENCES

Amran, A., Manaf Rosli Bin, A., & Che Haat Mohd Hassan, B. (2009). Risk reporting: An exploratory study on risk management disclosure in Malaysian annual reports. Managerial Auditing Journal, 24(1), 39–57. https://doi.org/10.1108/02686900910919893

ASEAN. (2020). ASEAN ICT Masterplan 2020.

Bello, Z., Yusuf, I., & Nuhu, A. (2019). Effect of Board and Corporate Characteristics on Risk Management Disclosure of Listed Insurance Companies in Nigeria. MJBE Special Edition, 1(1), 2289–8018. https://jurcon.ums.edu.my/ojums/index.php/mjbe/article/view/2062

Chau, G., & Gray, S. J. (2010). Family ownership, board independence and voluntary disclosure: Evidence from Hong Kong. Journal of International Accounting, Auditing and Taxation, 19(2), 93–109. https://doi.org/10.1016/j.intaccaudtax.2010.07.002

CNN. (2020). RI Jadi Target Serangan Siber Terbesar Ke-2 di ASEAN Kala WFH. CNN Indonesia. https://www.cnnindonesia.com/teknologi/20200512172258-185-502625/ri-jadi-target-serangan-siber-terbesar-ke-2-di-asean-kala-wfh

CyberRisk. (2016). What is cyber risk, and why should I care? Northbridge Insurance. https://www.nbins.com/blog/cyber-risk/what-is-cyber-risk-2/

Deloitte. (2020). The Thailand Digital Transformation Survey Report 2020. https://www2.deloitte.com/content/dam/Deloitte/th/Documents/technology/th-tech-the-thailand-digital-transformation-report.pdf

Drisko, J. W., & Maschi, T. (2016). Content Analysis. Oxford University Press.

Haes, S. De, & Grembergen, W. Van. (2017). An Exploratory Study into IT Governance Implementations and its Impact on Business / IT Alignment An Exploratory Study into IT Governance Implementations and its Impact on Business / IT Alignment. Information Systems Management, 0530(October). https://doi.org/10.1080/10580530902794786

Hashim, F., & Koon, L. T. (2016). Corporate Risk Management Disclosure and Sustainability of Public Listed Companies in Malaysia: the Role of Diversification. Global Business and Management Research: An International Journal, January, 1–16.

Jia, J., Li, Z., & Munro, L. (2019). Risk management committee and risk management disclosure: evidence from Australia. Pacific Accounting Review, 31(3), 438–461. https://doi.org/10.1108/PAR-11-2018-0097

Joshi, A., Bollen, L., & Hassink, H. (2013). An Empirical Assessment of IT Governance Transparency: Evidence from Commercial Banking. Information Systems Management, 30(2), 116–136. https://doi.org/10.1080/10580530.2013.773805

Joshi, A., Bollen, L., Hassink, H., De Haes, S., & Van Grembergen, W. (2018). Explaining IT governance disclosure through the constructs of IT governance maturity and IT strategic role. Information and Management, 55(3), 368–380. https://doi.org/10.1016/j.im.2017.09.003

Kamaruzaman, S. A., Ali, M. M., Ghani, E. K., & Gunardi, A. (2019). Ownership structure, corporate risk disclosure and firm value: A Malaysian perspective. International Journal of Managerial and Financial Accounting, 11(2), 113–131. https://doi.org/10.1504/IJMFA.2019.099766

Kosub, T. (2015a). Components and challenges of integrated cyber risk management. Zeitschrift Für Die Gesamte Versicherungswissenschaft. https://link.springer.com/article/10.1007/s12297-015-0316-8

Kosub, T. (2015b). Determinants and Challenges of Integrated Cyber Risk Management. In Zeitschrift für die gesamte Versicherungswissenschaft. actuaries.asn.au. https://www.actuaries.asn.au/Library/Events/ASTINAFIRERMColloquium/2015/AFIRERM6Determinantsand.pdf

Kunjana, G. (2017). Revolusi Digital. Investor Daily. https://investor.id/editorial/revolusi-digital

Martin, R., Yadiati, W., & Pratama, A. (2018). Corporate Social Responsibility Disclosure and Company Financial Performance: Do High and Low Profile Industry Moderate the Result? Indonesian Journal of Sustainability Accounting and Management, 2(1), 15. https://doi.org/10.28992/ijsam.v2i1.42

McKinsey&Company. (2020). COVID-19-Facts-and-Insights-July-6. Global Health and Crisis Response, 1–54.

Nagel, L. (2020). The influence of the COVID-19 pandemic on the digital transformation of work. International Journal of Sociology and Social Policy, 40(9), 861–875. https://doi.org/10.1108/IJSSP-07-2020-0323

Natalia, E. C. (2018). Rp 10 kuadriliun, Risiko Kerugian Serangan Siber di ASEAN. CNBC Indonesia. https://www.cnbcindonesia.com/tech/20180124060959-37-2350/rp-10-kuadriliun-risiko-kerugian-serangan-siber-di-asean

OECD. (2017). OECD Survey of Corporate Governance Frameworks in Asia.

Okul, Ş., Muratoğlu, O., Aydın, M. A., & Bilge, H. Ş. (2019). A Review on Cyber Risk Management. Acta INFOLOGICA, 3(1). https://doi.org/10.26650/acin.502589

Suhardjanto, D., & Miranti, L. (2010). Indonesian Environmental Reporting Index. Jurnal Akuntansi Dan Auditing Indonesia, 13(1), 63–67.

Wiki, I. L. (2012). Cyber asset. Https://Itlaw.Fandom.Com/Wiki/Cyber_asset. https://itlaw.fandom.com/wiki/Cyber_asset

Zeghal, D. (2005). A Content Analysis of Risk Management Disclosures in Canadian Annual Reports. file:///H:/AADISERTASI UMI/AADISERTASI/MANAJEMEN RESIKO/RISK DISCLOSURE/lajili2005.pdf